

**VI CONGRESSO INTERNACIONAL DE
DIREITO E INTELIGÊNCIA
ARTIFICIAL (VI CIDIA)**

REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL II

R344

Regulação da inteligência artificial II [Recurso eletrônico on-line] organização VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: Danúbia Patrícia de Paiva, David França Carvalho e Renata Kretzmann – Belo Horizonte: Skema Business School, 2025.

Inclui bibliografia

ISBN: 978-65-5274-354-1

Modo de acesso: www.conpedi.org.br em publicações

Tema: Perspectivas globais para a regulação da inteligência artificial.

1. Compliance. 2. Ética. 3. Legislação. I. VI Congresso Internacional de Direito e Inteligência Artificial (1:2025 : Belo Horizonte, MG).

CDU: 34

skema
BUSINESS SCHOOL

LAW SCHOOL
FOR BUSINESS

VI CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (VI CIDIA)

REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL II

Apresentação

A SKEMA Business School é uma organização francesa sem fins lucrativos, com presença em sete países diferentes ao redor do mundo (França, EUA, China, Brasil, Emirados Árabes Unidos, África do Sul e Canadá) e detentora de três prestigiadas creditações internacionais (AMBA, EQUIS e AACSB), refletindo seu compromisso com a pesquisa de alta qualidade na economia do conhecimento. A SKEMA reconhece que, em um mundo cada vez mais digital, é essencial adotar uma abordagem transdisciplinar.

Cumprindo esse propósito, o VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA), realizado nos dias 18 e 19 de setembro de 2025, em formato híbrido, manteve-se como o principal evento acadêmico sediado no Brasil com o propósito de fomentar ricas discussões sobre as diversas interseções entre o direito e a inteligência artificial. O evento, que teve como tema central a "Regulação da Inteligência Artificial", contou com a presença de renomados especialistas nacionais e internacionais, que abordaram temas de relevância crescente no cenário jurídico contemporâneo.

Profissionais e estudantes dos cursos de Direito, Administração, Economia, Ciência de Dados, Ciência da Computação, entre outros, tiveram a oportunidade de se conectar e compartilhar conhecimentos, promovendo um ambiente de rica troca intelectual. O VI CIDIA contou com a participação de acadêmicos e profissionais provenientes de diversas regiões do Brasil e do exterior. Entre os estados brasileiros representados, estavam: Alagoas (AL), Bahia (BA), Ceará (CE), Goiás (GO), Maranhão (MA), Mato Grosso do Sul (MS), Minas Gerais (MG), Pará (PA), Paraíba (PB), Paraná (PR), Pernambuco (PE), Piauí (PI), Rio de Janeiro

Foram discutidos assuntos variados, desde a própria regulação da inteligência artificial, eixo central do evento, até as novas perspectivas de negócios e inovação, destacando como os algoritmos estão remodelando setores tradicionais e impulsionando a criação de empresas inovadoras. Com uma programação abrangente, o congresso proporcionou um espaço vital para discutir os desafios e oportunidades que emergem com o desenvolvimento algorítmico, reforçando a importância de uma abordagem jurídica e ética robusta nesse contexto em constante evolução.

A programação teve início às 13h, com o check-in dos participantes e o aquecimento do público presente. Às 13h30, a abertura oficial foi conduzida pela Prof.^a Dr.^a Geneviève Poulingue, que, em sua fala de boas-vindas, destacou a relevância do congresso para a agenda global de inovação e o papel da SKEMA Brasil como ponte entre a academia e o setor produtivo.

Em seguida, às 14h, ocorreu um dos momentos mais aguardados: a Keynote Lecture do Prof. Dr. Ryan Calo, renomado especialista internacional em direito e tecnologia e professor da University of Washington. Em uma conferência instigante, o professor explorou os desafios metodológicos da regulação da inteligência artificial, trazendo exemplos de sua atuação junto ao Senado dos Estados Unidos e ao Bundestag alemão.

A palestra foi seguida por uma sessão de comentários e análise crítica conduzida pelo Prof. Dr. José Luiz de Moura Faleiros Júnior, que contextualizou as reflexões de Calo para a realidade brasileira e fomentou o debate com o público. O primeiro dia foi encerrado às 14h50 com as considerações finais, deixando os participantes inspirados para as discussões do dia seguinte.

As atividades do segundo dia tiveram início cedo, com o check-in às 7h30. Às 8h20, a Prof.^a Dr.^a Margherita Pagani abriu a programação matinal com a conferência Unlocking Business

Após um breve e merecido coffee break às 9h40, os participantes retornaram para uma manhã de intensas reflexões. Às 10h30, o pesquisador Prof. Dr. Steve Ataky apresentou a conferência Regulatory Perspectives on AI, compartilhando avanços e desafios no campo da regulação técnica e ética da inteligência artificial a partir de uma perspectiva global.

