

International Journal Research Publication Analysis

Page: 01-18

ONLINE GENDER-BASED VIOLENCE IN INDIA: LEGAL PROTECTION AND THE ENFORCEMENT GAP

***Jayshree Bhanushali**

India.

Article Received: 06 August 2026

*Corresponding Author: Jayshree Bhanushali

Article Revised: 26 August 2026

India.

Published on: 16 September 2026

DOI: <https://doi-doi.org/101555/ijrpa.3947>

ABSTRACT

The rapid expansion of social media, digital communication and artificial intelligence has transformed the nature and scale of gender-based violence in India. Violence against women is no longer confined to physical spaces; it increasingly occurs through social-media platforms, messaging applications, email, online communities and other digital environments. Online gender-based violence includes cyberstalking, online sexual harassment, non-consensual dissemination of intimate images, impersonation, doxxing, threats, image-based sexual abuse, digitally facilitated extortion and technologically manipulated or synthetically generated intimate content.

India does not presently regulate online gender-based violence through a single comprehensive statute. Instead, victims rely upon a combination of provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 (BNS), the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended, and the Digital Personal Data Protection Act, 2023. The BNS expressly recognises offences such as stalking, voyeurism, sexual harassment and acts intruding upon a woman's privacy, while the IT Act addresses privacy violations and sexually explicit electronic material.

The paper argues that India's principal problem is not the complete absence of legal protection but the fragmentation and uneven enforcement of existing remedies. Victims may encounter difficulties in identifying perpetrators, preserving digital evidence, obtaining prompt removal of harmful content, navigating multiple reporting mechanisms and securing effective investigation and prosecution. The problem has become more complex with generative artificial intelligence. The 2026 amendments to the IT Rules now expressly regulate certain forms of synthetically generated information and require intermediaries to

adopt safeguards against unlawful synthetic content, including non-consensual intimate imagery.

This paper examines the existing legal framework, identifies the principal enforcement gaps and proposes a victim-centred model based upon rapid content removal, stronger intermediary accountability, specialised investigation, privacy-preserving evidence procedures and effective access to remedies.

KEYWORDS: Online Gender-Based Violence, Cybercrime, Women, Privacy, Cyberstalking, Image-Based Sexual Abuse, Deepfakes, Artificial Intelligence, IT Act, BNS, Intermediary Liability.

I. INTRODUCTION

The internet has become an essential part of modern social, educational, professional and economic life. Digital platforms have created unprecedented opportunities for communication and participation, but they have also created new environments in which violence and discrimination can occur.

Gender-based violence is increasingly capable of being initiated, amplified or permanently reproduced online. A threatening message can be sent within seconds; an intimate image can be copied thousands of times; a fake social-media profile can impersonate a victim; and an artificial-intelligence-generated image can falsely portray a person in an intimate situation without any physical contact having occurred.

The consequences, however, are not merely “virtual”.

Online abuse can affect a victim's reputation, employment, education, mental well-being, personal relationships and physical safety. Digital harassment may also escalate into offline stalking, intimidation or violence. The boundary between online and offline violence has therefore become increasingly difficult to maintain.

Indian constitutional jurisprudence provides a strong foundation for addressing these harms. Article 21 protects life and personal liberty, while the Supreme Court has interpreted privacy as encompassing decisional autonomy, dignity and informational privacy. The constitutional commitment to equality under Articles 14 and 15 further requires the legal system to respond meaningfully to gender-based discrimination and violence.

At the statutory level, India possesses several relevant laws. The BNS contains provisions concerning sexual harassment, voyeurism, stalking and intrusion upon the privacy of women.

The Information Technology Act, 2000 contains provisions addressing violation of privacy and publication or transmission of obscene and sexually explicit material in electronic form.

The IT Rules, 2021 also provide mechanisms for grievance redressal and removal of certain intimate or sexually explicit material. The Ministry of Electronics and Information Technology has specifically stated that complaints concerning revenge pornography and similar content are subject to a 24-hour removal mechanism under Rule 3(2)(b).

More recently, amendments effective in 2026 have introduced a regulatory framework concerning “synthetically generated information”, including safeguards against non-consensual intimate imagery and other unlawful synthetic content.

Despite these legal developments, an important gap remains between **legal recognition and effective protection**.

This paper therefore examines the question:

Does India's existing legal framework provide an effective and accessible remedy against online gender-based violence, or does fragmentation and weak enforcement continue to leave victims inadequately protected?

II. CONCEPTUALISING ONLINE GENDER-BASED VIOLENCE

Online gender-based violence may be understood as harmful conduct committed, facilitated or amplified through digital technologies because of a person's gender or in a manner that disproportionately affects persons on the basis of gender.

It may include:

1. cyberstalking;
2. online sexual harassment;
3. repeated unwanted digital communication;
4. threats of sexual violence;
5. non-consensual dissemination of intimate images;
6. creation of fake or impersonation accounts;
7. doxxing and publication of private information;
8. online sexual extortion;
9. morphing or manipulation of photographs;
10. AI-generated intimate images or videos;
11. coordinated online harassment; and
12. publication of sexually explicit content without consent.

