IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS V

VIVIANNE RIGOLDI

JÉSSICA FACHIN

ROSANE TERESINHA PORTO

Copyright © 2026 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU – São Paulo
Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:
Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão
Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais
Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte
Prof. Dr. Fernando Passos – UNIARA - São Paulo
Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná
Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia
Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal
Comunicação:
Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul
Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe
Relações Internacionais para o Continente Americano:
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão
Prof. Dr. Felipe Chiarello de Souza Pinto - UPM – São Paulo
Relações Internacionais para os demais Continentes:
Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará
Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul
Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI – Santa Catarina
Educação Jurídica
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR
Prof. Dr. Rubens Beçak - USP - SP
Profa. Dra. Livia Gaigher Bosio Campello – UFMS – MS
Eventos:
Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo
Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina
Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial
Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ
Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB
Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG
Prof. Dr. Rogério Borba - UNIFACVEST - SC

D598

Direito, governança e novas tecnologias V [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Vivianne Rigoldi; Jéssica Fachin; Rosane Teresinha Porto – Florianópolis: CONPEDI, 2026.

Inclui bibliografia
ISBN: 978-65-5274-589-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS V

Apresentação

O Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), referência na difusão de pesquisas que abordam os novos fenômenos envolvendo o Direito, firma-se como espaço qualificado para apresentação de pesquisas produzidas na área das novas tecnologias em face do Direito.

O tema, recorrente nos artigos apresentados - o uso da inteligência artificial no âmbito jurídico, demonstra que a maior sociedade científica na área jurídica do Brasil se mantém atenta às inovações tecnológicas, ao avanço de diversas tecnologias, novas experiências no judiciário e nos escritórios de advocacia. Artigos, de alta relevância acadêmica e científica, destacam que o Direito não está imune a essas transformações e reiteram a necessidade de atenção aos desafios regulatórios do uso da inteligência artificial no mundo jurídico.

Diferentes pesquisas, apresentadas no Grupo de Trabalho 'Direito, Governança e Novas Tecnologias V', alertam para os efeitos deletérios da opacidade algorítmica,

referindo-se à falta de transparência sobre como sistemas de inteligência artificial e seus algoritmos produzem decisões, dentro e fora do judiciário. Nos textos, a governança

digital é debatida, com rigorosa visão científica, objetivando garantir o uso estratégico de tecnologias de informação e comunicação para gerir serviços, promover a segurança

de dados e integrar processos, de forma transparente, eficiente, com foco na participação ativa do cidadão na tomada de decisões.

algorítmico e tecnológico do sistema de justiça, englobando a investigação de cibercrimes, a digitalização de procedimentos policiais e judiciais, provas digitais e a

regulação de plataformas para combater conteúdos ilícitos.

Destarte, os artigos apresentados e os debates produzidos no Grupo de Trabalho ‘Direito, Governança e Novas Tecnologias V’ são essenciais para o

fortalecimento das diretrizes nacionais de regulação das novas tecnologias, pela formação de parâmetros normativos e procedimentais adequados à proteção dos

direitos humanos e fundamentais, à garantia da segurança da informação, à gestão de riscos e ao fortalecimento da transparência e do alinhamento legal no uso das novas

tecnologias no âmbito jurídico.

Por essas razões, as coordenadoras do GT convidam para a leitura do teor integral dos artigos, agradecendo a participação dos autores pesquisadores desta edição.

Vivianne Rigoldi/Jéssica Fachin/Rosane Porto

RECONHECIMENTO FACIAL NOS ESTÁDIOS: VIGILÂNCIA TECNOLÓGICA, PROTEÇÃO DE DADOS E OS LIMITES DO DIREITO NA SOCIEDADE EM REDE.

FACIAL RECOGNITION IN STADIUMS: TECHNOLOGICAL SURVEILLANCE, DATA PROTECTION AND THE LIMITS OF LAW IN THE NETWORK SOCIETY

Gustavo André Espindola Palma [1]
Emerson Wendt [2]

Resumo

O artigo analisa a implementação da tecnologia de reconhecimento facial nos estádios brasileiros, com atenção especial aos casos da dupla Gre-Nal, a partir da tensão entre segurança, vigilância tecnológica e proteção de dados pessoais. O problema de pesquisa consiste em verificar em que medida o uso dessa tecnologia, ao envolver tratamento automatizado de dados biométricos sensíveis, mostra-se compatível com as garantias de transparência, revisão e controle previstas na Lei Geral de Proteção de Dados. O objetivo é examinar os limites jurídicos do reconhecimento facial em ambientes esportivos mediante a articulação entre o referencial da cibernética de Norbert Wiener e o debate sobre opacidade algorítmica, decisões automatizadas e governança de dados. Metodologicamente, a pesquisa adota abordagem qualitativa, com revisão bibliográfica e documental, mobilizando literatura jurídica e teórica, documentos normativos, políticas de privacidade e materiais jornalísticos relacionados à implementação do sistema em estádios. Conclui-se que o reconhecimento facial, embora apresentado como instrumento de segurança e eficiência, opera com déficit de transparência, dificuldade de revisão efetiva e potencial discriminatório, o que fragiliza sua legitimidade jurídica. Nessa perspectiva, a regulação do tratamento biométrico deve atuar como mecanismo de feedback negativo, impondo limites, auditabilidade e canais efetivos de contestação.

Palavras-chave: Cibernética, Lgpd, Proteção de dados pessoais, Reconhecimento facial, Vigilância tecnológica

Abstract/Resumen/Résumé

transparency, review and control provided for in the Brazilian General Data Protection Law. The objective is to examine the legal limits of facial recognition in sports environments through the articulation between Norbert Wiener's cybernetic framework and the debate on algorithmic opacity, automated decisions and data governance. Methodologically, the research adopts a qualitative approach, with bibliographic and documentary review, mobilizing legal and theoretical literature, normative documents, privacy policies and journalistic materials related to the implementation of the system in stadiums. It concludes that facial recognition, although presented as an instrument of security and efficiency, operates with a deficit of transparency, difficulty of effective review and discriminatory potential, which weakens its legal legitimacy. From this perspective, the regulation of biometric processing must act as a negative feedback mechanism, imposing limits, auditability and effective channels for contestation.

Keywords/Palabras-claves/Mots-clés: Cybernetics, Brazilian general data protection law, Personal data protection, Facial recognition, Technological surveillance

1 INTRODUÇÃO

Intensificada a partir de 2025, a tecnologia de reconhecimento facial tornou-se obrigatória nos estádios com capacidade superior a 20 mil pessoas, conforme previsão da Lei Geral do Esporte (Lei nº 14.597/2023), sancionada em junho de 2023. O Artigo 148 da referida lei estabelece requisitos específicos, como o monitoramento por imagem nas catracas, a identificação biométrica dos espectadores e a criação de uma central técnica de informações voltada a essa finalidade.

Tal medida pode ser analisada como uma resposta estatal às demandas por maior segurança em eventos esportivos de grande porte. Nesse cenário, o presente artigo tem como objeto de análise a implementação da tecnologia de reconhecimento facial nos estádios brasileiros, com especial atenção aos casos da dupla Gre-Nal, buscando compreender as tensões jurídicas e sociais que emergem entre as promessas de segurança e os riscos aos direitos fundamentais, especialmente à privacidade.