Encerrando o ciclo de palestras, às 11h10, o Prof. Dr. Filipe Medon trouxe ao público uma análise profunda sobre o cenário brasileiro, com a palestra AI Regulation in Brazil. Sua exposição percorreu desde a criação do Marco Legal da Inteligência Artificial até os desafios atuais para sua implementação, envolvendo aspectos legislativos, econômicos e sociais.

Nas tardes dos dois dias, foram realizados grupos de trabalho que contaram com a apresentação de cerca de 60 trabalhos acadêmicos relacionados à temática do evento. Com isso, o evento foi encerrado, após intensas discussões e troca de ideias que estabeleceram um panorama abrangente das tendências e desafios da inteligência artificial em nível global.

Os GTs tiveram os seguintes eixos de discussão, sob coordenação de renomados especialistas nos respectivos campos de pesquisa:

a) Startups e Empreendedorismo de Base Tecnológica – Coordenado por Allan Fuezi de Moura Barbosa, Laurence Duarte Araújo Pereira, Cildo Giolo Júnior, Maria Cláudia Viana Hissa Dias do Vale Gangana e Yago Oliveira

b) Jurimetria Cibernética Jurídica e Ciência de Dados – Coordenado por Arthur Salles de Paula Moreira, Gabriel Ribeiro de Lima, Isabela Campos Vidigal Martins, João Victor Doreto e Tales Calaza

c) Decisões Automatizadas e Gestão Empresarial / Algoritmos, Modelos de Linguagem e Propriedade Intelectual – Coordenado por Alisson Jose Maia Melo, Guilherme Mucelin e

f) Regulação da Inteligência Artificial – III – Coordenado por Ana Júlia Silva Alves Guimarães, Erick Hitoshi Guimarães Makiya, Jessica Fernandes Rocha, João Alexandre Silva Alves Guimarães e Luiz Felipe Vieira de Siqueira

g) Inteligência Artificial, Mercados Globais e Contratos – Coordenado por Gustavo da Silva Melo, Rodrigo Gugliara e Vitor Ottoboni Pavan

h) Privacidade, Proteção de Dados Pessoais e Negócios Inovadores – I – Coordenado por Dineia Anziliero Dal Pizzol, Evaldo Osorio Hackmann, Gabriel Fraga Hamester, Guilherme Mucelin e Guilherme Spillari Costa

i) Privacidade, Proteção de Dados Pessoais e Negócios Inovadores – II – Coordenado por Alexandre Schmitt da Silva Mello, Lorenzo Antonini Itabaiana, Marcelo Fonseca Santos, Mariana de Moraes Palmeira e Pietra Daneluzzi Quinelato

j) Empresa, Tecnologia e Sustentabilidade – Coordenado por Marcia Andrea Bühring, Ana Cláudia Redecker, Jessica Mello Tahim e Maraluce Maria Custódio.

Cada GT proporcionou um espaço de diálogo e troca de experiências entre pesquisadores e profissionais, contribuindo para o avanço das discussões sobre a aplicação da inteligência artificial no direito e em outros campos relacionados.

Um sucesso desse porte não seria possível sem o apoio institucional do Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, que desde a primeira edição do evento provê uma parceria sólida e indispensável ao seu sucesso. A colaboração contínua do CONPEDI tem sido fundamental para a organização e realização deste congresso, assegurando a qualidade e a relevância dos debates promovidos.

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Ms. Dorival Guimarães Pereira Júnior

Coordenador do Curso de Direito – SKEMA Law School

Prof. Dr. José Luiz de Moura Faleiros Júnior

Coordenador de Pesquisa – SKEMA Law School

**RECONHECIMENTO FACIAL E VIGILÂNCIA EM ESTÁDIOS COM
INTELIGÊNCIA ARTIFICIAL: LIMITES À PRIVACIDADE NA PERSPECTIVA
DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

**FACIAL RECOGNITION AND SURVEILLANCE IN STADIUMS WITH
ARTIFICIAL INTELLIGENCE: LIMITS TO PRIVACY FROM THE
PERSPECTIVE OF THE GENERAL PERSONAL DATA PROTECTION LAW**

**Ruan Hagno de Assis Moura
Mateus Arruda do Nascimento
Fabrício Germano Alves**

Resumo

O uso de reconhecimento facial com inteligência artificial em estádios visa aumentar a segurança, mas gera problemas com a privacidade e a Lei Geral de Proteção de Dados Pessoais (LGPD). A pesquisa analisa se essa tecnologia se alinha com as leis brasileiras, considerando as tensões entre segurança pública e privacidade. A coleta de dados biométricos sem consentimento adequado ameaça a dignidade. A tecnologia precisaria de regulamentos rigorosos para garantir que a segurança não infrinja direitos individuais. O estudo questiona se a vigilância em massa é proporcional e necessária. Questiona se a vigilância em massa, que trata dados biométricos sensíveis (LGPD, Art. 5º, II), pode ser considerada proporcional e necessária.