The common feature of these forms of abuse is the misuse of technology to exercise power over another person.

The digital environment creates several characteristics that distinguish online violence from conventional forms of harassment.

A. Replicability

Digital material can be copied and redistributed almost instantly.

B. Persistence

Once content is uploaded, complete removal may be practically impossible because copies may exist on multiple platforms or devices.

C. Anonymity

Perpetrators can use pseudonymous accounts, temporary numbers, fake email addresses and other mechanisms to conceal their identity.

D. Scale

A single harmful post can reach thousands or millions of users.

E. Technological manipulation

Artificial intelligence can now create highly realistic images, audio and videos that falsely portray individuals.

These characteristics require legal remedies capable of responding faster than traditional criminal processes.

III. CONSTITUTIONAL DIMENSION

A. Right to Equality

Article 14 guarantees equality before law and equal protection of laws. Article 15 prohibits discrimination on specified grounds, including sex.

Online gender-based violence can reinforce structural gender inequality by discouraging women from participating in public digital spaces.

A woman who repeatedly receives sexual threats or harassment because she expresses an opinion online may ultimately withdraw from public discussion. Thus, online abuse can indirectly restrict equal participation in education, employment, politics and public discourse.

The constitutional problem is consequently larger than the individual abusive message.

It concerns whether women can participate in digital public life on terms of substantive equality.

B. Right to Privacy

The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* recognised privacy as a constitutionally protected right and connected privacy with dignity and autonomy.

This principle has direct relevance to image-based sexual abuse.

A person may choose to create or privately share an intimate image. That decision does not constitute consent to its subsequent public dissemination.

The distinction between **consent to creation** and **consent to dissemination** is therefore legally crucial.

The BNS's voyeurism provision expressly recognises this distinction. Section 77 provides that where a woman consents to the capture of an image but does not consent to its dissemination to third persons, subsequent dissemination may constitute an offence.

This is an important recognition of informational and bodily privacy in the digital context.

C. Freedom of Speech and Its Limits

Online gender-based violence also intersects with Article 19(1)(a), which protects freedom of speech and expression.

A regulatory framework cannot treat all offensive or unpopular expression as criminal.

However, constitutional freedom of speech is subject to the reasonable restrictions listed in Article 19(2), including interests such as public order, decency, morality, defamation and incitement to an offence.

The challenge is therefore to distinguish between legitimate expression and targeted conduct designed to threaten, sexually humiliate, stalk or invade another person's privacy.

A victim-centred approach must not become a mechanism for suppressing legitimate criticism or political speech. At the same time, freedom of expression cannot be used as a blanket defence for conduct that independently constitutes a criminal offence.

IV. EXISTING LEGAL FRAMEWORK IN INDIA

A. Bharatiya Nyaya Sanhita, 2023

The BNS, which replaced the Indian Penal Code as the principal substantive criminal law, contains several provisions directly relevant to online gender-based violence.

Section 75: Sexual Harassment

Section 75 criminalises specified forms of sexual harassment, including unwelcome sexual overtures, demands for sexual favours, showing pornography against a woman's will and sexually coloured remarks.

Although the provision is not specifically drafted as a “cybercrime” provision, certain prohibited conduct can occur through digital communications.

Section 77: Voyeurism

Section 77 addresses watching, capturing or disseminating images of a woman engaged in a private act. Importantly, it recognises that consent to capture does not necessarily amount to consent to dissemination.

This makes the provision particularly relevant to non-consensual intimate-image dissemination.

Section 78: Stalking

Section 78 expressly includes monitoring a woman's use of the internet, email or other electronic communication within the statutory definition of stalking.

This is significant because it recognises that stalking need not involve physical following.

Section 79: Insult to Modesty and Intrusion upon Privacy

Section 79 criminalises specified words, sounds, gestures or acts intended to insult the modesty of a woman and expressly includes intrusion upon her privacy.

These provisions provide an important criminal-law foundation for addressing digitally facilitated gender-based abuse.

V. INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act continues to play an important role in cybercrime regulation.

Section 66E addresses violation of privacy.

Sections 67 and 67A address publication or transmission of obscene and sexually explicit material in electronic form, while Section 67B specifically addresses material depicting children in sexually explicit acts. Section 67C concerns preservation and retention of information by intermediaries.

These provisions can become relevant when sexually explicit material is circulated through digital platforms.

However, the IT Act was not originally designed as a comprehensive framework for gender-based digital violence. Its provisions must therefore frequently operate alongside the BNS and intermediary regulations.

This produces a fragmented legal structure.

VI. INFORMATION TECHNOLOGY RULES, 2021

The IT Rules, 2021 represent an important component of intermediary regulation.

The Rules require intermediaries to maintain grievance-redressal mechanisms and establish processes for dealing with unlawful content.

The Ministry of Electronics and Information Technology has specifically identified revenge pornography, sexual extortion, non-consensual pornography and similar content as material for which the Rules provide a 24-hour removal mechanism following a complaint.