Para analisar esse fenômeno, adota-se a lente teórica da cibernética de Norbert Wiener (1970). Sob essa ótica, o estádio não é mais visto apenas como um local de lazer, mas um sistema de controle e comunicação desenhado para combater a "entropia" (a desordem natural das multidões) por meio da aplicação intensiva de "negentropia" (informação estruturada sob a forma da biometria facial).

O sistema busca transformar a incerteza da massa em dados identificáveis, operando como uma "Máquina de Governar" que substitui o julgamento humano por processos estatísticos. O foco central da análise reside, portanto, na incompatibilidade entre a implementação desses sistemas, que realizam tratamento automatizado de dados pessoais sensíveis e produzem decisões com impacto direto sobre os indivíduos, e a efetividade das garantias previstas na Lei Geral de Proteção de Dados.

Embora a LGPD estabeleça instrumentos como o direito à transparência e à revisão de decisões automatizadas, tais mecanismos mostram-se, na prática, limitados diante da opacidade dos sistemas algorítmicos, da dificuldade de acesso à informação pelos titulares e da atuação de entes privados sob a justificativa de segurança pública.

Como consequência, consolida-se um cenário em que decisões potencialmente falhas ou discriminatórias são tomadas sem adequada explicação, contestação ou correção, evidenciando uma fragilidade estrutural no controle jurídico dessas tecnologias.

Diante desse cenário, o problema de pesquisa consiste em verificar em que medida a implementação do reconhecimento facial nos estádios brasileiros, especialmente nos casos da

dupla Gre-Nal, é compatível com as garantias de transparência, revisão e controle previstas na Lei Geral de Proteção de Dados, considerando a opacidade dos sistemas algorítmicos e o tratamento de dados pessoais sensíveis sob a justificativa de segurança.

O artigo tem por objetivo analisar essas tensões jurídicas e sociais a partir da cibernética de Norbert Wiener (1970). Metodologicamente, adota-se abordagem qualitativa, com revisão bibliográfica e documental, articulando literatura jurídica e teórica, documentos normativos, políticas institucionais e materiais jornalísticos relacionados ao uso da biometria facial em estádios.

2 TECNOLOGIA DE RECONHECIMENTO FACIAL: POSSIBILIDADES E USOS A PARTIR DA INTELIGÊNCIA ARTIFICIAL

Ao analisar o dispositivo legal, observa-se que o art. 148 da LGE limita-se a estabelecer que o monitoramento recai sobre os espectadores e deve ser realizado por meio de imagens e identificação biométrica. Nesse contexto, dispõe a Lei nº 14.597/2023:

> Art. 148. O controle e a fiscalização do acesso do público a arena esportiva com capacidade para mais de 20.000 (vinte mil) pessoas deverão contar **com meio de monitoramento por imagem das catracas e com identificação biométrica dos espectadores** (Brasil, 2023, art. 148, grifo nosso).

Para compreender a tecnologia, o estudo preliminar da Autoridade Nacional de Proteção de Dados (ANPD) define que o reconhecimento facial é uma tecnologia que analisa, por métodos matemáticos e estatísticos, as características fisiológicas do rosto de um indivíduo. Nesse sentido:

> A biometria é a análise técnica, realizada por meios matemáticos e estatísticos, das características fisiológicas (tais como impressão digital, face, íris, geometria da mão, vascularização da mão, DNA e voz) ou comportamentais (voz, expressão facial, assinatura, modo de andar etc.) de um indivíduo. Quanto maior a quantidade de dados presentes na amostra biométrica provenientes de uma ou mais características, maior será a probabilidade de que ela tenha uma correspondência única, ou seja, a amostra apresentará maior qualidade para que a análise seja mais precisa e confiável. (Cebrian *et al*, 2024, p. 6).

Conforme anteriormente citado, a tecnologia tem ganhado popularidade pelo seu imenso potencial de aumento da segurança e da possível aplicação em diversas situações, sendo aprimorada pelo uso de Inteligência Artificial (IA), como *machine learning* e *deep learning,* o que otimizou os sistemas tradicionais, tornando a identificação mais rápida e precisa.

O funcionamento dessa tecnologia pode ser entendido de forma didática por meio de cinco etapas principais: primeiramente, ocorre a detecção, que consiste em encontrar e localizar rostos em imagens e vídeos, focando somente em perceber e determinar a posição das faces, sem atribuir características ou identidades específicas. Em seguida, na fase de análise e captura, a imagem do rosto é capturada e analisada; essa análise pode ler a geometria da face, examinando, por exemplo, a distância entre os olhos, a profundidade das órbitas oculares, a distância entre a testa e o queixo, e o formato das maçãs do rosto, lábios, orelhas e queixo, transformando esses pontos de referência em um modelo biométrico armazenado com a imagem original.

A terceira etapa é a identificação, onde o modelo biométrico de uma pessoa é comparado com outros armazenados em um banco de dados para verificar se a pessoa já está cadastrada e a quem pertence, sendo uma correspondência considerada positiva quando há correlação entre os modelos. Posteriormente, há a verificação, que compara dois modelos biométricos para determinar se são compatíveis ou correspondentes, sem a necessidade de conhecer a identidade exata dos indivíduos.

Finalmente, a última etapa é a classificação, na qual, com base no modelo biométrico, o indivíduo pode ser categorizado por atributos como gênero, raça, etnia, idade estimada, ou até mesmo por expressões (sorriso, choro) e estados emocionais (alegre, feliz, triste, nervoso, apático).

Os sistemas de *Deep Learning*, ao contrário de programas lineares cujas decisões seguem um caminho lógico e auditável, operam mediante operações matemáticas não lineares distribuídas em múltiplas camadas ocultas (*hidden layers*). Tais derivações da Inteligência Artificial consistem em modelos computacionais que permitem o aprendizado automático de padrões complexos a partir de volumes massivos de dados.

No contexto do reconhecimento facial, essas tecnologias aprimoram significativamente a precisão e a eficiência do sistema, possibilitando a extração automatizada de características biométricas e a sua comparação em larga escala. No entanto, essa mesma estrutura arquitetônica gera uma opacidade técnica intrínseca.

Conforme advertem Alves e Andrade (2021, p. 3), a sobreposição dessas múltiplas redes neurais cria uma barreira interpretativa entre a entrada de dados (input) e a predição final (output), tornando a cadeia de raciocínio da máquina um mistério insondável não apenas para o usuário médio, mas, frequentemente, para os próprios especialistas dotados de competências avançadas na área.

3 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

A implementação e funcionamento da tecnologia de reconhecimento facial em estádios no Brasil levanta questões sobre a compatibilidade dessa tecnologia com o direito fundamental à proteção de dados pessoais (Sousa; Souza Júnior, 2025).

A proteção de dados pessoais tem fundamentos robustos no arcabouço legal brasileiro. Afinal, a Constituição Federal de 1988 já assegurava, em seu Artigo 5º, inciso X:

> 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;

Em 2022, a Emenda Constitucional nº 115 reforçou essa proteção, elevando a proteção de dados pessoais à categoria de direito e garantia fundamental (Brasil, 2022).

> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Observando o plano legislativo, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018 (Brasil, 2018), complementa essa proteção ao buscar garantir os direitos de liberdade, privacidade e o livre desenvolvimento da personalidade. A lei classifica os dados biométricos, utilizados no reconhecimento facial, como dados pessoais sensíveis. Portanto, exige-se um nível de proteção elevado, pois, ao contrário de outros dados, os biométricos são permanentes e não podem ser alterados, tornando um vazamento potencialmente irreversível.

Consoante a cartilha emitida pelo Conselho da Justiça Federal, o "tratamento de dados" refere-se a toda operação realizada com dados pessoais por meios automatizados ou não. Quando esse tratamento envolve dados sensíveis, ele deve seguir rigorosamente os princípios da LGPD, como Finalidade, Adequação, Necessidade, Não-Discriminação e Transparência.

A regra geral da norma é que o tratamento desses dados só pode ocorrer com o consentimento livre, informado e inequívoco do titular. Nesse sentido:

> 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 [...] (Brasil, 2018, art. 11).

No entanto, o consentimento se torna um grande desafio em contratos de adesão, como a compra de ingressos, pois a exigência de dados biométricos como condição para o acesso ao estádio pode ser interpretada como um vício no consentimento, tornando-o nulo (Sousa; Souza Júnior, 2025), criando uma falta de liberdade e transparência, forçando o torcedor a escolher entre fornecer seus dados sensíveis para participar do evento ou ter seu acesso negado.

Atualmente, não há uma legislação federal específica no Brasil que regulamente o uso de reconhecimento facial. Além disso, a LGPD restringe o tratamento de dados para fins de segurança pública por entidades privadas, salvo em procedimentos sob a tutela de uma pessoa jurídica de direito público. Nesse sentido:

> [...] § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo (Brasil, 2018, art. 4).

O tratamento de dados pessoais de crianças e adolescentes no Brasil requer um regime jurídico de proteção rigoroso, fundamentado na Lei Geral de Proteção de Dados Pessoais (LGPD) e no Estatuto da Criança e do Adolescente (ECA). Nesse sentido o texto do art. 14 da LGPD, que estabelece:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. [...] § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal [...] § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei. (Brasil, 2018, art. 14).

Ocorre, contudo, que essa robusta arquitetura protetiva se tenciona drasticamente quando confrontada com as exceções de aplicabilidade da LGPD, notadamente aquela prevista em seu artigo 4º, inciso III, que permite, sob certas condições, o tratamento e o compartilhamento de dados sem o consentimento do titular quando realizado para fins exclusivos de segurança pública (Brasil, 2018).

Nos estádios, que são operados por empresas privadas, a invocação dessa exceção legal para justificar o uso do reconhecimento facial evidencia um cenário de vácuo regulatório, uma vez que o §1º do referido artigo exige legislação específica que garanta a proporcionalidade e o devido processo legal. Quando essa fronteira da vigilância avança sobre

a biometria de crianças e adolescentes, o princípio do "melhor interesse" acaba por ser subvertido. Ocorre, nesse ponto, um profundo desvio de finalidade informacional os dados capturados sob o pretexto de acesso a um evento civil de entretenimento são na verdade para finalidades de segurança pública. Nesse sentido:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...] III - realizado para fins exclusivos de: [...] a) segurança pública; [...]§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. [...] § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Brasil, 2018).

A controvérsia se aprofunda ao se reconhecer que o uso de reconhecimento facial em estádios configura, em regra, tratamento automatizado de dados pessoais capaz de produzir decisões com efeitos diretos sobre os titulares, por exemplo, através da autorização ou negativa de acesso do torcedor, portanto enquadrando-se, no art. 20 da LGPD, ainda que se invoque a exceção do art. 4º, III, para fins de segurança pública, sua aplicação é juridicamente limitada, sobretudo quando operacionalizada por entes privados e sem a legislação específica exigida pelo §1º, tudo isso fragiliza sua legitimidade.

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) [...] § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. [...] § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. (Brasil, 2018).

Nesse cenário, o art. 20 surgiria como mecanismo essencial de contenção, ao assegurar o direito à revisão de decisões automatizadas e à transparência dos critérios utilizados, contudo, na prática, observa-se a prevalência de sistemas opacos, nos quais as empresas não esclarecem adequadamente o funcionamento dos algoritmos, tampouco a origem de eventuais erros ou as medidas adotadas para sua correção. Essa realidade foi descrita no relatório emitido pelo CESeC, sobre reportagem noticiada pelo portal UOL, descrevendo um caso concreto de falha no sistema:

> João foi retirado do meio da torcida por mais de dois policiais militares do estado. Naquele momento, a única explicação que o torcedor teve foi de que teria sido identificado pelo sistema de reconhecimento facial do estádio como uma pessoa que estava com mandado de prisão em aberto. Segundo João, durante o diálogo, o policial disse que a tecnologia 'dificilmente erra'. O sistema, contudo, estava errado. (Sousa *et al*., 2024, p. 5).

4 A CIBERNÉTICA E OS MECANISMOS DE CONTROLE (MECANISMO DE CONTROLE, REGULAÇÃO E CAIXA PRETA)

Na teoria da Cibernética de Norbert Wiener (1970)[1], são explorados mecanismos de controle que se baseiam em informações. Partindo dessa ideia, a multidão presente em um estádio é vista como algo que tende ao caos, ou seja, imprevisível, confusa e difícil de controlar.

Nesse contexto, a organização e a regulação desse ambiente dependem de um ciclo contínuo composto por entrada de dados (*input*), processamento e geração de respostas (*output*), além da retroalimentação (*feedback*), que permite ajustar o sistema com base nos resultados obtidos. Assim, tecnologias como o reconhecimento facial operam como instrumentos cibernéticos de controle, na medida em que captam informações dos indivíduos, processam esses dados e produzem decisões que, posteriormente, influenciam o próprio comportamento do sistema, estabelecendo um fluxo constante de monitoramento e correção.

Surge assim, o sistema de reconhecimento facial como uma forma de tentar organizar essa situação, transformando pessoas em dados, rostos em cálculos matemáticos e comportamentos em previsões. Essa mudança permite que o sistema diminua as dúvidas e aumente sua capacidade de prever e agir. Essa forma de organização, contudo, distribui seus custos de maneira desigual, pois, enquanto para alguns representa maior eficiência e segurança, para outros implica perda de privacidade, exclusão e exposição a erros sistêmicos.

> Relata-se o caso de um algoritmo classificador de imagens que venceu vários prêmios na área. Mais tarde, foi averiguado que sua predição, muitas vezes, não detectava o objeto principal. Em vez disso, apenas utilizava correlações e dados indiretos para chegar ao resultado. Embora acertasse frequentemente, verificou-se que o modelo reconhecia barcos pela presença de água, trens pela presença de trilhos e até cavalos pela presença de uma marca d'água de direitos autorais embutida na imagem. Esses "preditores Clever Hans" podem ter bom desempenho em cenários de teste, mas certamente falharão quando implementados no mundo real, onde os objetos reconhecidos muitas vezes estão fora do seu contexto original. (Alves; Andrade, 2021, p. 6).

[1] Os estudos de Norbert Wiener e todo o contexto histórico da Teoria Cibernética podem ser buscados em Losano (2019, p. 1 a 141).

