AI in Sports: Applications, Data Collection and the Athlete's Position

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*

1. The AI-driven sports ecosystem: scope and scale

The integration of AI in sports is not a peripheral development. It has restructured how athletes train, how teams 'strategies, how injuries are predicted and prevented, how talent is identified, and how fans consume sporting content. The Indian sports technology market alone is projected to grow to over USD 1.4 billion by 2033, driven by wearables, predictive analytics platforms, and data-driven decision-making tools.[1] Major Indian leagues including the IPL, Pro Kabaddi League (PKL), and Indian Super League (ISL) have already integrated GPS vests, AI-powered analytics dashboards, and real-time performance monitoring into their operations.[2]This chapter maps the specific AI technologies deployed across the Indian sports ecosystem, examines the data they collect and how that data flows through institutional structures, analyses the contractual frameworks within which athletes consent to data collection, and identifies the legal vulnerabilities that arise from the power imbalance between athletes and the organisations that employ them.

[1]The Indian Sports Technology Market Is Projected to Grow to Over USD 1.4 Billion by 2033, cited in Outlook India Hub4SportsTech (June 20, 2025).

[2]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. (visited on 16/03/2026 10:18 a.m)

2. Wearable devices and biometric monitoring systems

The most direct interface between AI and the athlete's body is the wearable device. Modern sports wearable's are not simple fitness trackers. They are sophisticated data collection instruments that capture physiological, biomechanical, and neurological information continuously throughout training and competition.[3]

GPS-embedded compression vests are now standard equipment in Indian cricket. The Indian cricket team uses these vests to monitor players' running distance, sprint effort, and heart rate during training sessions and match play.[4] The data collected through these vests feeds into AI algorithms that model training load, predict fatigue thresholds, and recommend recovery schedules. IPL franchises use similar technology, with AI systems processing wearable sensor data to create personalised training and recovery plans tailored to each player.[5]

Several India-based companies have entered this space. STATSports provides scientifically validated GPS wearable systems specifically designed for cricket teams, with data processed through their Sonra software platform.[6]StanceBeam, an Indian company, manufactures smart cricket bat sensors that attach to the bat handle and capture bat speed, swing angle, impact position, and shot timing data, processed through cloud-based AI analytics.[7] Str8bat, another Indian venture, offers an IoT-enabled wearable sensor for bats that has recorded and analysed over 2 million shots, using machine learning algorithms to benchmark player performance.[8]Footrax, based in Ahmedabad, is developing affordable GPS trackers for grassroots athletes, while KIBI Sports in Pune combines wearables with AI to provide real-time fitness feedback.[9]

The data these devices collect is not limited to athletic performance metrics. Heart rate variability, blood oxygen saturation, sleep quality, recovery patterns, and fatigue markers are all health data. Advanced bio-monitoring systems now under development integrate EEG sensors into helmets and caps to measure concentration levels, reaction times, and stress markers.[10] This means that AI wearables in sports collect data that falls squarely within the definition of "sensitive personal data" under Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which classifies medical records, biometric information, and health conditions as sensitive personal data requiring heightened protection.[11]

The DPDPA 2023 does not create a separate category of "sensitive personal data" in the way the IT Rules 2011 and the GDPR do.[12] However, the DPDP Rules, 2025 establish standards for Data Protection Impact Assessments (DPIAs) that apply to Significant Data Fiduciaries processing large volumes of personal data.[13] Whether IPL franchises, national sports federations, or Sports Authority of India (SAI) training centres qualify as Significant Data Fiduciaries under the DPDPA is a question that will depend on the volume and nature of data they process,

[3]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/.(visited on 16/02/2026 09:03 a.m)

[4]The Indian Cricket Team Uses GPS-Embedded Compression Vests to Monitor Players' Running Distance, Sprint Effort, and Heart Rate, cited in Outlook India Hub4SportsTech (June 20, 2025).

[5]IPL 2025 and How AI is Changing the Future of Cricket, TECH COLLECTIVE (Apr. 23, 2025), https://techcollectivesea.com/2025/04/23/ipl-2025-ai-cricket/.(visited on 06/03/2026 10:03 a.m)

[6]STATSports, Athlete Monitoring for Cricket Teams, https://pro.statsportcom/cricket/ (last visited Apr. 2026).

[7]StanceBeam, Smart Cricket Bat Sensor, https://www.stancebeam.com/ (last visited Apr. 2026).

[8]Str8bat, IoT-Enabled Wearable Sensor for Cricket, https://medium.com/@hybrid.minds/str8bat-transforming-cricket-with-iot-and-analytics-3d260951c4d9.

