

**III CONGRESSO INTERNACIONAL  
DE DIREITO, POLÍTICAS PÚBLICAS,  
TECNOLOGIA E INTERNET**

**TECNOLOGIAS DISRUPTIVAS, DIREITO E  
PROTEÇÃO DE DADOS I**

---

T255

Tecnologias disruptivas, direito e proteção de dados I [Recurso eletrônico on-line] organização  
III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade  
de Direito de Franca – Franca;

Coordenadores: Cildo Giolo Junior, Fausto Santos de Moraes e Suelen Carls – Franca:  
Faculdade de Direito de Franca, 2025.

Inclui bibliografia

ISBN: 978-65-5274-417-3

Modo de acesso: [www.conpedi.org.br](http://www.conpedi.org.br) em publicações

Tema: Governança, regulação e o futuro da inteligência artificial.

1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional  
de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

---

# **III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET**

## **TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS I**

---

### **Apresentação**

Entre os dias 30 de setembro e 3 de outubro de 2025, a Faculdade de Direito de Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 3 discute os impactos das tecnologias destrutivas no campo jurídico, com foco na aplicação da Lei Geral de Proteção de Dados e nas novas fronteiras da privacidade digital. As apresentações analisam o papel da inovação, da transparência e da responsabilidade jurídica em contextos digitais complexos. O grupo contribui para o debate sobre como a tecnologia pode ser aliada na proteção da dignidade humana e da segurança informacional.

# **COMERCIALIZAÇÃO DE DADOS BIOMÉTRICOS: A VENDA DA ÍRIS HUMANA NA PERSPECTIVA ÉTICA E LEGAL**

## **COMMERCIALIZATION OF BIOMETRIC DATA: THE SALE OF THE HUMAN IRIS FROM AN ETHICAL AND LEGAL PERSPECTIVE**

**Laura Helena Sato Herrera  
Mariana Clarindo dos Santos Facadio**

### **Resumo**

A pesquisa aborda a comercialização de dados biométricos, com foco na íris humana, sob a ótica ética e legal. O objetivo é analisar os impactos dessa prática à luz da Lei Geral de Proteção de Dados (LGPD), investigando riscos à privacidade e aos direitos fundamentais. A metodologia combina abordagem dedutiva e indutiva, com pesquisa bibliográfica, documental e de campo. O estudo examina o papel do Poder Judiciário e da Autoridade Nacional de Proteção de Dados (ANPD) na regulamentação do tema, propondo reflexões sobre a necessidade de maior proteção normativa frente aos avanços tecnológicos e ao uso comercial de dados sensíveis.

**Palavras-chave:** Dados biométricos, Lgpd, privacidade, Ética digital, Comercialização da íris

### **Abstract/Resumen/Résumé**

The research addresses the commercialization of biometric data, focusing on the human iris, from an ethical and legal perspective. The objective is to analyze the impacts of this practice in light of the General Data Protection Law (LGPD), investigating risks to privacy and fundamental rights. The methodology combines deductive and inductive approaches, including bibliographic, documentary, and field research. The study examines the role of the Judiciary and the National Data Protection Authority (ANPD) in regulating the issue, proposing reflections on the need for stronger legal safeguards in response to technological advances and the commercial use of sensitive data.

**Keywords/Palabras-claves/Mots-clés:** Biometric data, Lgpd, Privacy, Digital ethics, Iris commercialization

## INTRODUÇÃO

Em um cenário global em que os dados se tornaram a principal moeda de troca, a biometria passou a ocupar papel central na identificação e autenticação de indivíduos. Entre as diversas formas de dados biométricos, a íris humana se destaca por sua singularidade, imutabilidade e elevado grau de precisão, sendo considerada um dos métodos mais seguros para validação de identidade. Sua utilização, antes restrita a entidades governamentais e de alta segurança, foi amplamente incorporada por empresas privadas, instituições financeiras e plataformas digitais.

Entretanto, o avanço acelerado dessas tecnologias não foi acompanhado em conjunto por mecanismos normativos e garantias éticas. A possibilidade de comercialização da íris, isto é, a sua coleta, armazenamento e uso mediante algum tipo de retribuição financeira, escancara dilemas estruturais relacionados ao consentimento, à dignidade humana e à proteção de dados sensíveis. A prática, ainda que voluntária, impõe desafios jurídicos e morais, especialmente quando realizada junto a populações vulneráveis, que muitas vezes não compreendem integralmente o alcance do que estão cedendo. Entende-se necessário pesquisar como o uso comercial da biometria ocular, sem o devido marco regulatório, representa uma forma contemporânea de exploração consentida.