Portanto, os sistemas de biometria funcionam como verdadeiras “caixas-pretas”, nas quais os processos internos de decisão não são acessíveis ou plenamente compreensíveis. Isso ocorre porque, em sistemas de inteligência artificial, a dificuldade de compreender as relações entre os dados de entrada (*input*) e os resultados gerados (*output*) compromete a transparência do processo decisório, tornando arriscada a atribuição de decisões sensíveis a tais tecnologias. Afinal, a opacidade da cadeia de raciocínio algorítmico pode ocultar falhas ou até mesmo vieses discriminatórios, dificultando a confiança e o controle sobre esses sistemas (Alves; Andrade, 2021).

Nesse cenário, por vezes, o torcedor não consegue entender por que foi barrado ou sinalizado, enquanto o próprio Estado enfrenta dificuldades para explicar de forma completa como o algoritmo chegou a determinada conclusão. As empresas desenvolvedoras, por sua vez, frequentemente se resguardam sob o argumento do segredo industrial para não divulgar o funcionamento de seus modelos. Esse contexto gera tensão no sistema jurídico, que exige transparência, fundamentação das decisões e possibilidade de contraditório, sobretudo porque, conforme apontado na literatura, ainda são limitadas as ferramentas e técnicas disponíveis para tornar inteligíveis as decisões produzidas por sistemas baseados em múltiplas redes neurais artificiais (Cortiz, 2021, *apud* Alves; Andrade, 2021).

Estudos mostram que sistemas de reconhecimento facial apresentam taxas de erro mais elevadas em relação a pessoas negras, mulheres, idosos e crianças, o que já resultou em casos de prisões injustas e constrangimentos públicos (Sousa *et al.*, 2024, p. 18). No contexto brasileiro, esse problema é agravado pelo tensionamento entre a Lei Geral do Esporte e a LGPD, na medida em que argumentos de segurança pública têm sido utilizados para legitimar a ampliação de mecanismos de vigilância sem a devida limitação normativa. Tal cenário se torna ainda mais preocupante diante da opacidade inerente aos sistemas de inteligência artificial, já que modelos baseados em aprendizado de máquina operam por meio de sequências preditivas frequentemente incompreensíveis para seres humanos, o que dificulta a identificação e correção de vieses (Alves; Andrade, 2021).

Além disso, pesquisas indicam que a acurácia desses sistemas varia significativamente entre grupos demográficos, com taxas de erro substancialmente mais altas para mulheres negras em comparação a homens brancos, evidenciando uma assimetria estrutural que reforça discriminações já existentes (Buolamwini; Gebru, 2018, *apud* Sousa *et al.*, 2024 p. 18).

Nesse caso, pode-se refletir utilizando a metáfora da “Garra do Macaco”, usada por Wiener, onde o algoritmo faz o que foi programado de forma literal, priorizando os cálculos e ignorando questões sociais, jurídicas e éticas. Mesmo que as taxas de erro pareçam pequenas,

podem apresentar consequências graves quando aplicadas a multidões de pessoas, gerando falsos positivos que afetam diretamente os direitos fundamentais.

Dessarte, do ponto de vista da Cibernética, também se percebe que não há um "feedback negativo" eficaz. A pessoa que é barrada injustamente não tem acesso a mecanismos adequados para auxiliar na correção do sistema, e a falha não melhora o modelo. Pelo contrário, cria-se um ciclo vicioso, no qual dados antigos e tendenciosos reforçam a vigilância sobre certos grupos, alimentando a seletividade e a exclusão. Nesse sentido:

> Tal controle da máquina com base no seu desempenho efetivo em vez de no seu desempenho esperado é conhecido como realimentação (feedback) [...] A função desses mecanismos é a de controlar a tendência mecânica para a desorganização; em outras palavras, de produzir uma inversão temporária e local da direção normal da entropia. (Wiener, 1970, p. 22).

Wiener (1970), já nos alertava sobre os perigos de sistemas de controle inflexíveis, usando a imagem de uma formiga, que não consegue se adaptar a novas situações. Aplicado a lógica do sistema de reconhecimento facial, esse modelo, por vezes, implica tratar indivíduos como funções fixas, definidas por registros passados ou correlações estatísticas, sem consideração por trajetórias de mudança, reabilitação ou circunstâncias específicas. O autor afirma que "No organismo vivo, como no próprio universo, a repetição exata é absolutamente impossível." (Wiener, 1970, p. 44).

Além disso, em termos cibernéticos, pode-se falar em entropia social. A ordem técnica produzida dentro do estádio não elimina o caos, mas o desloca. Filas seletivas, discriminação algorítmica, exclusões arbitrárias e estigmatização de grupos vulneráveis indicam que a redução da entropia em um ponto do sistema gera desordem em outro, distribuída de forma desigual na sociedade.

Se, no plano teórico, a cibernética permite compreender o reconhecimento facial como mecanismo de controle orientado por informação e feedback, no plano empírico o estádio surge como espaço privilegiado para observar a materialização desses processos. É nesse ambiente que a promessa de ordem técnica encontra seus limites sociais, jurídicos e operacionais.

5 O ESTÁDIO COMO LABORATÓRIO DE VIGILÂNCIA

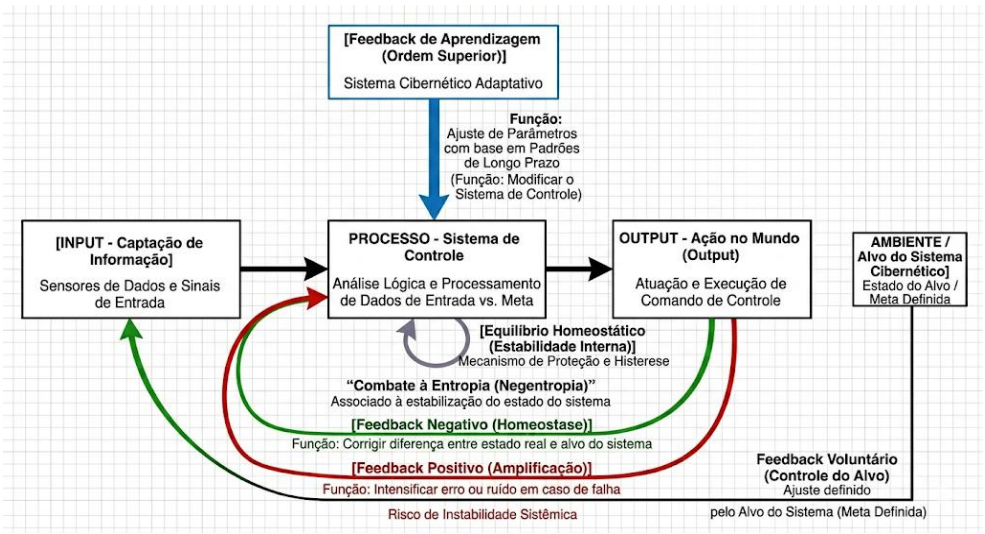
Para compreender a implementação do reconhecimento facial nos estádios brasileiros, é necessário afastar-se temporariamente do debate moral e observar o ambiente sob a ótica da cibernética de Norbert Wiener. Nessa perspectiva teórica, a sociedade e as máquinas

automáticas são compreendidas por meio do estudo dos seus sistemas de comunicação e controle.

