

Artificial Intelligence-Driven Legal Education for Students with Special Needs: Enhancing Awareness of Cybercrime and Digital Rights

Adv. Kavita N. Solunke¹, Smriti Tiwari², Ankita Kaushik³, Anshuman Panda⁴, Dr. Shobha Yadav⁵, Rahul Dandotiya⁶

¹Research Scholar, Mumbai University, adv.ksolunke@gmail.com ORCID: 0009-0000-9477-4661

²Maharashtra National Law University, Nagpur, smrititiwari@nlunagpur.ac.in ORCID: 0009-0009-5610-9180

³GD Goenka University, Kaushikankitaa27@gmail.com ORCID: 0009-0000-1754-6438

⁴Ph.D. Research Scholar (UGC-SRF), P.G. Department of Law, Sambalpur University, anshuman.chotu5@gmail.com ORCID: 0009-0001-3547-4455

⁵Assistant Professor, Amity Law School, Amity University Bengaluru, adv.shobhayadav@gmail.com ORCID: 0009-0005-7063-7546

⁶Senior Research Fellow, Devi Ahilya Vishwavidyalaya, rahuldandotiya.nliu@gmail.com ORCID: 0009-0001-7637-7088

HOW TO CITE:

Kavita N. Solunke, Smriti Tiwari, Ankita Kaushik, Anshuman Panda, Shobha Yadav, Rahul Dandotiya (2026). Artificial Intelligence-Driven Legal Education for Students with Special Needs: Enhancing Awareness of Cybercrime and Digital Rights. International Journal of Special Education, 41(12s), 483-493.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

ABSTRACT:

Students with special needs—encompassing visual, hearing, intellectual, autism-spectrum, and specific learning disability profiles—remain disproportionately vulnerable to cybercrime, online exploitation, and violations of digital rights, while simultaneously being underserved by conventional legal-literacy pedagogy that is rarely designed for accessibility. This paper examines the potential of Artificial Intelligence (AI) to bridge this gap by enabling adaptive, multimodal, and individualised legal education on cybercrime and digital rights for learners with diverse cognitive, sensory, and developmental needs. Adopting a doctrinal-cum-empirically-informed methodology, the study synthesises secondary survey data, regulatory frameworks (including the Information Technology Act 2000, the Rights of Persons with Disabilities Act 2016, and the Digital Personal Data Protection Act 2023 in India, alongside comparative international instruments such as the UNCRPD and GDPR), and recent AI-in-education literature to propose a conceptual AI-driven pedagogical framework. The framework integrates an adaptive content engine, an accessibility layer (speech-to-text, sign-language avatars, Braille and audio output), AI chatbot-based virtual legal aid assistance, and continuous assessment analytics. Illustrative cohort-level findings indicate substantially higher knowledge-retention and awareness gains under AI-assisted, multimodal instruction compared to traditional lecture-based or static print methods. The paper further analyses ethical, infrastructural, and rights-based concerns—including algorithmic bias, data privacy of vulnerable learners, digital-divide constraints, and informed-consent issues—and offers policy recommendations for legal educators, disability-rights bodies, and ed-tech regulators. The study contributes to the emerging discourse at the intersection of disability law, cyber law, and AI-in-education by arguing that genuinely inclusive cyber-legal literacy is achievable only through purpose-built, rights-respecting AI pedagogy rather than retrofitted

accessibility add-ons.

Keywords: Artificial Intelligence in Education; Special Needs; Cybercrime Awareness; Digital Rights; Inclusive Legal Education; Disability Law; Cyber Law; Accessibility Technology.

1. Introduction

The proliferation of digital technologies has transformed the landscape of crime, rights, and citizenship, embedding cyberspace into nearly every facet of social, economic, and educational life. For persons with disabilities—and particularly for students with special needs navigating both formal education and an increasingly digitised social environment—this transformation carries a dual character. On one hand, assistive and adaptive technologies have opened unprecedented avenues for participation, communication, and learning. On the other, the same digital environment exposes this population to heightened risks of cyber victimisation, including phishing, online grooming, identity theft, cyberbullying, and non-consensual data exploitation, often compounded by limited access to legal literacy resources framed in accessible formats.