Palavras-chave: Direitos fundamentais, Dados pessoais, Inteligência artificial, Reconhecimento facial

Abstract/Resumen/Résumé

The use of artificial intelligence-based facial recognition in stadiums aims to increase security, but it raises privacy concerns and raises concerns regarding the General Data Protection Law (LGPD). The study analyzes whether this technology aligns with Brazilian law, considering the tensions between public safety and privacy. Collecting biometric data without proper consent threatens dignity. The technology would require strict regulations to

1 INTRODUÇÃO

O avanço da tecnologia digital, sobretudo das ferramentas de inteligência artificial, tem transformado profundamente as formas de controle e vigilância em espaços públicos. Um dos campos mais impactados por essa nova lógica é o dos eventos esportivos, especialmente os realizados em estádios de futebol, onde grandes aglomerações e a diversidade dos públicos sempre representaram um desafio para a segurança e a organização.

A implementação de câmeras com sistemas de reconhecimento facial, muitas vezes integrados a bancos de dados de procurados ou torcedores punidos, onde sofreram alguma sanção desportiva, onde tem sido apresentada como solução eficiente para coibir a violência, impedir o acesso de pessoas indesejadas e até mesmo prevenir a atuação de cambistas. Tal tecnologia também visa a velocidade na entrada de torcedores nos estádios, além da agilidade, o reconhecimento facial tem como objetivo reforçar a segurança. No entanto, essa prática vem sendo adotada de forma precipitada, muitas vezes sem o devido debate público ou regulamentação jurídica específica, o que levanta uma série de questionamentos sobre sua legalidade, especialmente a compatibilidade com os direitos fundamentais de ir e vir em ambientes públicos e o direito de lazer.

A coleta e o tratamento de dados biométricos em larga escala – como os realizados por meio do reconhecimento facial – não são operações neutras ou livres de impactos sociais e jurídicos. Trata-se, na verdade, de um processo profundamente invasivo que pode comprometer princípios fundamentais como a autodeterminação informacional, a privacidade e a liberdade de locomoção (LGPD, Art. 2º; CF/88, Art. 5º, X; CF/88, Art. 5º, XV).

Embora se reconheça a importância de medidas de segurança em ambientes de grande circulação, como os estádios, é preciso que tais medidas estejam ancoradas em fundamentos legais claros, observem os princípios da proporcionalidade e da necessidade que estão previstos na Constituição Federal em seu artigo 5º e também no artigo 6º, § 1º, da LGPD, e garantam ao cidadão meios eficazes de controle sobre seus próprios dados.

A premissa de que o avanço tecnológico pode justificar a restrição de liberdades civis tem sido criticada por diversos juristas, como Bruno Ricardo Barreto e Danilo Doneda. Tais autores alertam para os riscos de uma interpretação constitucional funcionalista e utilitária, que ignora os limites impostos pela dignidade da pessoa humana e pela necessidade de contenção do poder, inclusive o tecnológico. A hermenêutica constitucional, nesse sentido, deve ser orientada pela

proteção efetiva dos direitos fundamentais e não por interesses circunstanciais de eficiência ou controle social. O reconhecimento facial, enquanto tecnologia de vigilância, precisa ser submetido a critérios rigorosos de legalidade, transparência, responsabilidade e reversibilidade, sob pena de se tornar um instrumento de opressão silenciosa e permanente.

A problemática se agrava quando se considera que o ambiente dos estádios é, historicamente, um espaço de convivência popular, plural e democrático. Transformar esses espaços em zonas de exceção tecnológica, em que todos os presentes estão sujeitos à vigilância biométrica permanente, sem o devido controle legal e social, equivale a reduzir o público a objetos de rastreamento. A segurança, em tais contextos, não pode ser vista como justificativa absoluta que permite a suspensão de garantias legais. Conforme observa-se, os direitos fundamentais somente têm valor real quando se estruturam mecanismos de proteção capazes de resistir aos impulsos autoritários e aos discursos de emergência.