[9]Footrax (Ahmedabad), GPS Trackers for Grassroots Athletes; KIBI Sports (Pune), AI-Powered Real-Time Fitness Feedback, cited in Outlook India Hub4SportsTech (June 20, 2025).

[10]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. (visited on 06/02/2026 10:45 a.m)

[11]The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3.

[12]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, S.S. 4-5, INDIA CODE (2023).

[13]The Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology Notification (Nov. 13, 2025).

but the scale of biometric data collection in professional sports suggests that at least the larger organisations will fall within this classification.[14]

3. AI-driven injury prediction and talent identification

Beyond performance monitoring, AI is increasingly used for two high-stakes functions that directly affect athletes' careers and livelihoods: injury prediction and talent identification. Injury prediction systems combine historical injury data, training load metrics, biomechanical analysis, and real-time physiological data to estimate the probability that a specific athlete will suffer a specific type of injury within a given timeframe. Industry reports indicate that knee and ankle injuries among Indian football and cricket players have surged by 500% in recent years, while anterior cruciate ligament (ACL) tears have risen by 400%.[15]

In the IPL, AI injury prediction models use convolutional neural networks (CNNs) to detect body posture, movement patterns, and player fatigue from training and match videos. K-Means clustering algorithms group players based on fitness levels or fatigue patterns. Regression models predict recovery time or performance loss after injury.[16] If the prediction is wrong and the player loses match time unnecessarily, the question of who bears responsibility for the error becomes legally relevant.

Talent identification algorithms create similar legal exposure. AI systems now analyse performance data from junior-level competitions, domestic leagues, and training centres to identify players with potential for professional or international selection. These algorithms process batting averages, bowling speeds, fielding metrics, fitness data, and in some cases behavioural indicators to generate talent rankings and selection recommendations. When these algorithms exhibit bias, whether through training data that underrepresents certain demographics, geographies, or playing styles, the resulting selection decisions can discriminate against athletes from particular backgrounds without any human selector being aware that bias is operating in the system.[17]Wachter, Mittelstadt, and Floridi (2017) demonstrated that the GDPR does not provide a meaningful right to explanation for automated decisions. Under Article 22 of the GDPR, individuals have the right not to be subject to decisions based solely on automated processing that produce legal effects.[18] The DPDPA 2023 does not contain an equivalent to GDPR Article 22. Indian law currently provides no statutory right for an athlete to challenge or obtain an explanation for an AI-generated selection recommendation that adversely affects their career.

4. The contractual framework: how athletes consent to data collection

The legal architecture for athlete data collection in India operates primarily through contract rather than statute. Athletes at the professional level, including IPL contracted players, ISL footballers, PKL kabaddi players, and athletes in SAI training centres, typically sign agreements that include clauses authorising the collection, processing, and sharing of their personal and performance data. These clauses are embedded in broader employment or participation contracts and are rarely the subject of individual negotiation.

Banerjee (2026) examined how the DPDPA interacts with these contractual arrangements and concluded that athletes qualify as "data principals" under the Act, which gives them statutory rights to consent, access, correction, and erasure of their personal data.[19] A kabaddi player selected for a national training camp is unlikely to refuse biometric monitoring when compliance is presented as a condition of participation.

[14]Riya Rajkumar Sharma, How India's New Data Protection Laws Will Impact the Sports and Gaming Industry, LAWINSPORT (July 17, 2025), https://www.lawinsport.com/topics/item/how-indias-new-data-protection-laws-will-impact-the-sports-and-gaming-industry. (visited on 16/02/2026 10:03 a.m)

[15]Knee and Ankle Injuries Among Indian Football and Cricket Players Have Surged by 500% in Recent Years; ACL Tears Have Risen by 400%, cited in Outlook India Hub4SportsTech (June 20, 2025).

[16]AI and Data Science in IPL in 2026, CREDO SYSTEMZ (Jan. 3, 2026), https://www.credosystemz.com/blog/powering-the-pitch-the-impact-of-ai-and-data-science-in-the-ipl/. (visited on 09/02/2026 11:03 a.m)

[17]Sandra Wachter et al., why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR, 7 INT'L DATA PRIVACY L. 76 (2017).

[18]Regulation (EU) 2016/679, art. 22 (General Data Protection Regulation).

[19]Chirayato Banerjee, Owning the Numbers: India's New Legal Framework for Athlete Data Control (Part 1), LAWINSPORT (Mar. 11, 2026), https://www.lawinsport.com/topics/item/owning-the-numbers-indias-new-legal-framework-for-athlete-data-control-part-1.

