Institutional Accountability and Liability for AI-Driven Harm in Sports

Author: Aman Anand

LL.M (Cyber Law), The ICFAI University, Dehradun

Co-Author: Dr. Razit Sharma

Assitant Professor, The ICFAI University,Dehradun

ABSTRACT

The sports industry has undergone a structural transformation driven by AI technologies that now permeate athlete performance analysis, biometric monitoring, injury prediction, talent scouting, and fan engagement. In India, this transformation has accelerated in the wake of two legislative developments: the Digital Personal Data Protection Act, 2023 (DPDPA) and the National Sports Governance Act, 2025 (NSG Act).The DPDPA introduces consent-based data processing obligations that apply when sports organisations collect athlete biometric and health data through AI-powered wearable devices and monitoring systems. The NSG Act creates a statutory governance framework for national sports bodies, mandating ethics committees, athlete representation, and grievance redressed mechanisms, but does not specifically address data protection or AI-related risks. It examines whether the consent mechanisms in standard athlete employment contracts satisfy the DPDPA's requirement of free, specific, informed, and unambiguous consent when athletes face structural power imbalances in their relationships with clubs and federations. It further investigates how legal liability for AI-related harm in sports, including algorithmic bias in athlete selection, data breaches, and automated decision-making errors, should be distributed among sports organisations, technology vendors, and governing bodies under Indian law.

Keywords: *Artificial Intelligence, Sports Law, Cyber Law, Athlete Privacy, Biometric Data, Fan Engagement, Data Protection, Institutional Accountability, personal data*

The accountability problem: who is liable when AI causes harm in sports?

When an AI system causes harm in the sports context, whether through algorithmic bias in athlete selection, an inaccurate injury prediction that sidelines a player unnecessarily, a data breach that exposes sensitive health information, or a discriminatory automated decision that affects an athlete's career, the question of legal liability does not have a straightforward answer. The reason is structural: AI-driven decisions in sports involve a chain of actors, each contributing a different element to the final outcome, and existing Indian law does not assign liability to this distributed chain as a whole.

The actors in this chain typically include the sports organisation (the IPL franchise, the national federation, or SAI) that deploys the AI system and acts on its outputs, the technology vendor that developed the AI algorithm and maintains the analytics platform, the wearable device manufacturer that collects raw biometric data from the athlete's body, the data processor that stores and processes data on behalf of the sports organisation, and in some cases the governing body (such as the BCCI or a national sports federation under the NSG Act) that mandates the use of specific technologies or data collection practices across the sport.

Chesterman (2021) argued that the fundamental challenge of AI liability is that traditional legal frameworks assign responsibility to identifiable human decision-makers, whereas AI systems distribute decision-making across algorithms, data inputs, and institutional processes in ways that obscure individual responsibility.[1] Brownsword (2019) framed this as a problem of "regulatory disconnection" where legal concepts like consent and negligence, designed for human-to-human interactions, lose their analytical grip when applied to automated systems.[2]

---

[1]Simon Chesterman, WE, THE ROBOTS: REGULATING ARTIFICIAL INTELLIGENCE 45-50 (Cambridge University Press, 2021).

[2]Roger Brownsword, LAW, TECHNOLOGY AND SOCIETY: RE-IMAGINING THE REGULATORY ENVIRONMENT 110-118 (Routledge, 2019).

In the Indian legal framework, three statutory provisions are potentially applicable to AI liability in sports: Section 43A of the IT Act, Section 72A of the IT Act, and the data fiduciary obligations under Section 8 of the DPDPA. Additionally, the Consumer Protection Act, 2019 introduces product liability concepts that may apply to AI systems. Each of these is examined in the sections that follow.

1. Algorithmic bias in athlete selection and performance evaluation

Algorithmic bias in sports AI is not a theoretical concern. A systematic scoping review published in the Journal of Sport and Health Science (2025), covering studies from inception through November 2024, identified fairness and bias as one of the four critical ethical concerns in AI-driven sports systems, alongside transparency, privacy, and accountability.[3] The review found that AI systems in sports can produce discriminatory outcomes when trained on historical data that reflects pre-existing inequalities in selection practices, scouting networks, or performance evaluation criteria.