Dessarte, é necessário destacar os grandes riscos de privacidade e discriminação com a criação de enormes bancos de dados biométricos, que são classificados como sensíveis pela Lei Geral de Proteção de Dados Pessoais (LGPD) no seu artigo 5º Inciso II, representa um alvo valioso para ataques cibernéticos, dessa forma ocasionando uma vulnerabilidade dos dados e riscos de segurança cibernética. Assim, um vazamento desses dados teria enormes consequências para a parcela afetada, podendo trazer impactos permanentes na vida desses torcedores que à primeira vista iriam usufruir de lazer e diversão.

Ademais, o uso do reconhecimento facial para fins como a identificação de cambistas, embora revestido de uma pretensa legitimidade, pode ser excessivamente invasivo. A figura do cambista, frequentemente associada à informalidade e à criminalização seletiva, não pode servir como pretexto para a adoção de práticas que violam garantias constitucionais. O combate à revenda de ingressos deve ser realizado por meios proporcionais, como o uso de bilhetes digitais com rastreabilidade, auditorias nos canais oficiais de venda e campanhas educativas, e não pela coleta massiva de dados biométricos dos espectadores. O princípio da proporcionalidade, consagrado no direito constitucional, Artigo 5º, Constituição Federal de 1988, que trata dos direitos e garantias fundamentais, e na jurisprudência dos tribunais superiores, exige que as

medidas restritivas de direitos sejam adequadas, necessárias e equilibradas em relação ao fim que se pretende alcançar.

Ao se examinar o uso do reconhecimento facial nos estádios sob a ótica da LGPD, constata-se que a ausência de consentimento específico e informado dos titulares dos dados, a falta de transparência quanto às bases de dados utilizadas e a inexistência de mecanismos claros de contestação ou correção tornam essas práticas juridicamente frágeis. Entende-se que a validade de qualquer medida restritiva de direitos deve derivar de uma norma jurídica devidamente constituída, dentro do sistema normativo vigente. A ausência de uma legislação específica que regule o uso dessa tecnologia em ambientes esportivos, aliada à omissão de parâmetros técnicos pela Autoridade Nacional de Proteção de Dados (ANPD), compromete não apenas a legalidade da prática, mas também sua legitimidade democrática.

Por outro lado, a doutrina especializada em proteção de dados tem enfatizado que a coleta e o tratamento de dados sensíveis devem obedecer a um regime jurídico mais rigoroso. Argumenta-se que a proteção de dados não deve ser vista como um entrave à inovação, mas como um parâmetro ético e jurídico que permite a incorporação segura e legítima da tecnologia na vida social. A conformidade com a LGPD é, portanto, condição necessária para que o uso do reconhecimento facial não infrinja direitos fundamentais. Isso implica a realização de relatórios de impacto à proteção de dados, a adoção de medidas de mitigação de riscos, a prestação de contas e a disponibilização de canais eficazes para que os titulares possam exercer seus direitos.

Importante também observar que, em contextos de grande vulnerabilidade social e desigualdade estrutural, como os que marcam o acesso ao lazer e ao esporte no Brasil, a vigilância algorítmica tende a recair com mais intensidade sobre determinados grupos sociais. Torcedores organizados, moradores das periferias urbanas e frequentadores assíduos das arquibancadas populares acabam sendo os principais alvos dos sistemas de monitoramento, reproduzindo um padrão de criminalização seletiva que já é conhecido em outras áreas da política de segurança pública. É possível advertir que, a tecnologia, quando desprovida de controle crítico, tende a reforçar preconceitos e assimetrias, transformando-se em ferramenta de exclusão e silenciamento.

Em vista disso, torna-se imprescindível que o debate sobre reconhecimento facial em estádios seja conduzido com seriedade, transparência e respeito aos princípios constitucionais. Não se trata de rejeitar a tecnologia em si, mas de estabelecer parâmetros normativos e institucionais que garantam sua compatibilidade com os direitos fundamentais. A liberdade de ir e vir, a privacidade, a igualdade e a presunção de inocência A liberdade de ir e vir, a privacidade, a igualdade e a presunção de inocência são garantias constitucionais expressamente previstas no artigo 5º da Constituição Federal de 1988, sendo invioláveis e de observância obrigatória por qualquer medida estatal ou privada que pretenda restringir direitos individuais. O direito à locomoção está previsto no inciso XV, a inviolabilidade da vida privada no inciso X, a igualdade no caput do artigo, e a presunção de inocência no inciso LVII da referida norma (BRASIL, 2024). não podem ser relativizadas em nome de uma segurança que, muitas vezes, é apenas simbólica. Assim, a efetividade dos direitos não decorre apenas de sua previsão formal, mas de sua proteção prática contra abusos e retrocessos.