The DPDPA requires that consent be "free, specific, informed and unambiguous" and given through a "clear affirmative action."[20] The question is whether consent embedded in a standard-form contract, offered on a take-it-or-leave-it basis to an athlete whose livelihood depends on acceptance, meets this standard.

Kwon (2025) described this as the problem of "athlete data sovereignty," noting that although biometric and performance data originates from athletes' bodies, legal ownership remains uncertain because contractual arrangements typically assign data rights to the employer or organisation.[21] Osborne and Cunningham (2017) argued earlier that the absence of sport-specific data protection legislation leaves athletes exposed to exploitation, a concern that remains relevant despite the DPDPA's enactment because the Act is sector-neutral and does not contain provisions tailored to the specific vulnerabilities of athlete-employer relationships.[22]

The NSG Act 2025 does not resolve this gap. While the Act mandates that recognised sports organisations establish ethics committees, grievance redressal mechanisms, and athlete welfare measures,[2324] it does not specifically require these organisations to adopt data protection policies, obtain DPDPA-compliant consent for biometric monitoring, or provide athletes with transparency about how their data is used, shared, or monetised. The S&R Associates analysis (2025) noted that while the NSG Act creates institutional structures for athlete welfare, it "does not include a clause for enforceable rights" and maintains a "governance-first, athlete-second strategy."[25]

5. AI-driven fan engagement and spectator data collection

The data collection ecosystem in sports extends beyond athletes to fans and spectators. Sports organisations use AI-driven tools to analyse fan behaviour, personalise advertising, manage ticketing, deploy facial recognition in stadiums, and create digital engagement platforms that capture behavioural data at scale.

Facial recognition technology has become a standard feature in major sports venues globally. By 2025, Wicket, a leading facial authentication provider, supported more than 50 professional teams across the NFL, NBA, NHL, MLB, MLS, and other leagues.[26] The technology enables fans to enter stadiums without physical tickets by linking their biometric facial data to their ticketing accounts. At the LA Clippers' Intuit Dome, which opened in 2024, approximately 75% of fans enrolled in the stadium's facial authentication system by the end of an average game.[27]

In India, while facial recognition deployment in sports stadiums is less advanced than in the US, the trajectory is clear. Indian stadiums are increasingly adopting smart ticketing, crowd management, and personalised promotional systems.[28] The Indian government has separately deployed facial recognition through the Automated Facial Recognition System (AFRS) for law enforcement, and the technology's extension to sports venues is a

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

[21]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. (visited on 11/03/2026 10:03 a.m)

[22]Barbara Osborne & Jennifer L. Cunningham, Legal and Ethical Implications of Athletes' Biometric Data Collection in Professional Sport, 28 MARQ. SPORTS L. REV. 37 (2017).

[23]The National Sports Governance Act, 2025, No. 25 of 2025, S. 15, INDIA CODE (2025).

[24]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.

[25]The National Sports Governance Act, 2025: Regulatory Developments and New Opportunities, S&R ASSOCIATES (Dec. 3, 2025), https://www.snrlaw.in/the-national-sports-governance-act-2025-regulatory-developments-and-new-opportunities/.

[26]How Facial Recognition Technology Spread Across U. Sporting Events, SPORTICO (Dec. 31, 2025), https://www.sportico.com/business/tech/2025/facial-recognition-ai-scanning-sports-teams-stadium-laws-1234880030/.

matter of when rather than whether. The legal concerns around fan data collection are distinct from athlete data concerns but equally serious. In a 2024 US class action lawsuit, plaintiffs alleged that a sports venue collected facial scans of over 100,000 visitors and shared that biometric data with third-party software providers in violation of local privacy laws.[29] The ACLU has warned that facial recognition in stadiums threatens to normalise surveillance technology that could spread beyond sports into daily life, noting that there is "a big difference between face recognition being used by you, and face recognition being used on you."[30]

Under the DPDPA 2023, fans at Indian sporting events qualify as data principals whose personal data cannot be processed without consent meeting the Act's requirements. However, the practical reality of stadium entry creates conditions similar to those affecting athletes: if a stadium deploys facial recognition as part of its entry process, a fan who objects to biometric scanning may face the choice of submitting to the scan or not attending the event. The DPDPA's consent requirement, while theoretically protective, may not function effectively in environments where refusal carries a practical penalty.