A presente pesquisa parte, então, da hipótese de que apesar do avanço do ordenamento jurídico brasileiro, como com a Lei Geral de Proteção de Dados (LGPD), este ainda permite brechas que favorecem o uso comercial de dados biométricos sensíveis, como a íris, em contextos de vulnerabilidade. Dessa forma, propõe-se a análise crítica de como a comercialização da íris humana, sob a ótica da proteção de dados, da ética digital e da justiça social, pode violar direitos fundamentais à privacidade, dignidade e não discriminação e quais os limites do consentimento no contexto de poder.

Nesta análise, cujo reside na urgência de compreender os riscos éticos e estruturais da coleta biométrica em um cenário de crescente desigualdade digital e social, pretende-se examinar os limites jurídicos do consentimento em contextos assimétricos, discutir a atuação da Autoridade Nacional de Proteção de Dados (ANPD) e do Poder Judiciário frente a essas práticas e refletir sobre os impactos sociais da transformação da íris em ativo comercial.

A metodologia utilizada será qualitativa e bibliográfica, com apoio doutrinário nacional e internacional, jurisprudencial e legislativo. Adota-se como referencial teórico a obra de Ulrich Beck e sua noção de sociedade de risco, na qual as incertezas tecnológicas criadas pelo progresso científico afetam de maneira desigual os segmentos sociais. Essa teoria se mostra especialmente adequada para compreender como a coleta de dados biométricos em comunidades vulneráveis amplia riscos sociais e institui novas formas de desigualdade. Ao tratar da íris como produto, esvazia-se seu significado humano e constitucional, ao mesmo tempo em que se naturaliza uma prática que, no limite, transforma o corpo em insumo comercial.

## A LEGISLAÇÃO APLICADA À COMERCIALIZAÇÃO DE DADOS BIOMÉTRICOS

A comercialização de dados biométricos, como a íris humana, encontra-se hoje em um cenário jurídico ambíguo no Brasil. Apesar da crescente valorização dessas informações sensíveis por parte do setor privado, a legislação nacional ainda não prevê, de forma expressa, a proibição da sua compra e venda, o que gera lacunas normativas e desafios à proteção dos direitos fundamentais dos titulares desses dados.

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), define em seu artigo 5º, inciso II, que dados biométricos são considerados dados pessoais sensíveis, e, portanto, devem receber tratamento diferenciado e reforçado em termos de proteção. Já o artigo 11 da mesma lei estabelece que o tratamento desses dados só pode ocorrer mediante consentimento específico e destacado do titular, ou em hipóteses excepcionais como cumprimento de obrigação legal, políticas públicas, proteção da vida, tutela da saúde, entre outras.

Contudo, a LGPD não veda a comercialização de dados sensíveis e sim, apenas exige o consentimento, o que abre margem para práticas abusivas, especialmente quando o consentimento é obtido mediante estímulo financeiro em contextos de vulnerabilidade socioeconômica. Um exemplo emblemático ocorreu em 2025, com a atuação da empresa Worldcoin, que escaneava a íris de cidadãos brasileiros mediante pagamento, principalmente em comunidades periféricas, gerando ampla repercussão e a suspensão temporária da atividade pela atuação conjunta da ANPD e do governo federal.

Diante a esta realidade, foi apresentado o Projeto de Lei nº 36/2025, que propõe alterar a LGPD para proibir expressamente a comercialização de dados biométricos sensíveis, ainda que haja consentimento do titular. O PL também propõe um regime mais

rigoroso de responsabilização civil e administrativa para empresas que violem o princípio da dignidade da pessoa humana ao transformar características físicas inalteráveis em mercadoria. Essa proposta busca alinhar o ordenamento brasileiro com a lógica de prevenção ao risco, conforme o princípio da precaução e a defesa da autodeterminação informativa.

Além da LGPD, a Constituição Federal de 1988, em seu artigo 5º, incisos X e XII, protege a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação. Tais garantias reforçam o entendimento de que o corpo humano e seus dados não devem ser objeto de exploração comercial sem limites.

Também merece destaque o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece como princípios fundamentais do uso da internet no Brasil a proteção da privacidade e dos dados pessoais (art. 3º, incisos II e III), além da responsabilização de agentes por danos decorrentes de conteúdo ou coleta indevida de dados. Ainda que voltado principalmente ao ambiente digital, seus dispositivos são aplicáveis à circulação online de dados biométricos.