A narrative review published in AI journal (2025) examined 24 empirical and conceptual studies on AI-driven injury prediction and identified algorithmic fairness as a dominant ethical concern.[4] The review found that AI injury prediction systems can create a "novel form of structural discrimination" when athletes labelled as high-risk by an algorithm are excluded from training or competition based on the label alone, without contextual interpretation from qualified staff. The study recommended incorporating "human-in-the-loop mechanisms, ethical guidelines for label communication, and regular audits of decision outcomes" to prevent AI-generated risk labels from becoming automatic exclusionary criteria.

The LaLiga Business School analysis (2026) noted that performance metrics used by AI systems "do not exist in isolation" and that factors such as team role, tactical system, injury history, and competition level heavily influence data outputs.[5] When AI systems fail to contextualise these variables, they produce outputs that may systematically disadvantage athletes who play certain positions, operate within specific tactical systems, or compete at particular levels. The analysis warned that without transparency, "AI risks becoming an unquestionable authority rather than a support tool."

Under Indian law, an athlete who is denied selection or contract renewal based on a biased AI recommendation currently has limited legal recourse. Article 14 of the Constitution guarantees the right to equality and equal protection of laws.[6] However, when the discriminating actor is a private entity like an IPL franchise, Article 14 does not apply horizontally. The DPDPA's Section 8(3) requires data fiduciaries to ensure the "completeness, accuracy and consistency" of personal data used to make decisions affecting data principals.[7] But this provision addresses data quality, not algorithmic fairness. An AI algorithm can produce biased outputs from perfectly accurate and complete data if the algorithm itself encodes discriminatory patterns learned from historical training data.

2. Liability for AI-driven injury prediction failures

AI injury prediction systems generate outputs that directly affect whether athletes train, rest, or compete. Industry data shows that knee and ankle injuries among Indian football and cricket players have surged by 500% in recent years, and ACL tears have risen by 400%.[8] AI injury prediction systems are positioned as the solution, with vendors like Zone7 reporting dramatic reductions in injury rates for clubs that use their platforms. But the flip side of these claims is that AI injury prediction creates a duty of care: if a sports organisation deploys an AI system that claims to predict injuries and the system fails, the organisation's reliance on that system becomes legally relevant.

Under Section 43A of the IT Act, a body corporate that possesses, deals with, or handles sensitive personal data and is negligent in implementing and maintaining reasonable security practices and procedures is liable to pay

[3]Ethical Implications of Artificial Intelligence in Sport: A Systematic Scoping Review, 14 J. SPORT & HEALTH SCI. 101047 (2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12226371/.

[4]Ethical Bias in AI-Driven Injury Prediction in Sport: A Narrative Review of Athlete Health Data, Autonomy and Governance, 6 AI 283 (2025), https://www.mdpi.com/2673-2688/6/11/283.

[5]Ethical Challenges of Training with AI, LALIGA BUSINESS SCHOOL (Feb. 14, 2026), https://business-school.laliga.com/en/news/newsethics-bias-ia-sport-

[6]INDIA CONST. art. 14 (right to equality and equal protection).

[7]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, S. 8(3), INDIA CODE (2023) (accuracy, completeness and consistency of data used for decisions affecting data principals).

[8]Injury Prediction Tools: Predictive Tech Indian Sports Centers Can Adopt, OUTLOOK INDIA HUB4SPORTSTECH (June 20, 2025), https://www.outlookindia.com/hub4sportstech/injury-prediction-tools-predictive-tech-indian-sports-centers-can-adopt.

damages to the affected person.[9] Athlete health and biometric data qualifies as sensitive personal data under Rule 3 of the IT Rules, 2011.[10] If a technology vendor's negligent handling of an athlete's biometric data contributes to an incorrect injury prediction, for example by corrupting data inputs or failing to update calibration standards, Section 43A provides a basis for compensation.