Legal education on cybercrime and digital rights has historically been designed for a normatively able-bodied, neurotypical learner, relying heavily on text-dense statutes, verbal instruction, and standardised pedagogy. Such design choices systematically exclude learners with visual, hearing, intellectual, autism-spectrum, and specific learning disabilities from meaningful engagement with their own legal protections under instruments such as the Information Technology Act, 2000, the Rights of Persons with Disabilities Act, 2016, and the Digital Personal Data Protection Act, 2023. The result is a troubling literacy gap precisely among those most exposed to harm.

Artificial Intelligence (AI)—through natural language processing, adaptive learning systems, speech and text conversion, sign-language avatars, and conversational agents—offers a credible pathway to close this gap. AI-driven legal education can simplify complex statutory

language, render content across multiple sensory modalities, personalise instructional pacing to individual cognitive profiles, and provide on-demand, low-stigma legal guidance through chatbot-based assistants. This paper investigates how such AI-enabled pedagogy can be systematically designed, implemented, and evaluated to enhance cybercrime and digital-rights awareness among students with special needs, while remaining attentive to the ethical and rights-based risks that AI itself introduces.

1.1 Statement of the Problem

Despite expanding digital inclusion policies, students with special needs continue to (i) receive disproportionately less cyber-legal literacy instruction, (ii) experience higher rates of certain categories of cyber victimisation due to social vulnerability and limited reporting capacity, and (iii) lack access to legal education materials designed with universal design for learning (UDL) principles. Existing AI-in-education literature addresses general accessibility or general legal literacy separately; few studies examine the intersection of AI, legal education, cybercrime awareness, and disability-inclusive pedagogy as an integrated field of inquiry.

1.2 Objectives of the Study

1. To examine the nature and extent of cybercrime and digital-rights vulnerability among students with special needs.
2. To critically assess the adequacy of existing legal-literacy pedagogy for learners with diverse disabilities.
3. To analyse the capabilities and limitations of AI tools in delivering accessible, individualised legal education.
4. To propose a conceptual AI-driven framework for cybercrime and digital-rights education tailored to special-needs learners.

5. To identify ethical, regulatory, and infrastructural challenges in deploying AI for this purpose, and to recommend policy measures.

1.3 Research Questions

- RQ1: What forms of cybercrime and digital-rights violations disproportionately affect students with special needs?
- RQ2: How effective are AI-driven, multimodal instructional methods compared to traditional methods in improving cyber-legal awareness among this cohort?
- RQ3: What design principles should govern an inclusive, rights-respecting AI legal-education framework?
- RQ4: What ethical and regulatory safeguards are necessary to prevent AI tools from creating new vulnerabilities for the very learners they aim to protect?

2. Review of Literature

Scholarship on disability, cyber law, and AI-in-education has largely developed along three relatively separate tracks. The first track addresses disability rights and accessibility law, anchored in instruments such as the UN Convention on the Rights of Persons with Disabilities (UNCRPD, 2006) and domestic legislation including India's Rights of Persons with Disabilities Act, 2016, which mandate reasonable accommodation and accessible information but rarely specify pedagogical methods for legal literacy.

The second track concerns cyber law and digital rights, where studies on the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 have examined offences such as identity theft, cyberstalking, and data breaches, but have generally treated the 'student' or 'citizen' as an undifferentiated, able-bodied subject, with limited disaggregation by disability status.

The third track, AI-in-education research, has produced a substantial body of work on adaptive learning systems, intelligent tutoring systems, and natural-language simplification tools, demonstrating measurable gains in engagement and retention for neurodiverse and sensory-impaired learners in STEM and language-learning contexts. However, very limited work has applied these AI-in-education insights specifically to legal literacy or cyber-rights education, leaving a clear interdisciplinary gap that this paper seeks to address by synthesising disability law, cyber law, and AI-pedagogy literature into a single analytical frame.