Essa reflexão inicial conduz à necessidade de uma análise mais aprofundada sobre os limites legais e constitucionais da vigilância tecnológica em ambientes esportivos. O reconhecimento facial, por sua natureza invasiva, deve ser objeto de regulação estrita e de controle social amplo, sob pena de consolidar um estado de vigilância permanente que subverte os princípios basilares da democracia...

2 RECONHECIMENTO FACIAL E PROTEÇÃO DE DADOS PESSOAIS

A tecnologia de reconhecimento facial parte da extração de padrões biométricos únicos, como a distância entre os olhos e o formato do maxilar. Esses traços são processados por algoritmos treinados com base em grandes conjuntos de dados e servem para identificar ou verificar indivíduos. Apesar do discurso de neutralidade técnica, tais sistemas refletem escolhas humanas codificadas — os dados utilizados, os objetivos programados e os critérios de decisão não são neutros, mas carregam vieses econômicos, sociais e culturais (Doneda, 2021).

Do ponto de vista jurídico, a Lei nº 13.709/2018 — a Lei Geral de Proteção de Dados Pessoais (LGPD) — classifica os dados biométricos como sensíveis em seu artigo 5º, Inciso II, exigindo um regime mais rigoroso para seu tratamento. O artigo 11 da LGPD limita esse

tratamento a hipóteses excepcionais, como o consentimento do titular ou a proteção da vida e da incolumidade física. Além disso, os artigos 6º e 37 estabelecem princípios que devem nortear toda atividade de tratamento de dados: finalidade, adequação, necessidade, livre acesso, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Aplicar sistemas de reconhecimento facial em estádios sem que os titulares sejam previamente informados sobre as finalidades e os riscos envolvidos constitui violação à legislação. como o princípio da transparência no artigo 6º, VI da LGPD A ausência de transparência, canais de acesso e mecanismos para correção ou exclusão de dados compromete o exercício pleno da autodeterminação informacional. Trata-se de um direito fundamental previsto no artigo 2º, Inciso II da LGPD, que garante ao indivíduo o controle sobre seus próprios dados e sua visibilidade no espaço público (Doneda, 2021).

A coleta indiscriminada de dados biométricos em grandes eventos esportivos, sob pretexto de segurança, desconsidera o princípio da necessidade, previsto no artigo 6º, inciso III da LGPD, que exige a minimização da coleta de dados ao estritamente necessário — e o da finalidade específica — que exige clareza no propósito do tratamento. Quando não respeitados, esses princípios esvaziam as garantias normativas da LGPD e abrem margem para abusos sistêmicos. Em tais casos, a vigilância tecnológica ultrapassa o campo da legalidade e entra na zona do arbítrio.

Para além da análise da validade formal, a LGPD que permite o reconhecimento facial em estádios deve ser avaliada em outras duas dimensões. Primeiro, sob o critério da justiça, onde uma norma pode ser válida sem ser justa, onde apesar da teoria ser benéfica é possível questionar em relação a dignidade da pessoa humana e a presunção de inocência que transcendem a mera legalidade, tendo em vista que tais princípios são pilares da Constituição, por isso estão acima de qualquer lei comum. Por outro lado, é válido analisar se de fato a norma é eficaz, e a segurança não pode justificar a adoção de quaisquer meios. O uso de uma tecnologia, por mais eficaz que seja, deve ser sempre balizado pelos direitos fundamentais e princípios como a dignidade humana e a presunção de inocência, que servem como limites ao poder do Estado, pois uma norma pode ser válida sem ser eficaz (Bobbio, 2001).

Portanto, é imprescindível que qualquer projeto de implantação dessa natureza seja precedido de uma análise crítica dos fundamentos legais. O uso de dados sensíveis, em especial em espaços públicos, exige transparência radical, salvaguardas técnicas, consentimento informado sempre que possível e mecanismos efetivos de controle social e jurídico.

Outro ponto relevante é que a legislação de proteção de dados, tanto no Brasil quanto em outros países, tem evoluído no sentido de exigir a responsabilidade ativa dos controladores(GPDR, 2016). Isso significa que não basta declarar conformidade; é preciso demonstrar com transparência, que medidas técnicas e organizacionais foram efetivamente implementadas. Essa lógica busca assegurar que os indivíduos mantenham controle sobre seus próprios dados, especialmente em situações de coleta massiva, como ocorre nos estádios. Sem tais garantias, a tecnologia deixa de ser instrumento de segurança para se tornar uma ameaça permanente à autonomia informacional (DONEDA, 2021).