Por fim, cabe à Autoridade Nacional de Proteção de Dados (ANPD) o papel de órgão regulador e fiscalizador dessas práticas. Criada pela própria LGPD, a ANPD possui competência para editar normas, aplicar sanções administrativas e orientar o tratamento de dados sensíveis. No entanto, seu funcionamento ainda é limitado por restrições orçamentárias e estruturais, dificultando uma atuação proativa frente ao avanço de tecnologias que exploram a biometria como ativo econômico.

## A ÉTICA E OS RISCOS E VULNERABILIDADE DAS VÍTIMAS DA COMERCIALIZAÇÃO DE DADOS BIOMÉTRICOS

A comercialização de dados biométricos, como a íris humana, levanta uma série de dilemas éticos que transcendem a legalidade formal do consentimento. Embora o titular possa autorizar o uso de seus dados, a validade ética desse consentimento deve ser analisada à luz das condições reais em que ele é obtido, especialmente quando envolvem recompensas financeiras direcionadas a pessoas em situação de vulnerabilidade social.

Nesse contexto, a prática de escanear a íris de indivíduos em troca de pagamentos, como ocorreu no caso da Worldcoin, revela uma assimetria de poder entre empresas

detentoras da tecnologia e cidadãos que, por necessidade econômica, são levados a negociar partes inalienáveis de sua identidade. O que se apresenta como uma “escolha voluntária” pode, na prática, configurar uma forma de exploração consentida, o que afronta os princípios da dignidade da pessoa humana e da autodeterminação informativa.

A esse respeito, a teoria da Sociedade de Risco, proposta por Ulrich Beck, é especialmente útil. Segundo o autor, os avanços tecnológicos da modernidade geram novos tipos de riscos globais que fogem ao controle do indivíduo e das instituições tradicionais. A coleta massiva e o uso imprevisível de dados biométricos constituem um desses riscos, pois, uma vez que a informação é vazada ou utilizada de maneira indevida, o dano é irreversível. Diferente de uma senha, a íris não pode ser substituída ou “atualizada”.

Além disso, Beck alerta para o fenômeno da individualização do risco, em que os efeitos sistêmicos de decisões tecnológicas são atribuídos à responsabilidade pessoal da vítima. Isso se manifesta quando se culpabiliza o indivíduo por ter “aceitado” ceder seus dados, mesmo que esse consentimento tenha sido condicionado por uma situação de necessidade.

A ética digital, nesse cenário, demanda mais do que o cumprimento formal da legislação. É necessário que haja responsabilidade institucional, tanto por parte das empresas quanto do Estado, para garantir que decisões tomadas em contextos de desigualdade não resultem em violações permanentes aos direitos fundamentais.

A vulnerabilidade socioeconômica também precisa ser vista como um elemento central na avaliação ética da comercialização de dados. Em muitos casos, populações de baixa renda, com menor acesso à educação digital, acabam sendo alvo preferencial de programas que oferecem incentivos financeiros em troca de dados biométricos, o que fere os princípios da justiça distributiva e da equidade.

Portanto, a análise jurídica deve ser complementada por uma abordagem ético-social que reconheça as estruturas de poder, o contexto da escolha e as consequências de longo prazo para a dignidade, privacidade e liberdade dos indivíduos envolvidos. A ausência dessa visão pode naturalizar práticas abusivas e normalizar a mercantilização de partes essenciais da identidade humana.

## CONCLUSÃO PARCIAL



A comercialização da íris humana, apesar de ser uma inovação tecnológica com promessas de segurança e eficiência, revela um conjunto de riscos éticos, jurídicos e sociais que ainda não foram adequadamente enfrentados pelo ordenamento brasileiro. A ausência de uma vedação legal expressa, aliada à possibilidade de consentimento em contextos de vulnerabilidade, permite que práticas potencialmente abusivas sejam naturalizadas no discurso da modernização digital.

No plano individual, os riscos incluem o uso indevido por terceiros para fins de fraude, falsificação de identidade, invasão de sistemas de segurança e manipulação comportamental. Ao contrário de outros dados pessoais, os biométricos não podem ser trocados ou apagados, o que expõe permanentemente os titulares a possíveis violações. Uma vez que a íris é escaneada e armazenada, o indivíduo não tem meios eficazes de se proteger caso ocorra vazamento, tornando-se alvo constante de crimes cibernéticos.

Do ponto de vista social, o uso comercial de dados biométricos amplia a desigualdade e fragiliza grupos vulneráveis. Empresas têm atuado de forma agressiva em comunidades de baixa renda, oferecendo recompensas financeiras para coleta de íris. Tal prática, embora voluntária, levanta dúvidas éticas sobre o consentimento em contextos de vulnerabilidade socioeconômica, pois transforma a biometria em moeda de troca entre liberdade e necessidade.