The DPDPA's Section 8(3) creates a separate obligation. Where personal data is likely to be used to make a decision that affects the data principal, the data fiduciary must ensure its completeness, accuracy, and consistency. A sports organisation that makes training or selection decisions based on AI injury predictions is using personal data (biometric and health data) to make decisions affecting the athlete. If the underlying data is inaccurate or inconsistent, leading to a wrong prediction that causes harm, the organisation breaches its Section 8(3) obligation. However, neither Section 43A nor Section 8(3) addresses the situation where the data is accurate but the algorithm produces a faulty prediction due to model limitations, training bias, or contextual factors the model cannot capture. Farajpour et al. (2025) identified this as a core legal problem in AI-driven sports decision-making: "If an athlete or team suffers due to an AI-related error, determining accountability becomes a challenge" because the error may reside not in the data but in the algorithmic logic itself.[11]

3. Data breach liability in sports

Data breaches in sports are not hypothetical risks. The Sports Litigation Alert (2025) documented the growing web of compliance obligations facing sports organisations, clubs, leagues, and technology vendors that collect and process athlete biometric information, noting that these entities "must navigate a complex web of compliance obligations" under data protection laws globally.[12]Brabners (2025) identified data privacy and security as one of the critical legal challenges in sports digital transformation, warning that collecting and analysing personal data of athletes and fans "creates risks under data privacy laws" that many sports organisations are not yet equipped to manage.[13]

Under the DPDPA, data fiduciaries must implement "appropriate technical and organisational measures" to ensure compliance with the Act, and the DPDP Rules, 2025 (Rule 7) mandate intimation of personal data breaches to the Data Protection Board and affected data principals within 72 hours.[14]

The practical application of these provisions to sports data breaches creates layered liability. If an IPL franchise's cloud-based analytics platform is breached and athlete health data is exposed, the franchise (as data fiduciary) bears primary liability under the DPDPA for failing to implement adequate security measures.[15] The technology vendor that operates the analytics platform (as data processor) bears contractual liability to the franchise under the data processing agreement required by Section 8(2) of the DPDPA. And if any individual within the franchise or vendor organisation disclosed data in breach of a contractual confidentiality obligation, Section 72A of the IT Act creates personal criminal liability.

The Orrick analysis (2025) documented a 2024 US case in which plaintiffs alleged that a sports venue collected facial scans of over 100,000 visitors and shared biometric data with third-party software providers.[16] Under the

[9]The Information Technology Act, 2000, No. 21 of 2000, S. 43A, INDIA CODE (2000) (compensation for failure to protect data).

[10]The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3 (defining sensitive personal data).

[11]Farajpour et al., AI-Driven Arbitration in Sports: Legal and Ethical Implications, 3 AI & TECH. IN BEHAV. & SOC. SCI. 21-28 (2025), https://www.journalkmanpub.com/index.php/aitechbesosci/article/download/3737/5855/17609.

[12]Biometric Data and Athletes: Privacy Law and Compliance Implications, SPORTS LITIGATION ALERT (Nov. 28, 2025), https://sportslitigationalert.com/biometric-data-and-athletes-privacy-law-and-compliance-implications/.

[13]Enabling Digital Transformation in Sport: The Legal Pitfalls Around Data Security and Regulation, BRABNERS (Nov. 12, 2025), https://www.brabnercom/insights/sport/enabling-digital-transformation-in-sport-the-legal-pitfalls-around-data-security-and-regulation.

[14]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, S. 8(5), INDIA CODE (2023) (reasonable security safeguards).

[15]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, S. 8(1), INDIA CODE (2023) (data fiduciary responsible for compliance irrespective of any agreement to the contrary).