Ao mesmo tempo, é importante compreender que a existência de normas jurídicas não basta para garantir a proteção dos cidadãos. Os direitos precisam ser acompanhados de mecanismos práticos que os tornem efetivos, de modo que a promessa de proteção não se limite ao plano teórico(BOBBIO, 2004). Quando o reconhecimento facial é aplicado sem considerar esses limites, a consequência é um esvaziamento dos próprios fundamentos da democracia, pois se coloca em risco a dignidade individual e se normaliza uma lógica de vigilância contínua sobre a vida cotidiana(BARRETO, 2022).

3 CONSTITUCIONALIDADE, LEGALIDADE E DESPROPORCIONALIDADE DO USO EM ESTÁDIOS

O reconhecimento facial aplicado à segurança em estádios esbarra em importantes limitações constitucionais. O princípio da legalidade, previsto no artigo 5º, inciso II, da Constituição Federal de 1988, conforme a teoria normativa de Hans Kelsen (1998), exige que todo ato estatal, especialmente os que restringem direitos fundamentais, esteja fundado em norma válida e abstrata. A inexistência de lei específica autorizando o uso dessa tecnologia configura afronta direta a esse princípio, tornando a prática jurídica e politicamente questionável.

Ainda que promovido por entes privados, como clubes ou concessionárias, o uso de reconhecimento facial deve obedecer aos limites constitucionais, considerando que o tratamento de dados pessoais sensíveis incide em esfera protegida. A legalidade, nesse caso, não pode ser suprida por termos de uso genéricos ou por justificativas unilaterais de segurança pública. O uso dessa tecnologia sem respaldo legal aproxima-se de um modelo autoritário de gestão da ordem (Barreto, 2022).

Para além da legalidade, impõe-se a aplicação do princípio da proporcionalidade. Conforme estabelece Sarlet (2008), o exame de proporcionalidade se desdobra em três critérios: adequação (a medida deve ser apta a atingir o fim proposto), necessidade (não deve haver outro meio menos lesivo disponível) e proporcionalidade em sentido estrito (o benefício alcançado deve justificar o sacrifício imposto ao direito restringido).

Nesse contexto, o uso de reconhecimento facial para combater o cambismo revela-se desproporcional. A revenda irregular de ingressos é uma infração administrativa, previsto no artigo 42, da Lei nº 10.671/2003, que pode ser reprimida por meios menos invasivos, como controle digital de bilhetes, credenciamento reforçado ou uso de câmeras comuns. Submeter milhares de pessoas à vigilância biométrica por condutas de poucos é tratar o lazer e o consumo como atividades suspeitas por natureza.

A extrapolação do controle, sem base legal ou parâmetros objetivos, fere ainda o princípio da presunção de inocência. Quando todos os frequentadores são monitorados de forma invisível e contínua, inverte-se a lógica democrática: presume-se a culpabilidade e exige-se do cidadão que prove sua inocência perante uma estrutura algorítmica opaca e incontrolável. Trata-se, portanto, não de uma simples escolha técnica, mas de uma grave decisão política que afeta o núcleo duro dos direitos fundamentais.

O princípio da legalidade exige que qualquer medida restritiva de direitos encontre respaldo em norma clara e específica. A implantação de sistemas de reconhecimento facial sem esse fundamento normativo cria um descompasso no próprio ordenamento, uma vez que se introduzem restrições sem a devida legitimidade. Na prática, isso significa ampliar o poder de vigilância sem que haja mediação adequada por parte da lei, o que fragiliza o equilíbrio entre Estado e cidadão (KELSEN, 1998)

Além disso, a avaliação da proporcionalidade não pode se limitar a cálculos utilitaristas (STRECK, 2017). É necessário considerar que certos direitos possuem um núcleo essencial que não pode ser sacrificado em nome de uma suposta eficiência. Submeter milhares de pessoas a controles invasivos para combater práticas pontuais, como o cambismo, representa uma distorção dessa lógica. A medida, nesse contexto, revela-se não apenas desnecessária, mas também incompatível com a estrutura de proteção de direitos assegurada pela Constituição (SARLET, 2008).

4 VIGILÂNCIA, DISCRIMINAÇÃO E AUSÊNCIA DE REGULAMENTAÇÃO

Os riscos da vigilância algorítmica em estádios não são apenas abstratos, há evidências empíricas que apontam falhas sistemáticas na identificação de determinados grupos sociais. Estudos realizados nos Estados Unidos demonstraram que sistemas de reconhecimento facial têm maiores taxas de erro na identificação de pessoas negras, mulheres e jovens, o que levou diversas cidades a banirem completamente seu uso em espaços públicos. Esses vieses decorrem da base de dados e dos critérios de treinamento dos algoritmos, revelando uma reprodução técnica de desigualdades sociais (Streck, 2017).

