Summary of DSCI's submissions on the Preliminary Draft of the Regulations for Use of Artificial Intelligence in Courts, 2026

The Data Security Council of India (DSCI) has provided feedback on the preliminary draft of the Regulations for Use of Artificial Intelligence in Courts, 2026 (Draft Regulations). DSCI appreciates the objective of governing judicial AI through principles of human primacy, transparency, accountability, data protection, and judicial independence, and welcomes the proposed governance bodies (the Apex Body and AI Secretariats) as well as the alignment with the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000.

While supporting these objectives, DSCI has offered targeted recommendations to ensure the framework is consistent, secure, and auditable in implementation across Courts.

Regulation-by-Regulation Feedback

Regulation 3(zh) read with Regulation 48: Definition and ambit of "sensitive judicial data"

Concern: The definition covers both personally identifiable information and Court-related information whose disclosure may cause harm, but it draws no distinction between categories such as sealed documents and publicly available case information. This may result in disproportionate obligations under Regulation 48 of the Draft Regulations, where lower-sensitivity data is overprotected while higher-sensitivity data is inadequately safeguarded. Sensitivity is also time-dependent, and the uniform approach sits uneasily with Indian procedural law, which recognizes varying levels of confidentiality, such as the in-camera safeguards under Sections 366(2) and 366(3) of the Bharatiya Nagarik Suraksha Sanhita, 2023.

Recommendation: Introduce a tiered classification of sensitive judicial data based on the potential harm from unauthorized disclosure, modification, or misuse, distinguishing, at a minimum, publicly available case information from data concerning victims of crimes against women and children. Regulation 48 could then apply proportionate security obligations to each tier rather than a single uniform standard.

Regulation 7: Transparency and explainability

Concern: DSCI supports heightened scrutiny of high-risk applications affecting liberty and recognizes AI's potential to strengthen judicial reasoning and access to justice. However, it seeks clarity on how transparency and explainability obligations apply to Large Language Model (LLM)-based systems, which operate through probabilistic inference rather than discrete, auditable decision pathways. Requirements premised on access to model internals or architectural disclosure may be technically infeasible for LLMs and could exclude capable, well-tested systems on grounds unrelated to their fitness for judicial use.

Recommendation: Reorient the provisions around functional explainability rather than architectural transparency, requiring documented disclosure of an AI System's purpose, capabilities, limitations, and known failure modes in a verifiable form. This should be embedded through mechanisms already contemplated in the Draft Regulations, namely the Technical and Ethical Impact Assessment (Regulation 35 of the Draft Regulations), the AI Register maintained as a living record, and disclosure to affected parties on request. Where a system cannot meet these requirements for a given application, its use should require documented approval from the Designated Officer with reasons recorded.

Regulation 8: Accountability

Concern: DSCI supports central human accountability but notes that the "reasonable care" standard under Regulation 8(3) of the Draft Regulations is undefined and does not reflect the materially different roles of judicial and non-judicial officers; non-judicial officers may be held to standards of legal judgment outside their function. Separately, while Regulation 46(4)(i) of the Draft Regulations indemnifies Courts against vendor-introduced defects, this protection does not extend to individual officers, who may remain personally exposed for errors they could not reasonably detect, risking a chilling effect on AI adoption.

Recommendation: Adopt differentiated accountability standards. For judicial officers, "reasonable care" could be defined by reference to a documented verification protocol that requires legal evaluation and recorded reasoning, rather than a technical audit. For non-judicial officers, consequential AI-assisted outputs should require review and sign-off by a Designated Officer. Regulation 46 of the Draft Regulations should be clarified so that indemnification does not displace vendor accountability for defects in their own systems, and the Apex Body should develop training and capacity-building for officers.

Regulation 15: Cyber security

Concern: The Draft Regulations adopt the IT Act, 2000 definition of "cyber security" as the baseline, which addresses infrastructure-level threats but not the distinct, model-layer vulnerabilities arising from the design, training, and operation of AI systems, such as prompt injection, data and training-set poisoning, model extraction, and adversarial inputs. Given the sensitivity of judicial data, a compromised or manipulated AI output carries juridical, not merely technical, consequences, and the current gap is structural rather than merely a matter of degree.

Recommendation: Expand Regulation 15 of the Draft Regulations to establish a three-dimensional standard of security, safety, and trustworthiness as co-equal and interdependent requirements, and require that AI Systems satisfy both conventional cybersecurity requirements and an AI Security, Safety, and Trustworthiness Baseline issued by the Apex Body.

Regulation 38: Audits

Concern: Regulation 38(2) of the Draft Regulations mandates in-house audits only and prohibits the external sharing of source code, algorithms, or datasets. The specialised expertise required for adversarial testing, bias detection, and deep-learning model auditing is highly niche, and it is unclear whether every AI Secretariat, or even the Apex Body, currently has the internal capability to conduct such audits to the required standard.

Recommendation: Amend Regulation 38(2) of the Draft Regulations to permit audits by third-party auditors empaneled by the Apex Body, subject to defined confidentiality and access-control protocols, with empanelment criteria based on demonstrated expertise in AI governance, security, and privacy, and provision for periodic review.

Regulation 46(4)(j): Sovereign cloud and infrastructure agreements

Concern: The requirement for on-premises or sovereign-cloud deployment treats physical location as a proxy for security, whereas the outcomes that matter (data ownership, controlled and auditable access, and protection against misuse) can also be achieved through contractual, technical, and governance controls. Clarity is needed on the applicable criteria, standards, and certifying authority; whether qualifying infrastructure, such as government community clouds, can support compute-intensive AI workloads; and how interoperability and the DPDP Act's cross-border transfer framework will be reconciled.

Recommendation: Reframe the provision around enforceable security and control outcomes rather than physical location, requiring Courts to retain data ownership, maintain auditable access, apply strong encryption and key management, and meet a defined security baseline. Where a location-based requirement is retained, empower the Apex Body to specify certification standards, assess infrastructure capability, and prescribe common data and interface standards for interoperability, with equivalent safeguards for any processing outside India.