[16]Facial Recognition Technology Use in Stadiums: Key Takeaways, ORRICK (Nov. 3, 2025), https://www.orrick.com/en/Insights/2025/11/Facial-Recognition-Technology-Use-in-Stadiums-Key-Takeaway

DPDPA, such sharing without consent would violate the purpose limitation principle and the consent requirements of Section 6.[17]

4.The distributed liability chain: sports organisations, technology vendors, and governing bodies

The most significant liability gap in Indian law concerns the distributed nature of AI decision-making in sports. When a sports organisation deploys an AI system developed by a third-party vendor, data collected by a separate wearable manufacturer, and processed through a cloud platform operated by yet another entity, liability for harm is distributed across multiple actors. Current Indian law assigns primary responsibility to the data fiduciary (the sports organisation) under Section 8(1) of the DPDPA, which holds the fiduciary responsible "irrespective of any agreement to the contrary."

However, this arrangement creates a gap. The sports organisation is liable for compliance failures even though the algorithmic logic that produced the harmful output was designed by the technology vendor, the training data may have been curated by a separate data analytics firm, and the raw data may have been collected by a wearable manufacturer whose devices the organisation did not design or calibrate.

Guo et al. (2024) mapped this distributed structure through stakeholder analysis and identified sports organisations, technology vendors, and governing bodies as the three primary nodes in the data governance chain.[18] Kwon (2025) framed this as a problem of "athlete data sovereignty," arguing that when legal ownership of data is unclear and contractual arrangements assign processing rights to employers, the athlete loses effective control over their own biometric information.[19]

The Consumer Protection Act, 2019 provides a partial solution through its product liability provisions. Section 84 of the Act establishes product liability for defective products, covering manufacturers, sellers, and product service providers.[20] However, whether AI software qualifies as a "product" under the Act's definition in Section 2(33), which covers "any article or goods manufactured by any process," remains an open question in Indian law.

The NSG Act 2025 creates institutional governance structures that could partially address this gap. Section 15 requires recognised sports organisations to establish ethics committees, grievance redressal mechanisms, and safe sports policies.[21] A well-functioning grievance redressal mechanism could receive complaints from athletes about AI-related harm and direct them toward appropriate resolution. The National Sports Tribunal established under Section 17 has jurisdiction over sports-related disputes and could, in principle, adjudicate claims involving AI-driven decisions that affect athlete careers.[22]

5. Fan data and institutional accountability for stadium surveillance

The institutional accountability framework for fan data differs from athlete data because the relationship between fans and sports organisations is transactional rather than employment-based. Fans interact with sports organisations primarily through ticket purchases, app registrations, and stadium entry. The data collection that occurs through these interactions, including facial recognition at entry gates, behavioural tracking through stadium Wi-Fi networks, and purchase pattern analysis at concession stands, is governed by the general provisions of the DPDPA and the IT Act.

[17]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, S. 6, INDIA CODE (2023) (consent requirements).

[18]Xuguo Guo et al., Diversifying Configurational Paths for Athlete Data Protection, 14 SCI. REP. 32053 (2024), https://doi.org/10.1038/s41598-024-83792-8.

[19]Jun Woo Kwon, Athlete Data Sovereignty: Addressing the Legal and Policy Gaps in Sports Technology, 7 FRONTIERS IN SPORTS & ACTIVE LIVING 1742484 (2025), https://www.frontiersin.org/journals/sports-and-active-living/articles/10.3389/fspor.2025.1742484/full.

[20]The Consumer Protection Act, 2019, No. 35 of 2019, S. 84, INDIA CODE (2019) (product liability).

[21]The National Sports Governance Act, 2025, No. 25 of 2025, S. 15, INDIA CODE (2025) (duties of recognised sports organisations).

[22]The National Sports Governance Act, 2025, No. 25 of 2025, S. 17, INDIA CODE (2025) (National Sports Tribunal).