No Brasil, onde a população dos estádios é majoritariamente composta por jovens negros e moradores de periferias, como se pode ver no perfil dos torcedores brasileiros levantado realizado pelo O Globo, a aplicação dessa tecnologia tende a reforçar seletividades já consolidadas no sistema penal. O risco de discriminação algorítmica é ampliado quando se considera a opacidade do processo: muitas vezes, os torcedores sequer sabem que estão sendo monitorados ou não têm acesso às imagens e decisões tomadas. Isso inviabiliza o exercício dos direitos previstos na LGPD, como o acesso, a correção, a portabilidade e a exclusão dos dados, que estão previstos no artigo 18 da Lei Geral de Proteção de Dados Pessoais.

Com o uso de tecnologias feitas por Inteligência Artificial pelos clubes que são detentores da gestão dos estádios, também é possível atrelar uma causa de aumento no valor dos ingressos, muitas vezes amplificando a exclusão de pessoas com baixa renda. Além disso, é possível notar uma relação quase direta com a classe afetada pelo uso do reconhecimento facial, onde em sua maioria causará impactos para população menos favorecida e com baixa

escolaridade, que não saberão entender de fato as consequências diretas dessa falta de proteção de dados.

Ademais, o país carece de uma regulamentação específica para o uso de reconhecimento facial em eventos esportivos. A LGPD fornece apenas diretrizes gerais, mas não detalha requisitos técnicos, critérios de proporcionalidade, protocolos de auditoria ou mecanismos de reparação. Essa lacuna normativa favorece o uso arbitrário da tecnologia, sem supervisão ou responsabilização efetiva. A Autoridade Nacional de Proteção de Dados (ANPD), nesse cenário, precisa exercer seu papel normativo com urgência, estabelecendo padrões claros e exigências mínimas de conformidade.

Não se trata de negar a utilidade potencial da tecnologia, mas de submetê-la a uma lógica de legalidade estrita e de confidencialidade para a parcela que frequenta os estádios. É possível compatibilizar segurança e direitos fundamentais como o direito à privacidade e a intimidade, o direito à liberdade de locomoção, direito a dignidade da pessoa humana também a presunção de inocência desde que se implementem salvaguardas robustas: consentimento informado, relatórios de impacto à proteção de dados, auditorias independentes com participação da sociedade civil, limitação do tempo de retenção de dados e responsabilização transparente dos controladores.

A ausência dessas garantias transforma o reconhecimento facial de uma ferramenta de segurança em um aparato de coerção simbólica. Mais do que controlar acessos, a tecnologia passa a controlar corpos, identidades e trajetórias especialmente daqueles grupos que historicamente ocupam a posição de “alvo preferencial” do poder punitivo. Sem um debate público qualificado e regulação firme, o que se instala é um modelo de segurança baseado no medo e na exceção, incompatível com o projeto constitucional de democracia substantiva.

A ausência de regulamentação específica sobre o uso do reconhecimento facial em estádios agrava sobremaneira os riscos já identificados. Sem critérios claros de funcionamento, fiscalização e reparação, os torcedores ficam expostos a falsos positivos, usos indevidos dos dados e práticas discriminatórias. Esse vazio normativo dificulta a efetivação dos direitos fundamentais e transfere aos cidadãos o peso de enfrentar um sistema pouco transparente e desproporcionalmente controlado (DONEDA, 2021).

Também não se pode ignorar que a experiência internacional mostra avanços no sentido de condicionar o uso da biometria a regras rígidas de proporcionalidade, transparência e controle social. Quando essas salvaguardas não existem, cria-se um ambiente de insegurança jurídica e social que favorece práticas abusivas. Em um país marcado por desigualdades, a tendência é que tais excessos recaiam principalmente sobre grupos já vulneráveis, transformando estádios em espaços de seletividade e exclusão, ao invés de locais de convivência democrática (BARRETO, 2022).

5 CONSIDERAÇÕES FINAIS

A utilização de sistemas de reconhecimento facial em estádios de futebol evidencia um novo paradigma na relação entre segurança pública e direitos fundamentais. A promessa de maior controle e prevenção de delitos não pode, no entanto, justificar práticas que comprometem garantias constitucionais essenciais, como a privacidade, a autodeterminação informacional e a liberdade de locomoção. A coleta de dados biométricos sensíveis em espaços públicos representa uma intervenção severa sobre esferas da vida privada dos indivíduos.