5.1 *Input* e *Output*: a mecânica da "Máquina de Governar"

O funcionamento desse laboratório de controle estrutura-se em um ciclo contínuo. A primeira fase consiste na captação de informação do meio ambiente (input). Ao transformar a geometria facial de milhares de torcedores em modelos matemáticos decodificáveis nas catracas, o sistema importa informação estruturada e injeta "negentropia" (ordem) no ambiente. A informação, como define Wiener, é o conteúdo que permutamos com o mundo exterior para nos ajustarmos às suas contingências.

Figura 1 – Infográfico de feedback de aprendizagem



Fonte: Os autores (2026).

Em seguida, o dado biométrico passa pelo núcleo de processamento utilizando modelos de inteligência artificial, conforme já relatado, frequentemente baseados em *deep learning*, por tanto opacos, o sistema coteja a face com vastos bancos de dados. O resultado desse processamento gera um output material, que é a liberação mecânica da catraca, o bloqueio do torcedor ou a emissão de um alerta de segurança para as autoridades. O estádio converte-se, assim, naquilo que Wiener chamou de *machine à gouverner* (máquina de governar):

> Podemos sonhar com a época em que a *machine à gouverner* venha suprir - para o bem ou para o mal - a atual e óbvia insuficiência do cérebro, quando este se ocupa com a costumeira maquinaria da política. (Wiener, 1970, p. 167)

Ou seja, um sistema que substitui o controle humano direto por um controle informacional automatizado.

5.2 O discurso dos operadores: a promessa de menos entropia

Neste artigo, a legitimação pública desse mecanismo é analisada a partir do discurso adotado pela imprensa gaúcha, pelos clubes e pelas empresas operadoras de tecnologia, como a Imply[2], no Beira-Rio, e a Bepass[3], na Arena do Grêmio. Observa-se que esse discurso não se constrói de forma isolada, mas se insere em um movimento institucional mais amplo, no qual o uso de tecnologias de monitoramento é apresentado como resposta necessária ao problema da violência nos estádios. Nesse contexto, iniciativas estatais como o Projeto "Estádio Seguro", desenvolvido em parceria entre o governo federal e a CBF, reforçam essa narrativa ao propor a integração e o cruzamento de dados de torcedores como estratégia para ampliar a segurança, coibir práticas ilícitas e prevenir atos de violência (Brasil, 2023).

Nessa seara, o processo de implementação, que ganhou legitimidade a partir de episódios de violência em arenas esportivas, passa a ser apresentado como uma solução técnica indispensável, embora envolva relevantes preocupações relacionadas à privacidade dos torcedores, à vulnerabilização de crianças e adolescentes e ao já consolidado problema do racismo algorítmico (Sousa *et al*., 2024, p. 5).

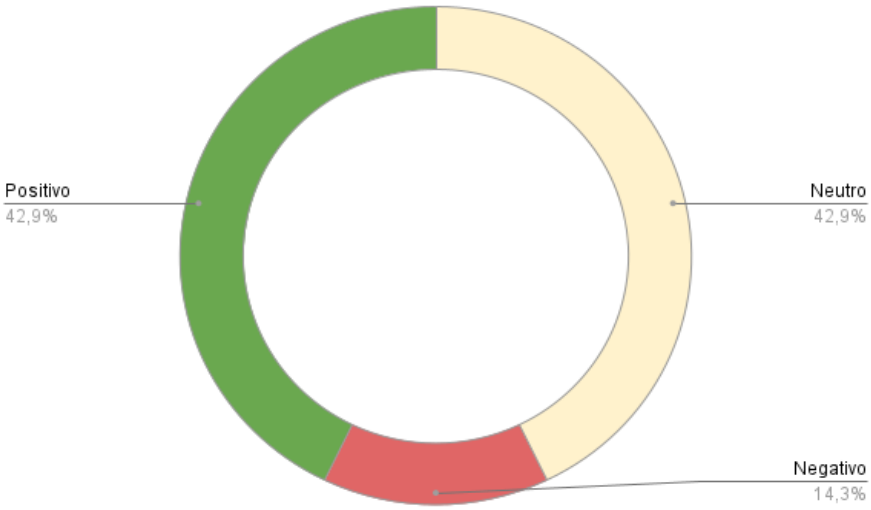
Para que um sistema cibernético mantenha sua estabilidade (homeostase) e consiga corrigir suas falhas, é indispensável a existência de canais íntegros de *feedback* (retroalimentação), por meio dos quais os resultados de suas ações retornam ao sistema como novas informações. No contexto analisado, a imprensa gaúcha foi analisada como um verdadeiro "termômetro" desse processo, ao mapear os fluxos comunicacionais e evidenciar os ciclos de retroalimentação que atravessam esse laboratório contemporâneo de vigilância.

A análise da cobertura de veículos como GZH (Biometria, 2025; Petrucci, 2025; Junior, 2025, Lisboa, 2025), Correio do Povo (Estudo, 2025; Inter, 2025; Mello, 2025), Jornal do Comércio (Arena, 2025; Inter, 2025) e O Sul (Redação O Sul, 2025) revela a existência de um duplo fluxo informacional. Conforme demonstrado na Figura 2, observa-se um equilíbrio entre narrativas positivas (42,9%) e neutras (42,9%), com menor incidência de abordagens

[2] Site: https://imply.com/pt/ (acesso em 21 abr. 2026).
[3] Site: https://bepass.com.br/ (acesso em 21 abr. 2026).

negativas (14,3%). Por um lado, o discurso institucional se sobressai de forma favorável, ecoando valores como segurança, agilidade e inovação tecnológica, o que reforça a percepção de que o sistema cumpre seu objetivo teleológico de ordenação e controle do ambiente.

Figura 2 – Narrativas sobre o sistema de reconhecimento facial



Fonte: Os autores (2026).

A narrativa positiva é demonstrada, por exemplo, na matéria veiculada no jornal GZH, por Pedro Petrucci (2025a), na arena do Grêmio se destacam argumentos sobre segurança e agilidade, com relatos de entradas até três vezes mais rápidas em comparação com cartões magnéticos e QR codes; o combate ao cambismo, mediante controle rigoroso do acesso; e (iii) inovação e eficiência, associadas à modernização da gestão de público.

Semelhantemente, no Beira-Rio, conforme reportagem veiculada pelo jornal O Sul, Victor Grunberg, vice-presidente do Internacional, comentou sobre as vantagens da ferramenta: “Entendo que a medida de tornar obrigatório o reconhecimento facial para estádios acima de 20 mil pessoas é extremamente válida. É uma forma eficaz de controle de segurança, porque é possível identificar todas as pessoas que estão ali e evitar que estejam em um evento privado, que é o futebol, indivíduos que têm um conflito com a lei e que potencialmente podem causar problemas dentro do estádio” (Redação O Sul, 2025).

Por outro lado, as matérias de cunho narrativo “negativo” funcionam como expressão do “ruído” sistêmico, ao revelar o contraponto empírico ao discurso institucional dominante; nesse sentido, a cobertura midiática registrou críticas relevantes, evidenciando falhas operacionais significativas, como longas filas e a necessidade de utilização de ingressos físicos

na Arena do Grêmio, além de riscos estruturais associados ao uso do reconhecimento facial (Petrucci, 2025b), ao passo que o jornal Correio do Povo destacou preocupações relativas à vigilância excessiva e à possível reprodução de vieses discriminatórios (Estudo, 2025).