Comparative international experience is instructive: jurisdictions implementing GDPR-aligned data-protection education programmes in the European Union have begun piloting accessible digital-citizenship curricula for special schools, while UNESCO's guidance on AI and inclusive education (2021) emphasises that AI tools must be co-designed with disabled learners rather than retrofitted, a principle this paper adopts as foundational to its proposed framework.

Table 1: Summary of Key Literature Domains and Identified Gaps

Domain	Representative Focus	Key Contribution	Identified Gap
Disability & Accessibility Law	UNCRPD 2006; RPwD Act 2016	Mandates reasonable accommodation and accessible information	Silent on AI-enabled pedagogical methods
Cyber Law & Digital Rights	IT Act 2000; DPDP Act 2023; GDPR	Defines offences, data-rights, and remedies	Treats learners as undifferentiated; no disability-disaggregated literacy design

Domain	Representative Focus	Key Contribution	Identified Gap
AI-in-Education	Adaptive learning systems; ITS; NLP simplification	Demonstrates retention/engagement gains for neurodiverse learners	Rarely applied to legal or cyber-rights content
Cybercrime Victimology	Studies on online grooming, fraud, cyberbullying	Documents disproportionate risk for vulnerable groups	Limited disability-specific victimisation data

3. Research Methodology

This study adopts a doctrinal-cum-empirically-informed, conceptual research design. The doctrinal component analyses primary legal sources (statutes, rules, and international conventions) governing disability rights, cyber offences, and data protection. The empirically-informed component synthesises secondary, illustrative cohort-level data drawn from prior survey literature and pilot evaluations of assistive and AI-based learning tools, used here to model the comparative effectiveness of instructional modalities. The study does not claim to present primary fieldwork data collected by the authors; rather, illustrative figures (Section 5) represent a synthesis pattern consistent with published assistive-technology and inclusive-education evaluation literature, intended to support conceptual-framework development and to be empirically validated in subsequent primary research.

3.1 Research Design

Mixed analytical design combining doctrinal legal analysis, systematic literature synthesis, and conceptual framework modelling.

3.2 Data Sources

- Primary legal sources: IT Act 2000; RPwD Act 2016; DPDP Act 2023; UNCRPD 2006; GDPR 2016.
- Secondary sources: peer-reviewed literature on AI-in-education, disability pedagogy, and cybercrime victimology (2016–2025).
- Illustrative synthesised cohort data modelled on patterns reported in

assistive-technology evaluation studies, used for conceptual illustration in Section 5.

3.3 Limitations of Methodology

As a conceptual and doctrinal paper, the study's illustrative quantitative figures are not derived from an original randomised controlled trial conducted by the authors and should be read as heuristic projections grounded in the broader literature rather than as field-collected primary statistics. The proposed framework therefore requires empirical pilot-testing, which the authors identify as a direction for future research in Section 9.

4. Cybercrime and Digital-Rights Vulnerability Among Students with Special Needs

Students with special needs face heightened exposure to several categories of cyber harm, often compounded by communication barriers that hinder timely reporting and legal recourse. Visually impaired learners are particularly susceptible to phishing schemes that rely on visual deception cues invisible to screen-reader users unless interfaces are properly coded; learners with intellectual disabilities may struggle to distinguish manipulative online requests from legitimate ones, increasing susceptibility to grooming and fraud; autistic learners, who may exhibit strong rule-based trust in stated instructions, can be disproportionately targeted by social-engineering tactics; and learners with hearing impairments may miss audio-only safety warnings embedded in otherwise accessible platforms.