A ausência de consentimento específico dos titulares e a escassez de transparência quanto ao uso e ao destino dos dados reforçam a fragilidade jurídica dessas medidas. Em contextos como o dos eventos esportivos, onde há grande fluxo populacional e diversidade de perfis sociais, o monitoramento biométrico generalizado não atende ao critério de necessidade, tampouco respeita o princípio da finalidade. Ao não observar essas exigências, a vigilância tecnológica incorre em desvio de finalidade e afronta à legalidade.

A proporcionalidade entre a medida adotada e o objetivo pretendido também se mostra desequilibrada. O combate a infrações como a revenda de ingressos ou a presença de pessoas proibidas judicialmente nos estádios pode ser realizado por meios menos invasivos, como bilhetagem digital rastreável, cadastros preventivos e fiscalização convencional. Submeter milhares de torcedores a um monitoramento algorítmico permanente ultrapassa os limites do razoável, convertendo o ambiente esportivo em um espaço de suspeição coletiva.

Outro aspecto relevante é a seletividade estrutural observada na aplicação dessa tecnologia. Grupos historicamente marginalizados, como jovens negros, moradores de periferias e integrantes de torcidas organizadas, acabam sendo os principais alvos da vigilância. O viés discriminatório embutido nos sistemas de reconhecimento facial contribui para a reprodução de desigualdades sociais, reforçando uma lógica de criminalização que já permeia outras esferas da política de segurança pública no país.

A carência de regulamentação específica agrava ainda mais esse cenário. A inexistência de normas técnicas claras, critérios objetivos de operação, tempo de retenção de dados e mecanismos eficazes de contestação dificultam qualquer forma de controle social ou institucional. A lacuna normativa favorece a arbitrariedade e enfraquece a legitimidade de práticas que deveriam estar subordinadas aos marcos do Estado de Direito.

A responsabilidade pelo tratamento de dados em contextos de vigilância não é exclusiva do Estado. Entidades privadas, como clubes, empresas de tecnologia e concessionárias de estádios, ao operarem ou controlarem dados biométricos, assumem obrigações jurídicas relevantes. Essas organizações devem adotar medidas como relatórios de impacto à proteção de dados, nomeação de encarregados, definição de protocolos internos e criação de canais de atendimento aos titulares.

A percepção pública sobre os estádios também é impactada pela vigilância constante. Espaços tradicionalmente associados à convivência social, ao lazer e à expressão cultural passam a ser entendidos como ambientes de controle e restrição. Isso altera comportamentos, gera autocensura e desencoraja a participação democrática. A imposição de um olhar vigilante contínuo mina a confiança entre cidadãos e instituições e reduz o potencial emancipatório dos eventos coletivos.

Diante disso, o reconhecimento facial, aplicado à vigilância em estádios, exige uma abordagem legal e política responsável. A compatibilização entre segurança e liberdade não será alcançada por meio de medidas tecnológicas arbitrárias, mas sim por meio de políticas públicas orientadas por direitos fundamentais. Sem regulação rigorosa, fiscalização efetiva e participação social ativa, essa tecnologia tende a se consolidar como instrumento de exclusão e opressão, incompatível com os pilares democráticos e com a proteção constitucional da privacidade.

REFERÊNCIAS

BARRETO, Bruno Ricardo. **Reconhecimento Facial e o Direito à Privacidade**. Revista Brasileira de Direito Desportivo, v. 38, 2022.

BOBBIO, Norberto. **A Era dos Direitos**. Rio de Janeiro: Elsevier, 2004.

BOBBIO, Norberto. **Teoria da Norma Jurídica**. Bauru, SP: Edipro, 2001.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 2024.

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.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: elementos da formação da cidadania informacional**. Rio de Janeiro: Renovar, 2021.

GDPR – General Data Protection Regulation. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016. Disponível em: <https://gdpr-info.eu>. Acesso em: 24 jul. 2025.

JUSBRASIL. **Reconhecimento Facial, LGPD e Estádios**. Disponível em: <https://www.jusbrasil.com.br>. Acesso em: 24 jul. 2025.

KELSEN, Hans. **Teoria Pura do Direito**. 6. ed. São Paulo: Martins Fontes, 1998.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**. 11. ed. rev. atual. ampl. Porto Alegre: Livraria do Advogado, 2008.

STRECK, Lenio Luiz. **Jurisdição Constitucional e Hermenêutica: uma nova crítica ao ativismo judicial**. 4. ed. Rio de Janeiro: Forense, 2017.