6. The data flow chain: from athlete's body to commercial exploitation

A significant gap in the current legal analysis of AI in sports is the failure to trace the complete data flow from collection to commercial exploitation. Data collected from an athlete's body through a wearable device does not stay within the club's training staff. It flows through a chain that typically involves the following nodes: the wearable device manufacturer (who may retain raw data on cloud servers), the AI analytics platform (which processes the data through proprietary algorithms), the sports organisation (which receives processed insights), the governing federation (which may require data submission for anti-doping or fitness certification purposes), broadcast and media partners (who may use performance data for commentary and graphics), and commercial sponsors (who may seek access to performance data for marketing purposes).

Each node in this chain is a potential point of data breach, unauthorised access, or purpose deviation. The DPDPA's requirement of purpose limitation under Section 5 means that data collected for injury prevention cannot be repurposed for commercial sponsorship decisions without fresh consent.

Guo et al. (2024) used stakeholder analysis to map the data governance interactions in sports and identified three primary nodes: sports organisations, technology vendors, and governing bodies.[31] Their analysis concluded that effective athlete data protection requires coordinated governance across all three nodes, which is difficult to achieve when each node operates under different contractual and regulatory frameworks. The IT Act's Section 43A creates liability for entities that fail to protect sensitive personal data,[32] and Section 72A penalises breach of confidentiality,[33] but these provisions apply to individual entities rather than to the data flow chain as a whole.

7. The Indian legal position: current protections and their limits

The constitutional foundation for athlete data protection lies in Article 21 of the Indian Constitution, which the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) interpreted to include the right to privacy as a fundamental right.[34] The Court's four-part proportionality test, requiring legality, legitimate aim, proportionality, and procedural safeguards, applies to any restriction on privacy by state or private actors. In *Ritesh Sinha v. State of Uttar Pradesh* (2019), the Court specifically addressed biometric data collection, holding that compelled collection of biometric information engages the right to privacy.[35]

The DPDPA 2023 provides the statutory framework for data protection, with Section 6 requiring consent to be free, specific, informed, and unambiguous, Section 8 imposing obligations on data fiduciaries to maintain accuracy, implement security safeguards, and delete data when the purpose has been served,[36] and Section 17

[29]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

[30]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.

[31]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.

[32]The Information Technology Act, 2000, No. 21 of 2000, S. 43A, INDIA CODE (2000).

[33]The Information Technology Act, 2000, No. 21 of 2000, S. 72A, INDIA CODE (2000).

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

[35]Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 C.C. 1 (India).

[36]The Digital Personal Data Protection Act, 2023, No. 22 of 2023, S. 8, INDIA CODE (2023).

granting the Central Government power to exempt state instrumentalities from the Act's obligations.[37] The DPDP Rules, 2025 operationalise these provisions with full compliance expected by May 2027.

The NSG Act 2025 creates institutional governance structures for sports bodies but, as the Lloyd Law College analysis (2026) noted, the Act "does not include a clause for enforceable rights" for athletes and "targets federations rather than athletes." The Act's silence on data protection, AI governance, and technology regulation means that the legal protection of athlete data depends entirely on the general provisions of the DPDPA and the IT Act, neither of which was drafted with the specific vulnerabilities of the sports industry in mind.

Indian courts have begun recognising AI-related privacy violations. In *Arijit Singh v. Codible Ventures LLP* (2024), the Bombay High Court restrained defendants from using AI to synthesise a singer's voice.[38] In *Jackie Shroff v. The Peppy Store* (2024), the Delhi High Court restrained exploitation of personality rights through AI.[39] While these cases involve entertainment industry figures rather than athletes, they establish judicial willingness to protect individuals against AI-driven exploitation of personal attributes, including voice, likeness, and biometric characteristics, a precedent directly transferable to athlete data rights.[40]

Conclusion

The AI technologies now embedded in Indian sports, from GPS-embedded compression vests used by the Indian cricket team to smart bat sensors manufactured by Indian companies like StanceBeam and Str8bat, to AI-powered injury prediction models using convolutional neural networks and K-Means clustering algorithms in the IPL. It traced the data flow from the athlete's body through a chain of institutional actors, wearable manufacturers, AI analytics platforms, clubs, federations, broadcasters, and sponsors, each representing a potential point of data breach, purpose deviation, or unauthorised commercial exploitation. The Indian sports technology market's projected growth to USD 1.4 billion by 2033 indicates that this integration will only deepen.

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)

B. 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

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

[38]Arijit Singh v. Codible Ventures LLP and Others (2024) (Bombay High Court).

[39]Jaikishsan Kakubhai Saraf alias Jackie Shroff v. The Peppy Store & Ors (2024) (Delhi High Court).

[40]Artificial Intelligence 2025 - India, CHAMBERS AND PARTNERS (May 22, 2025), https://practiceguidechambercom/practice-guides/artificial-intelligence-2025/india/trends-and-development