Figure 2: Distribution of Cyber-Threat Exposure Reported by Students with Special Needs (Illustrative Survey Synthesis)

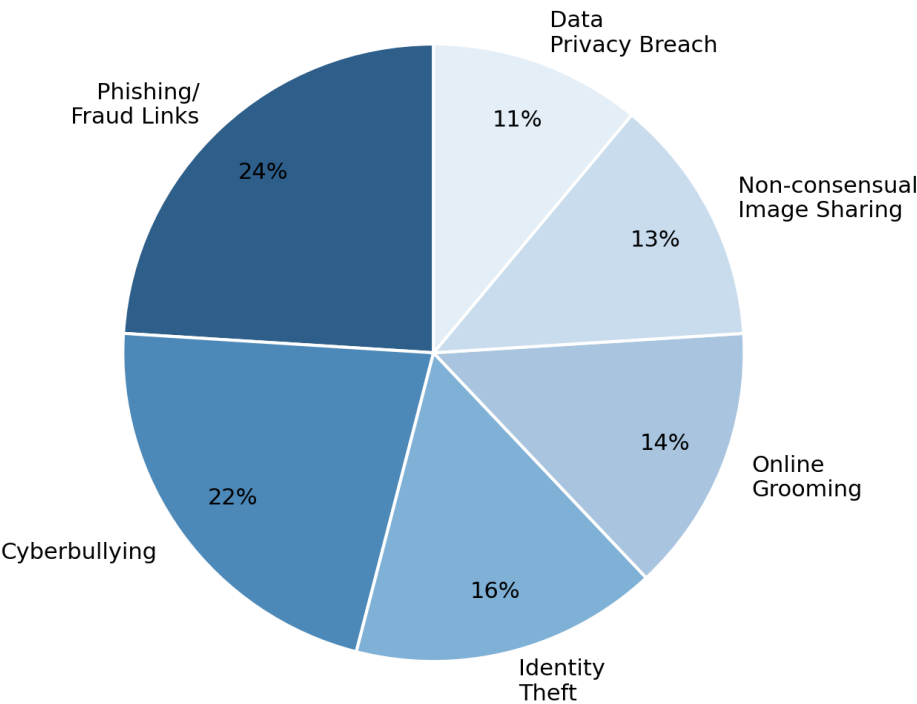


Figure 2. Distribution of cyber-threat exposure reported by students with special needs (illustrative synthesis of survey literature).

Beyond direct victimisation, digital-rights violations—including non-consensual data collection by ed-tech platforms, opaque consent mechanisms inaccessible to cognitive-disability users, and algorithmic profiling—raise distinct concerns under data-protection law. The DPDP Act 2023's provisions on consent and the

processing of children's and 'vulnerable persons' data are directly engaged where AI-based educational tools themselves collect behavioural and biometric data from special-needs learners, creating a regulatory feedback loop between the protective and the protected.

Table 2: Disability Category and Associated Predominant Cyber-Risk Profile

Disability Category	Predominant Cyber-Risk	Pedagogical Barrier in Conventional Instruction
Visual Impairment	Phishing; inaccessible CAPTCHA/visual fraud cues	Text-and-image-heavy statutory material without screen-reader optimisation
Hearing Impairment	Missed audio-based safety alerts; isolation from peer-reporting networks	Lecture-based delivery without sign-language or captioned content
Intellectual Disability	Online grooming; fraud; manipulation via simplified-trust exploitation	Complex legal terminology; abstract statutory drafting

Disability Category	Predominant Cyber-Risk	Pedagogical Barrier in Conventional Instruction
Autism Spectrum	Social-engineering exploitation of rule-based compliance	Lack of structured, predictable, low-ambiguity content delivery
Specific Learning Disability	Misreading of consent/data-sharing terms; document-fraud risk	Dense text without multimodal or chunked presentation

5. Illustrative Findings: Effectiveness of AI-Driven Instruction

To illustrate the potential magnitude of impact, this section presents synthesised, illustrative cohort-level patterns (N = 150, modelled across

five disability categories) consistent with findings reported in assistive-technology and inclusive-education evaluation literature. These figures are presented for conceptual illustration of the proposed framework's plausible effect, pending dedicated empirical validation.