Assim, embora a narrativa institucional enfatize ganhos como segurança, combate ao cambismo e eficiência operacional, a cobertura crítica expõe tensões concretas que evidenciam limitações técnicas e riscos sociais, demonstrando que o sistema não apenas produz ordem, mas também gera novos pontos de instabilidade que retroalimentam o ciclo de feedback e desafiam sua própria capacidade de regulação.

Cabe pontuar que, durante o desenvolvimento desta pesquisa, o Grêmio Foot-Ball Porto Alegrense atualizou sua Política de Privacidade e Proteção de Dados Pessoais. O novo documento incluiu uma nota de esclarecimento formalizando que, em cumprimento à Lei Geral do Esporte (Lei 14.597/2023), o cadastramento biométrico tornou-se um requisito obrigatório para a aquisição de ingressos e a validação de acesso às partidas (Grêmio..., 2026).

A leitura comparada desses documentos – Política de Privacidade e Proteção de Dados Pessoais relativos ao Grêmio (de outubro de 2025 e de abril de 2026) – evidencia que não houve abandono da disciplina da biometria facial, mas sim uma reorganização documental e institucional do tratamento de dados pessoais[4]. Os documentos da Arena, de outubro de 2025, foram elaborados para regular de maneira direta o cadastramento e a verificação de identidade mediante reconhecimento facial, detalhando bases legais, operadores envolvidos, fluxo operacional e retenção dos dados. Já a política atual, de abril de 2026, incorpora a biometria em uma moldura mais ampla de proteção de dados, relacionada ao conjunto das atividades do Grêmio perante torcedores e sócios, o que produz um ganho de integração sistêmica, mas, ao mesmo tempo, uma perda de densidade informativa específica sobre o tratamento biométrico facial.

Em síntese, as principais modificações realizadas foram: a substituição de documentos setoriais autônomos por uma política geral de caráter institucional; a mudança do sujeito que figura como centro da governança documental, da Arena para o Grêmio; a supressão de detalhes operacionais, como o papel nominal da Bepass, a janela temporal de migração dos dados para dispositivos e a referência expressa ao prazo adicional de 5 anos; e a atualização

[4] Vide Arena Porto-Alegrense S.A. — Política de Tratamento de Dados Pessoais Biométricos Faciais – Cadastramento (disponível em https://arenapoa.com.br/politicas-de-biometria-facial, com acesso em 06 out. 2025); Arena Porto-Alegrense S.A. — Política de Tratamento de Dados Pessoais Biométricos Faciais – Verificação de Identidade. Disponível em: https://arenapoa.com.br/politicas-de-privacidade/. Acesso em: 06 out. 2025 e; Política de Privacidade e Proteção de Dados Pessoais (disponível em https://gremio.net/politica_privacidade.pdf, acesso em 21 abr. 2026).

dos canais de contato e da estrutura de governança, com novo encarregado e novo e-mail institucional.

Essa legitimação discursiva não se esgota na cobertura midiática nem nas declarações institucionais. Ela também se projeta sobre a arquitetura documental que organiza o tratamento dos dados biométricos, razão pela qual a análise das políticas de privacidade e dos instrumentos de governança informacional se mostra indispensável para compreender como o sistema se estabiliza juridicamente.

5.3 A regulação jurídica como *feedback* negativo

Se, na linguagem da cibernética, o reconhecimento facial opera como um mecanismo de controle orientado à redução da entropia no ambiente do estádio, então o Direito deve ser compreendido como a instância encarregada de impor limites e correções ao próprio sistema de controle. Em outros termos, diante de uma tecnologia que coleta dados biométricos, processa informações sensíveis em larga escala e produz decisões com efeitos concretos sobre os torcedores, a regulação jurídica assume a função de feedback negativo, isto é, de mecanismo homeostático destinado a conter desvios, reduzir erros e impedir que a expansão operacional do sistema se converta em arbítrio tecnicamente legitimado (Brasil, 2018; 2023). Nessa chave de leitura, a intervenção jurídica não representa um obstáculo externo ao sistema, mas uma condição interna de sua legitimidade em uma ordem democrática.

A necessidade desse feedback jurídico torna-se ainda mais evidente quando se observa que o reconhecimento facial em estádios não se limita a um procedimento neutro de autenticação, mas envolve tratamento automatizado de dados pessoais sensíveis, com potencial para gerar bloqueios de acesso, constrangimentos indevidos e discriminações sistemáticas. A Lei Geral do Esporte tornou obrigatória a identificação biométrica em arenas com capacidade superior a vinte mil pessoas, mas essa imposição normativa não elimina, por si só, as exigências de proteção de dados, proporcionalidade e controle das decisões automatizadas (Brasil, 2023). Ao contrário, justamente porque o sistema passa a integrar a infraestrutura regular de acesso aos eventos esportivos, cresce a necessidade de mecanismos capazes de revisar seus resultados, auditar suas falhas e limitar os riscos produzidos por sua operação em larga escala (Brasil, 2018; Souza; Souza Júnior, 2025).

É nesse ponto que a crítica à caixa-preta algorítmica se articula diretamente com a noção cibernética de feedback. Um sistema só aprende e se corrige quando o resultado de sua operação retorna a ele sob a forma de informação apta a modificar seu comportamento futuro.

Contudo, quando o modelo decisório é opaco, os erros deixam de funcionar como insumos de correção e passam a ser absorvidos como externalidades suportadas pelos indivíduos atingidos. A passagem da caixa-preta à caixa de vidro, tal como proposta por Alves e Andrade (2021), não exige a eliminação completa da complexidade técnica, mas a criação de níveis suficientes de interpretabilidade, explicabilidade, verificabilidade e auditabilidade, especialmente em contextos de alto risco social. Sem isso, o titular barrado injustamente permanece diante de uma decisão cuja racionalidade lhe é inacessível, ao passo que o controlador preserva a autoridade da máquina sem demonstrar, de modo inteligível, por que ela errou, como errou e quais providências foram adotadas para evitar a repetição da falha.

Sob a perspectiva jurídica, esse déficit de retroalimentação corretiva entra em tensão direta com o art. 20 da LGPD, que assegura ao titular o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais e de obter informações claras e adequadas acerca dos critérios e procedimentos utilizados (Brasil, 2018). O problema, porém, é que a existência formal desse direito não garante sua efetividade material. Quando o sistema é estruturado por modelos preditivos opacos, protegidos por segredo comercial e operados em ambientes de vigilância massificada, a revisão tende a tornar-se residual, tardia ou meramente protocolar. Em vez de um verdadeiro feedback negativo, capaz de reconduzir o sistema a parâmetros juridicamente aceitáveis, corre-se o risco de instaurar um circuito de autorreforço, no qual a decisão automatizada presume a sua própria correção e desloca ao titular o ônus de contestar uma lógica que ele não pode conhecer.