No âmbito jurídico, a ausência de normas específicas que proíbam a comercialização cria brechas legais e incertezas quanto à responsabilização civil e administrativa em caso de incidentes. A LGPD exige o consentimento explícito, mas não impede que empresas lucrem com os dados desde que esse consentimento seja obtido – o que, muitas vezes, ocorre de forma obscura, sem a devida clareza para o titular. A consequência disso é a banalização do consentimento e a ineficácia da proteção jurídica.

O uso da biometria como moeda de troca expõe os titulares a danos praticamente irreversíveis, uma vez que características como a íris são únicas e imutáveis. Diferente de senhas, não podem ser modificadas em caso de vazamento, o que transforma qualquer uso indevido em um risco permanente à privacidade e à integridade da pessoa.

Tais práticas, ainda que travestidas de voluntárias, inserem-se em uma lógica de exploração consentida, especialmente quando direcionadas a populações economicamente fragilizadas. A troca de dados sensíveis por dinheiro ou benefícios reflete não liberdade de escolha, mas sim uma forma de vulnerabilidade estrutural explorada por interesses comerciais.

Nesse cenário, torna-se evidente que a proteção dos dados biométricos não pode depender exclusivamente do consentimento do titular. A dignidade da pessoa humana, enquanto fundamento do Estado Democrático de Direito, exige que o corpo, e suas informações que reforçam a individualidade, únicas e inerentes a identidade, não sejam reduzidos a mercadoria. A regulação específica, portanto, é medida urgente e indispensável.

A responsabilização ética, legal e institucional pelas consequências da comercialização da íris deve ir além da reparação individual, alcançando também a prevenção coletiva dos danos. É papel do Estado e da sociedade civil garantir que os avanços tecnológicos respeitem os limites impostos pelos direitos fundamentais e pela justiça social, para que não perpetuem formas disfarçadas de desigualdade e exploração.

## REFERÊNCIAS

AGAMBEN, Giorgio. *O que é o contemporâneo?* Chapecó: Argos, 2009.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. *Guia orientativo sobre tratamento de dados pessoais sensíveis*. Brasília: ANPD, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-tratamento-dados-pessoais-sensiveis.pdf>. Acesso em: jul. 2025.

BECK, Ulrich. *Sociedade de risco: rumo a uma outra modernidade*. 2. ed. São Paulo: Editora 34, 2011.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Dialética, 2018.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Senado Federal, 1988. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: jul. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. *Diário Oficial da União: seção 1*, Brasília, DF, 24 abr. 2014. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm). Acesso em: jul. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD): dispõe sobre o tratamento de dados pessoais*. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: jul. 2025.

BRASIL. Projeto de Lei nº 36, de 2025. *Altera a LGPD para proibir a comercialização de dados biométricos sensíveis*. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2409607>. Acesso em: jul. 2025.

BRASIL. Superior Tribunal de Justiça. *REsp 1.308.830/SP – Recurso Especial – Direito à Imagem – Dano Moral – Prova – Quantum Indenizatório – Revisão – Possibilidade*. Brasília, DF: STJ, 2013. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=1308830>. Acesso em: jul. 2025.

BRASIL. Superior Tribunal de Justiça. *REsp 1.767.592/SP*. Julgamento: 2019.

BRASIL. Tribunal de Justiça de São Paulo. *Apelação Cível nº 100XXXX-89.2023.8.26.0100*. Julgamento: 2023.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

G1. Empresa continua a pagar para escanear íris em SP; parte do olho é ferramenta mais precisa que impressão digital. *G1*, São Paulo, 28 jan. 2025. Disponível em: <https://g1.globo.com/jornal-nacional/noticia/2025/01/28/empresa-continua-a-pagar-para-escanear-iris-em-sp.ghtml>. Acesso em: jul. 2025.

G1. Pagamento por foto da íris atraiu meio milhão de brasileiros com foco na periferia de SP até ser barrado pelo governo. *G1*, São Paulo, 25 jan. 2025. Disponível em: <https://g1.globo.com/tecnologia/noticia/2025/01/25/pagamento-por-foto-da-iris-atraiu-meio-milhao-de-brasileiros.ghtml>. Acesso em: jul. 2025.

UNESCO. *Declaração Universal sobre Bioética e Direitos Humanos*. Paris: Organização das Nações Unidas para a Educação, a Ciência e a Cultura, 2005. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000146180>. Acesso em: jul. 2025.