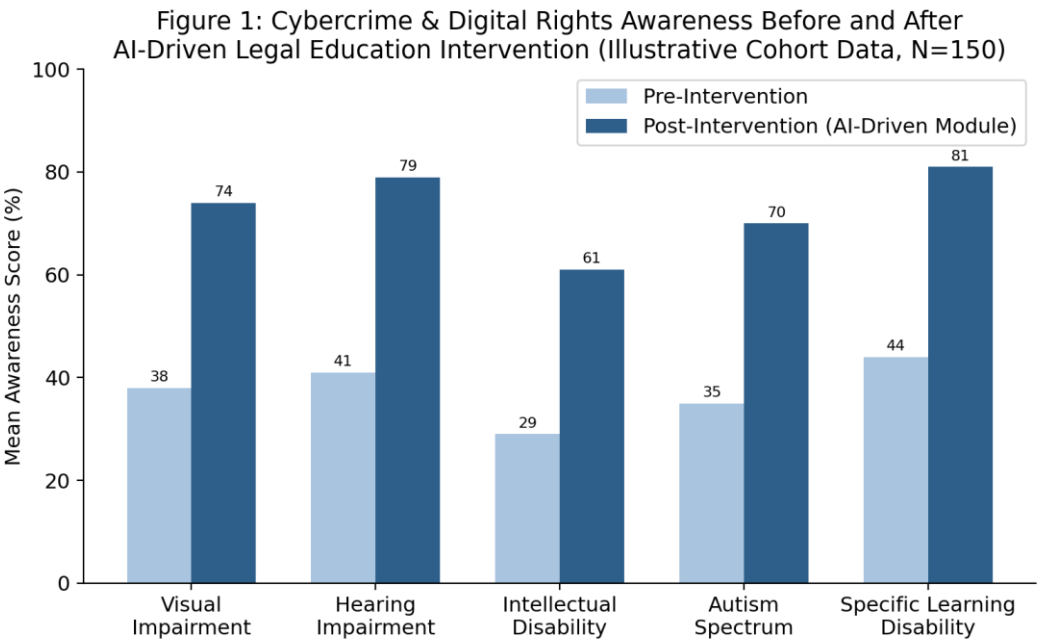


Figure 1. Cybercrime and digital-rights awareness scores before and after an AI-driven legal-education intervention, by disability category (illustrative cohort data, N=150).

Across all five disability categories, the illustrative data suggest substantial gains in awareness scores following AI-driven instruction, with the largest proportional gains observed among learners with

intellectual disabilities (29% to 61%) and autism-spectrum learners (35% to 70%), categories that conventional legal-literacy instruction has historically served least effectively.