Por isso, a regulação jurídica adequada do reconhecimento facial em estádios não pode restringir-se à autorização abstrata de uso nem à oferta genérica de canais de atendimento ao titular. Se o Direito pretende desempenhar a função de *feedback* negativo, deve estruturar exigências concretas de governança: avaliação de impacto, rastreabilidade das decisões, possibilidade de auditoria independente, dever de explicação compatível com a gravidade dos efeitos produzidos, revisão humana efetiva nos casos de bloqueio ou suspeita e demonstração empírica de não discriminação do sistema (Alves; Andrade, 2021; Sousa; Souza Júnior, 2025). Em termos cibernéticos, trata-se de reintroduzir informação qualificada no circuito de controle para que o sistema não apenas opere, mas também seja capaz de ser corrigido a partir de seus próprios erros.

Desse modo, a principal questão jurídica não reside apenas em saber se a tecnologia aumenta a eficiência do acesso ou reforça a segurança do estádio. A questão decisiva consiste em definir quais freios normativos devem incidir sobre essa máquina de governar para impedir que a promessa de ordem produza novas formas de opacidade, exclusão e violência

informacional. Se a biometria facial é apresentada como instrumento de redução da desordem, cabe ao Direito assegurar que essa redução não seja obtida mediante a erosão silenciosa das garantias fundamentais. O feedback negativo jurídico, nesse cenário, é o que transforma a mera operação técnica em operação controlável, contestável e democraticamente justificável.

6 CONSIDERAÇÕES FINAIS

O presente estudo examinou a implementação do reconhecimento facial nos estádios brasileiros, com especial atenção aos casos da dupla Gre-Nal, a partir da tensão entre segurança, vigilância tecnológica e proteção de dados pessoais. À luz da cibernética de Norbert Wiener (1970), procurou-se demonstrar que o estádio contemporâneo deixa de ser apenas espaço de lazer e circulação para converter-se em ambiente de comunicação e controle, no qual a biometria facial opera como mecanismo de redução da incerteza por meio da produção, processamento e circulação de informação.

A análise desenvolvida permitiu identificar que o reconhecimento facial, embora apresentado institucionalmente como instrumento de segurança, agilidade e eficiência operacional, não elimina a desordem, mas a reorganiza por meio de novas formas de vigilância informacional. Em vez de resolver integralmente o problema da violência e da imprevisibilidade nos ambientes esportivos, o sistema desloca parte da desordem para outros pontos da experiência social, produzindo riscos de bloqueios indevidos, constrangimentos públicos, exclusões arbitrárias e assimetrias na distribuição dos ônus da vigilância, sobretudo quando se consideram os efeitos da opacidade algorítmica e da possibilidade de discriminação indireta.

No plano jurídico, o trabalho mostrou que a obrigatoriedade da identificação biométrica prevista na Lei Geral do Esporte não afasta as exigências normativas impostas pela proteção de dados pessoais, especialmente quando estão em causa dados biométricos sensíveis submetidos a tratamento automatizado. Nesse sentido, verificou-se que a compatibilidade entre a implementação do reconhecimento facial e as garantias previstas na Lei Geral de Proteção de Dados permanece tensionada por fatores como a insuficiente transparência dos sistemas, a dificuldade de compreensão dos critérios decisórios, a limitação prática do direito à revisão de decisões automatizadas e a atuação de entes privados em um campo argumentativamente aproximado da segurança pública.

A partir do referencial cibernético adotado, conclui-se que a legitimidade desses sistemas depende da existência de canais efetivos de retroalimentação corretiva. Em outros

termos, a tecnologia somente pode ser juridicamente admitida em bases democráticas quando seus resultados puderem ser contestados, revisados e corrigidos de maneira inteligível e institucionalmente verificável. Foi precisamente nessa direção que se sustentou, no item 5.3, que a regulação jurídica deve operar como feedback negativo, isto é, como mecanismo de contenção dos desvios produzidos pela própria máquina de governar. Sem auditabilidade, explicabilidade, rastreabilidade e revisão humana efetiva, o reconhecimento facial tende a consolidar um circuito autorreferente de legitimação técnica, no qual o erro não se converte em aprendizado institucional, mas em custo suportado pelo indivíduo afetado.

Desse modo, a questão central não consiste apenas em saber se a tecnologia funciona ou se amplia a capacidade de controle nos estádios. A questão decisiva reside em definir sob quais condições jurídicas, institucionais e informacionais esse funcionamento pode ser considerado legítimo. O estudo indica que a promessa de ordem produzida pelo reconhecimento facial somente se sustenta normativamente quando acompanhada de limites proporcionais, mecanismos reais de contestação, governança transparente do tratamento de dados e instrumentos de responsabilização compatíveis com a gravidade dos efeitos que a decisão automatizada pode gerar sobre os titulares.

Por fim, a pesquisa abre caminho para o aprofundamento teórico e empírico do tema, indicando a necessidade de aprimoramento do referencial analítico sobre as relações entre cibernética, direito e tecnologias de vigilância. Do ponto de vista empírico, mostra-se especialmente relevante a obtenção de dados mais qualificados mediante contato direto com clubes, operadoras e administradoras responsáveis pela gestão dessas tecnologias, o que poderá oferecer maior precisão quanto às práticas de tratamento, compartilhamento, retenção e segurança dos dados biométricos. Também se recomenda a ampliação da investigação para incorporar de maneira mais sistemática a perspectiva dos torcedores, inclusive por meio da análise de manifestações em redes sociais e plataformas de reclamação, de modo a captar com maior densidade o feedback social produzido por esses sistemas. Tais desdobramentos podem contribuir para uma compreensão mais abrangente das implicações jurídicas, técnicas e sociais do reconhecimento facial em estádios, oferecendo subsídios para a formulação de políticas de governança de dados mais transparentes, proporcionais e compatíveis com parâmetros democráticos.

REFERÊNCIAS

ALVES, Marco Antônio Sousa; ANDRADE, Otávio Morato de. Da “caixa-preta” à “caixa de

vidro": o uso da explainable artificial intelligence (XAI) para reduzir a opacidade e enfrentar o enviesamento em modelos algorítmicos. **Direito Público**, [S. l.], v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.5973. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5973. Acesso em: 23 abr. 2026.

ARENA DO GRÊMIO. Políticas de biometria facial. Porto Alegre, [2025]. Disponível em: https://arenapoa.com.br/politicas-de-biometria-facial. Acesso em: 6 out. 2025.

ARENA DO GRÊMIO. Políticas de privacidade. Porto Alegre, [2025]. Disponível em: https://arenapoa.com.br/politicas-de-privacidade/. Acesso em: 6 out. 2025.

ARENA do Grêmio adota a partir de domingo reconhecimento facial para acesso ao estádio. **Jornal do comércio**, 2025. Disponível em: https://www.jornaldocomercio.com/esportes/2025/01/1187985-arena-do-gremio-adota-a-partir-de-domingo-reconhecimento-facial-para-acesso-ao-estadio.html. Acesso em: 23 abr. 2026.

BIOMETRIA facial passa a ser obrigatória no acesso à Arena e ao Beira-Rio; veja como se cadastrar. **Zero Hora**, 2025. Disponível em: https://gauchazh.clicrbs.com.br/esportes/noticia/2025/07/biometria-facial-passa-a-ser-obrigatoria-no-acesso-a-arena-do-gremio-e-ao-beira-rio-veja-como-se-cadastrar-cmcuzuyy800b6014ra0mheb51.html. Acesso em: 17 abr. 2026.