The ACLU (2024) warned that facial recognition in stadiums threatens to normalise surveillance technology, noting that stadiums could become "the future of surveillance" where biometric scanning is a condition of access to popular events.[23]

Under the DPDPA, a sports organisation that deploys facial recognition in a stadium is a data fiduciary processing biometric data of fans who are data principals. The organisation must provide notice under Section 5 explaining what biometric data is collected and the purpose. Consent under Section 6 must be free, specific, informed, and unambiguous. If the only alternative to facial recognition is a substantially longer entry queue or denial of entry, the "free" element of consent is compromised. Section 8(7) requires erasure when the purpose is served, which means that facial data captured for entry verification must be deleted after the fan exits the stadium.[24]

6. The Puttaswamy proportionality test applied to institutional accountability

The *Puttaswamy* proportionality test provides the constitutional framework for evaluating whether AI-driven data collection and decision-making in sports meets fundamental rights standards.[25] Applying each prong of the test to institutional accountability produces the following analysis.

Legality. The restriction on privacy must be backed by law. Currently, sports organisations that collect athlete biometric data rely on contractual consent rather than specific statutory authorisation. The DPDPA provides a general legislative framework, but it does not specifically authorise or regulate biometric data collection in employment or sporting contexts. The NSG Act does not address data collection at all.[26]

Legitimate aim. The purpose of AI-driven data collection in sports can be characterised as performance optimisation, injury prevention, fair competition, and spectator safety. These are legitimate aims. However, when the same data is repurposed for commercial exploitation, transfer market valuations, or third-party marketing, the legitimate aim shifts from athlete welfare to revenue generation, which is a weaker constitutional justification for privacy intrusion.

Proportionality. This prong requires that the scope of data collection be no more than necessary to achieve the stated aim. Continuous 24-hour biometric monitoring that tracks sleep patterns, heart rate variability, and stress markers extends well beyond what is necessary for match-day performance optimisation. The *Puttaswamy* proportionality standard requires that less intrusive alternatives be considered before more intrusive data collection is justified.

Conclusion

This article has examined institutional accountability and found that the distributed liability chain in sports AI is not addressed by any single statutory provision. The DPDPA holds data fiduciaries liable but not technology vendors whose algorithms cause the harm The IT Act provides compensation for data protection failures but not for algorithmic quality failures. The Consumer Protection Act's product liability provisions remain untested for AI software. Algorithmic bias in athlete selection, documented by Ghorbani Asiabar et al. (2025) and the Journal of Sport and Health Science systematic review (2025), can produce discriminatory outcomes that neither the DPDPA's data quality obligation nor Article 14's equality guarantee adequately addresses.

References

A. Statutes

1. The Constitution of India, 1950 (Articles 14, 21)
2. The Information Technology Act, 2000, No. 21 of 2000 (Sections 43A, 72A)
3. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rules 3, 5)
4. The Consumer Protection Act, 2019, No. 35 of 2019 (Section 84)
5. The Digital Personal Data Protection Act, 2023, No. 22 of 2023 (Sections 4, 5, 6, 7, 8, 9, 10, 17)
6. The National Sports Governance Act, 2025, No. 25 of 2025 (Sections 15, 17)

[23]Face Recognition Threatens to Replace Tickets, ID at Sports Events, ACLU (Dec. 17, 2024), https://www.aclu.org/news/privacy-technology/face-recognition-threatens-to-replace-tickets-id-at-sports-events-and-beyond.

[24]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, S. 8(7), INDIA CODE (2023) (erasure when purpose no longer served).

[25]Justice K. Puttaswamy (Retd.) v. Union of India, (2017) 10 C.C. 1 (India).

[26]The Sports Governance Act 2025: A Shift Toward Transparency, Accountability & Anti-Corruption, LLOYD L. COLLEGE (Jan. 19, 2026), https://www.lloydlawcollege.edu.in/blog/sports-governance-act.html.

B. Books

1. Chesterman, Simon, *We, the Robots: Regulating Artificial Intelligence* (Cambridge University Press, 2021)
2. Brownsword, Roger, *Law, Technology and Society: Re-Imagining the Regulatory Environment* (Routledge, 2019)

C. Journal Articles

1. Andrews, David L. et al., 'Big Data, Sport and Privacy' (2019) 24 Sport, Education and Society 1
2. Ethical Bias in AI-Driven Injury Prediction in Sport: A Narrative Review of Athlete Health Data, Autonomy and Governance (2025) 6 AI 283