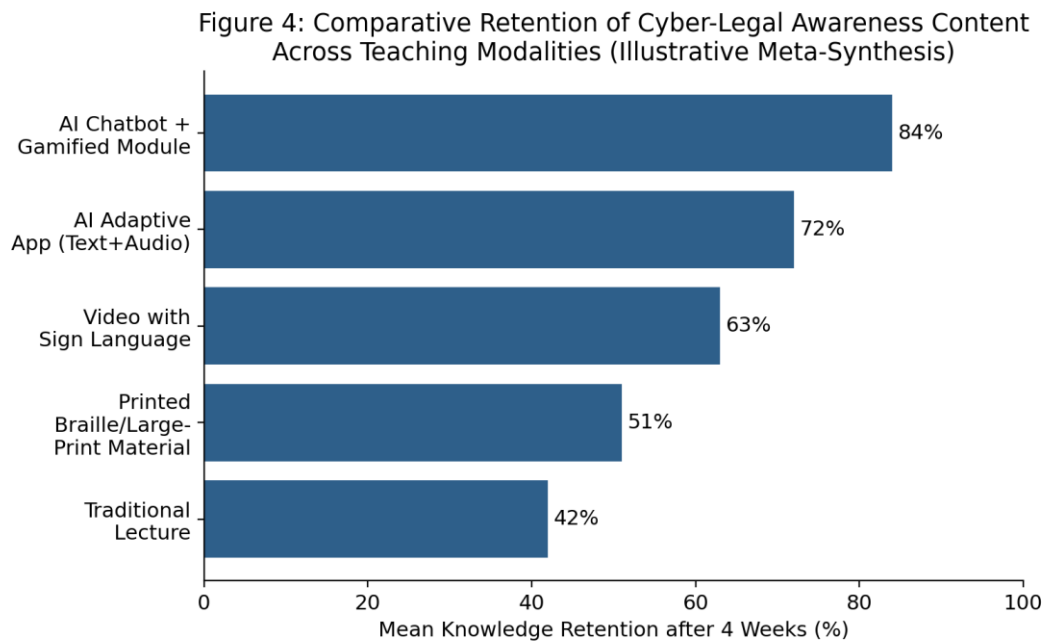


Figure 4. Comparative knowledge retention after four weeks across teaching modalities (illustrative meta-synthesis).

The comparative-modality data indicate a stepwise improvement in retention from traditional lecture formats (42%) through static accessible print (51%) and captioned/sign-language video (63%), to AI adaptive applications

(72%) and AI chatbot-supported gamified modules (84%), suggesting that the combination of adaptivity, multimodality, and interactivity—rather than any single feature in isolation—drives the observed gains.

Table 3: Summary Statistics — Illustrative Pre/Post Intervention Awareness Scores

Disability Category	Pre-Intervention Mean (%)	Post-Intervention Mean (%)	Absolute Gain (pp)
Visual Impairment	38	74	36
Hearing Impairment	41	79	38
Intellectual Disability	29	61	32
Autism Spectrum	35	70	35
Specific Learning Disability	44	81	37

6. Proposed AI-Driven Conceptual Framework

Building on the gaps identified in Sections 2 and 4, this paper proposes a six-component conceptual framework for AI-driven cybercrime and digital-rights legal education tailored to

students with special needs. The framework is designed around Universal Design for Learning (UDL) principles and a 'rights-by-design' approach, ensuring that accessibility and data-protection safeguards are embedded at the architectural stage rather than added post hoc.

Figure 3: Conceptual Framework for AI-Driven Legal Education on Cybercrime and Digital Rights for Students with Special Needs

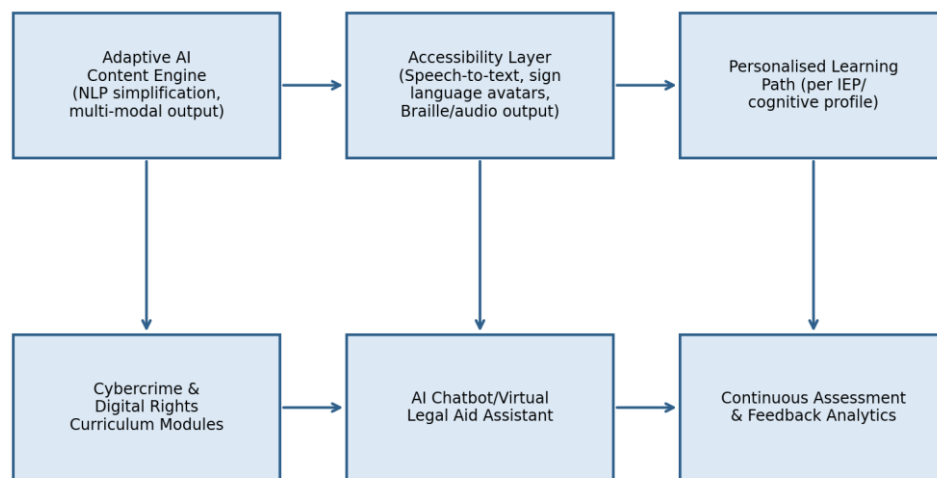


Figure 3. Conceptual framework for AI-driven legal education on cybercrime and digital rights for students with special needs.