BIOMETRIA facial: Torcedor Colorado, ainda está com dúvidas sobre a Biometria Facial? **Sport Club Internacional**. Porto Alegre [2025]. Disponível em: https://www.internacional.com.br/biometria-facial. Acesso em: 17 abr. 2026.

BRASIL. **Lei nº 14.597, de 14 de junho de 2023.** Institui a Lei Geral do Esporte. Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14597.htm. Acesso em: 7 ago. 2025.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14597.htm. Acesso em: 7 ago. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 7 ago. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 ago. 2025.

BRASIL. Ministério do Esporte. **Ministérios do Esporte e da Justiça assinam acordo de cooperação com CBF para implantação do projeto Estádio Seguro**. Disponível em: https://www.gov.br/esporte/pt-br/noticias-e-conteudos/esporte/ministerios-do-esporte-e-da-

justica-assinam-acordo-de-cooperacao-com-cbf-para-implantacao-do-projeto-estadio-seguro. Acesso em: 17 abr. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. **Nota Técnica nº 5/2025/FIS/CGF/ANPD.** Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnia-5_2025_fis_cgf_versao-publica_ocultado.pdf/view. Acesso em: 17 abr. 2026.

ESTUDO aponta riscos de tecnologias de reconhecimento facial. **Correio do Povo**. 2025. Disponível em: https://www.correiodopovo.com.br/jornal-com-tecnologia/estudo-aponta-riscos-de-tecnologias-de-reconhecimento-facial-1.1606015. Acesso em: 17 abr. 2026.

GRÊMIO FOOT-BALL PORTO ALEGRENSE. Política de privacidade e proteção de dados pessoais. Porto Alegre, [2026]. Disponível em: https://gremio.net/politica_privacidade.pdf Acesso em: 23 abr. 2026.

INTER testa sistema de reconhecimento facial em todos os setores do Beira-Rio. **Correio do Povo**, 2025. Disponível em: https://www.correiodopovo.com.br/esportes/inter/inter-testa-sistema-de-reconhecimento-facial-em-todos-os-setores-do-beira-rio-1.1575183. Acesso em: 17 abr. 2026.

INTER testa sistema de reconhecimento facial em todos os setores do Beira-Rio. **Jornal do comércio**, 2025. Disponível em: https://www.jornaldocomercio.com/esportes/2025/02/1189562-inter-testa-sistema-de-reconhecimento-facial-em-todos-os-setores-do-beira-rio.html. Acesso em: 17 abr. 2026.

JUNIOR, Valter. Velocidade, segurança e baixo índice de falhas: biometria facial agrada a Grêmio e Inter, apesar de ainda apresentar desafios. **Zero Hora**, 2025. Disponível em: https://gauchazh.clicrbs.com.br/esportes/noticia/2025/08/velocidade-seguranca-e-baixo-indice-de-falhas-biometria-facial-agrada-a-gremio-e-inter-apesar-de-ainda-apresentar-desafios-cme01oidz00zv012xdths2qvp.html. Acesso em: 17 abr. 2026.

LISBOA, Geison. Arena do Grêmio testará novo modelo de acesso ao estádio no jogo de domingo. **Zero Hora**, 2025. Disponível em: https://gauchazh.clicrbs.com.br/esportes/gremio/noticia/2025/01/arena-do-gremio-testara-novo-modelo-de-acesso-ao-estadio-no-jogo-de-domingo-cm69op3sw01t2015duk0lapqg.html. Acesso em: 17 abr. 2026.

LOSANO, Mario Giuseppe. Os sistemas cibernéticos do direito. *In* **Sistema e estrutura no Direito**: volume 3, do século XX a pós-modernidade. São Paulo: Ed. WMF Martins Fontes, 2019. p. 1 a 141.

LUHMANN, Niklas. **O direito da sociedade**. São Paulo: Martins Fontes, 2016.

MELLO, Lucas. Arena Porto-Alegrense rebate críticas do Grêmio sobre a operação do estádio. **Correio do Povo**, 2025. Disponível em: https://www.correiodopovo.com.br/esportes/grêmio/arena-porto-alegrense-rebate-críticas-do-grêmio-sobre-a-operação-do-estádio-1.1605942. Acesso em: 17 abr. 2026.

PETRUCCI, Pedro. Arena do Grêmio implanta catracas que agilizam acesso ao estádio e

auxiliam na segurança. **Zero Hora**, 2025a. Disponível em: https://gauchazh.clicrbs.com.br/esportes/gremio/noticia/2025/03/arena-do-gremio-implanta-catracas-que-agilizam-acesso-ao-estadio-e-auxiliam-na-seguranca-cm7z75h2b00bt016er71r201u.html. Acesso em: 17 abr. 2026.

PETRUCCI, Pedro. Falha no reconhecimento facial gera reclamação de torcedores do Grêmio na Arena. **Zero Hora**, 2025b. Disponível em: https://gauchazh.clicrbs.com.br/esportes/gremio/noticia/2025/05/falha-no-reconhecimento-facial-gera-reclamacao-de-torcedores-do-gremio-na-arena-cmabhe1ez008k014uwvmfz5lq.html. Acesso em: 17 abr. 2026.

REDAÇÃO O SUL. Reconhecimento facial passa a ser obrigatório nos estádios do Brasileirão. **Jornal O sul,** 2025. Disponível em: https://www.osul.com.br/reconhecimento-facial-passa-a-ser-obrigatorio-nos-estadios-do-brasileirao. Acesso em: 17 abr. 2026.

RECONHECIMENTO facial passa a ser obrigatório na Arena e no Beira-Rio. **Radio Grenal**, 2025. Disponível em: https://www.radiogrenal.com.br/reconhecimento-facial-passa-a-ser-obrigatorio-na-arena-e-no-beira-rio. Acesso em: 17 abr. 2026.

SOUSA, Raquel. *et al*. **ESPORTE, DADOS E DIREITOS**: O USO DE RECONHECIMENTO FACIAL NOS ESTÁDIOS BRASILEIROS. Rio de Janeiro: CESeC, 2024. Disponível em: https://drive.google.com/file/d/1ZK9d75us3HYYoeRjf3UR7SWfEWQQTGaQ/view. Acesso em: 17 abr. 2026.

SOUSA, Raquel de Oliveira; SOUZA JÚNIOR, Roberto. Reconhecimento facial nos estádios, tecnologia de segurança ou mecanismo de vigilância? Notas etnográficas sobre a importância da perspectiva torcedora para o debate. **Temáticas**, Campinas, SP, v. 33, n. 65, p. 51–78, 2025. Disponível em: https://econtents.bc.unicamp.br/inpec/index.php/tematicas/article/view/20025. Acesso em: 17 abr. 2026.

WENDT, Emerson; SCHWARTZ, Germano. **Dos algoritmos à Inteligência Artificial**: o cibersistema da internet e as expectativas algonormativas na diferenciação funcional do direito. Leme-SP: Mizuno, 2025.

WIENER, Norbert. **Cibernética e sociedade**: o uso humano de seres humanos. São Paulo: Cultrix, 1970.