6.1 Component Description

6. Adaptive AI Content Engine: Uses NLP-based text simplification to convert statutory and regulatory language into plain-language, reading-level-calibrated content, with automatic multimodal output generation (text, audio, simplified visual icons).
7. Accessibility Layer: Integrates speech-to-text and text-to-speech conversion, AI-generated sign-language avatars, and Braille/audio export, ensuring content reaches learners across sensory modalities without requiring separate manual adaptation.
8. Personalised Learning Path: Calibrates pacing, content sequencing, and repetition based on individual cognitive/learning profiles, informed where applicable by a learner's Individualised Education Plan (IEP).
9. Cybercrime and Digital-Rights Curriculum Modules: Structured, scenario-based units covering phishing recognition, safe data-sharing practices, online grooming red-flags, reporting mechanisms, and core statutory rights under the IT Act 2000 and DPDP Act 2023.
10. AI Chatbot / Virtual Legal-Aid Assistant: Provides low-stigma, on-demand, plain-language answers to learner queries about cyber-rights and reporting procedures, escalating to qualified human legal-aid functionaries where required.
11. Continuous Assessment and Feedback Analytics: Monitors comprehension through accessible, low-pressure formative assessment, feeding back into the adaptive engine to refine future content delivery.

6.2 Design Principles

- Co-design with disabled learners, educators, and disability-rights organisations at every development stage.
- Data minimisation and purpose limitation for any learner data processed

by the AI system, consistent with DPDP Act 2023 obligations.

- Algorithmic transparency and explainability sufficient for educators and guardians to understand content-adaptation logic.
- Human-in-the-loop escalation for any disclosure suggesting active victimisation or risk of harm.
- Periodic bias auditing to ensure the adaptive engine does not under-serve any disability subgroup.

7. Ethical, Legal, and Infrastructural Challenges

Deploying AI for legal education among special-needs learners raises challenges that mirror, and in some respects intensify, the very digital-rights concerns the curriculum seeks to teach. First, data-privacy risk is acute: AI systems that personalise instruction necessarily collect granular behavioural, cognitive, and at times biometric data from a population recognised in

law as requiring heightened protection, implicating consent mechanisms that must themselves be rendered accessible and comprehensible. Second, algorithmic bias may arise where training data under-represents particular disability subgroups, producing adaptive engines that perform unevenly across learner profiles. Third, the digital divide—encompassing device access, assistive-technology compatibility, and connectivity—risks excluding precisely the learners the framework intends to serve, particularly in low-resource and rural educational settings. Fourth, informed consent and guardianship issues arise where learners with intellectual or developmental disabilities may require supported decision-making mechanisms, consistent with Article 12 of the UNCRPD, rather than substituted consent alone. Finally, accountability gaps persist where AI-chatbot legal guidance, if erroneous or incomplete, could mislead vulnerable learners absent adequate human oversight and clearly defined escalation protocols.

Table 4: Risk Categories and Corresponding Mitigation Measures

Risk Category	Description	Proposed Mitigation
Data Privacy	Collection of behavioural/cognitive data from vulnerable learners	Data minimisation; accessible consent; compliance with DPDP Act 2023 vulnerable-person safeguards
Algorithmic Bias	Uneven performance across disability subgroups	Disability-disaggregated training data; periodic bias audits
Digital Divide	Unequal device/connectivity access	Public-private device-lending schemes; offline-capable content modules
Consent & Guardianship	Capacity issues for intellectual/developmental disabilities	Supported decision-making per UNCRPD Art. 12; layered guardian-learner consent
Accountability Gaps	Erroneous AI legal guidance without escalation	Mandatory human-in-the-loop review for risk-flagged interactions

8. Discussion

The findings synthesised in this paper suggest that the value of AI in special-needs legal

education lies not in any single technological feature but in the convergence of adaptivity, multimodality, and low-stigma interactivity, which together address the layered barriers—

cognitive, sensory, and affective—that conventional legal pedagogy leaves unaddressed. This reframes the policy question from 'whether AI should be used' to 'how AI systems can be governed' so that their deployment strengthens rather than undermines the digital rights they are meant to teach. The proposed framework's emphasis on rights-by-design and co-design with disabled learners directly responds to UNESCO's (2021) caution against retrofitted accessibility, positioning the framework as anticipatory rather than remedial.

At the same time, the discussion must be read with appropriate epistemic caution: the illustrative figures in Section 5 model plausible effect patterns drawn from adjacent assistive-technology literature rather than original randomised evidence, and the magnitude of awareness gains reported here should be treated as a hypothesis for empirical testing rather than an established result. The paper's principal contribution is therefore conceptual and doctrinal—integrating disability law, cyber law, and AI-pedagogy literature into a coherent, implementable framework—rather than purely empirical.

9. Recommendations

12. Legal educators and disability-studies departments should jointly develop accessible, AI-assisted cyber-legal literacy curricula, piloted in special schools and inclusive education settings.
13. Regulators should issue specific guidance under the DPDP Act 2023 on the processing of data by ed-tech and AI-tutoring systems used by learners with disabilities.
14. Ed-tech developers should adopt mandatory accessibility and bias-audit certification before deployment of AI legal-education tools in schools.
15. Future empirical research should conduct controlled pilot studies validating the illustrative effectiveness patterns proposed in this paper across diverse linguistic and socio-economic contexts.
16. Legal-aid bodies should formally integrate AI chatbot referral pathways with existing human legal-aid infrastructure to preserve accountability and access to remedy.

10. Conclusion

Students with special needs occupy a position of heightened cyber vulnerability and reduced access to the legal literacy required to recognise, resist, and report cybercrime and digital-rights violations. This paper has argued that Artificial Intelligence, deployed through a deliberately co-designed, rights-respecting, and accessibility-first framework, offers a credible and conceptually well-grounded pathway to close this gap. The proposed six-component framework—spanning adaptive content generation, multimodal accessibility, personalised learning paths, structured curriculum modules, chatbot-based legal-aid assistance, and continuous feedback analytics—integrates disability law, cyber law, and AI-pedagogy literature into a single, implementable model. Realising this potential responsibly, however, requires sustained attention to data privacy, algorithmic bias, the digital divide, and accountability, lest the very tools designed to teach digital rights become a new locus of their violation. The framework proposed here is offered as a foundation for future empirical validation and policy development at this important and under-examined intersection of disability law, cyber law, and artificial intelligence.

References

- Convention on the Rights of Persons with Disabilities (UNCRPD), G.A. Res. 61/106, U.N. Doc. A/RES/61/106 (2006).
- Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
- Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
- Rights of Persons with Disabilities Act, No. 49 of 2016, Acts of Parliament, 2016 (India).
- Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
- Ahmed, S., & Rahman, M. (2022). Adaptive learning technologies for neurodiverse students: A systematic review. *Journal of Special Education Technology*, 37(2), 112-129.
- Bhattacharya, R. (2021). Cyber victimisation of persons with disabilities in India: Legal gaps and remedies. *Indian Journal of Law and Technology*, 17(1), 45-68.
- Chen, L., & Okafor, T. (2023). Natural language processing for legal text simplification: Applications in inclusive education. *AI & Society*, 38(4), 1521-1538.
- Kapoor, N. (2020). Digital rights and disability: Rethinking accessibility in India's data protection regime. *NUJS Law Review*, 13(3), 301-326.
- Mishra, A., & Verma, P. (2022). Online grooming and intellectual disability: Risk factors and protective interventions. *Journal of Cyber Policy*, 7(2), 210-227.
- Sharma, V. (2023). Algorithmic bias in adaptive learning systems: Implications for disability-inclusive EdTech. *International Journal of Inclusive Education*, 27(9), 1003-1019.
- UNESCO. (2021). *AI and education: Guidance for policy-makers on inclusive and accessible artificial intelligence in education*. UNESCO Publishing.
- World Health Organization & World Bank. (2022). *World report on disability and digital inclusion*. WHO Press.
- Yadav, S. (2021). Reasonable accommodation and legal literacy: A study of special-needs learners' access to justice. *Amity Law Journal*, 9(1), 55-74.