This mechanism is significant because criminal investigation may take considerably longer than the spread of harmful material.

A victim may therefore require two separate forms of relief:

**first, removal or restriction of access to the harmful content; and
second, investigation and prosecution of the perpetrator.**

Content removal should not replace criminal accountability, and criminal investigation should not be used as a reason to delay urgent protective measures.

VII. THE 2026 IT RULES AND SYNTHETICALLY GENERATED INFORMATION

The development of generative artificial intelligence has fundamentally changed the legal landscape.

A person can now potentially be depicted in realistic sexual imagery without the original photograph ever having contained such material.

The 2026 amendments to the IT Rules introduced provisions concerning “synthetically generated information” (SGI). The Ministry's explanatory material describes SGI as artificially or algorithmically created, generated, modified or altered audio-visual information that may appear real or authentic and portray an individual or event in a manner likely to be perceived as indistinguishable from reality.

The amended Rules specifically address unlawful synthetic content, including:

- Child sexual abuse material;
- Non-consensual intimate imagery;

- Obscene or pornographic material;
- Material invasive of another person's privacy; and
- False portrayals of a natural person's identity, voice, conduct or statements in specified circumstances.

Intermediaries that facilitate the creation or dissemination of SGI are required to deploy reasonable and appropriate technical measures to prevent specified unlawful content. Other SGI is subject to prominent labelling and provenance-related requirements.

This is a major regulatory development.

However, technological regulation will remain effective only if platforms can detect harmful material quickly and victims can access simple reporting mechanisms.

VIII. DIGITAL PERSONAL DATA PROTECTION AND PRIVACY

The Digital Personal Data Protection Act, 2023 establishes a statutory framework governing digital personal data and recognises rights including access, correction and erasure and grievance redressal.

Its relevance to online gender-based violence arises from the fact that abusive digital conduct may involve the unlawful disclosure, processing or circulation of personal information.

Doxxing provides a clear example.

A perpetrator may publish a woman's phone number, home address, workplace information or other personal details with the intention of facilitating harassment.

Data protection law can therefore complement criminal law by strengthening individual control over personal information.

However, the DPDP framework should not be treated as a complete solution to gender-based online violence. It primarily regulates processing of digital personal data and is not designed as a comprehensive criminal-law framework for harassment, threats or image-based sexual abuse.

Furthermore, the Act's provisions are subject to a phased commencement framework, with different provisions taking effect at different times following the Government's November 2025 notifications.

This makes coordination between data protection, cybercrime and criminal law particularly important.

IX. THE ENFORCEMENT GAP

The central weakness in India's framework is not necessarily the absence of laws. It is the gap between **legal entitlement and practical enforcement**.

1. Fragmentation of Remedies

A single incident may potentially involve the BNS, IT Act, IT Rules and data-protection principles.

For a legally trained professional, identifying the applicable provisions may be manageable.

For an ordinary victim, however, navigating multiple institutions can be extremely difficult.

The victim may not know whether to approach:

- The local police;
- A cybercrime police station;
- The national cyber crime reporting portal;
- The platform's grievance mechanism;
- A court; or
- Another statutory authority.

A better system should present the victim with a **single-door reporting mechanism** capable of routing the complaint to the appropriate authorities.

2. Delay in Content Removal

Digital abuse operates at internet speed, while criminal investigations operate through procedural timelines.

By the time an FIR is registered, harmful content may already have been downloaded, reposted or moved to other platforms.

The existing 24-hour mechanism for specified intimate-content complaints is therefore important, but its practical effectiveness depends upon awareness, accessibility and platform compliance.

The legal system should distinguish between:

emergency protective relief and **final adjudication of criminal liability**.

A platform can temporarily restrict access to clearly unlawful intimate material while the investigation proceeds.

3. Identification of Anonymous Perpetrators

Anonymity is one of the greatest challenges in cybercrime.

Perpetrators may use:

- Fake accounts;
- Temporary email addresses;
- Virtual numbers;
- Vpns;
- Foreign platforms; and
- Multiple accounts.

Digital evidence may also disappear rapidly.

Effective investigation therefore requires specialised cyber-forensic capabilities and timely preservation of relevant data.

4. Evidence Challenges

Digital evidence may include:

- Screenshots;
- Urls;
- Account identifiers;
- Ip information;
- Metadata;
- Emails;
- Chat records;
- Photographs;
- Videos;
- Audio files; and
- Platform records.

Screenshots alone may not always establish the complete evidentiary chain.

Victims therefore need accessible guidance concerning preservation of evidence.

The National Cyber Crime Reporting Portal recognises the importance of digital evidence and explains that a hash value can function as a unique digital fingerprint for an electronic file submitted as evidence.

This illustrates the importance of technical evidence preservation in cybercrime investigations.

X. NATIONAL CYBER CRIME REPORTING PORTAL

The Government's National Cyber Crime Reporting Portal is a significant institutional mechanism.

The portal permits reporting of cybercrime complaints and has a dedicated category for women and children-related cybercrime. It also provides options to report certain complaints anonymously and to track complaints.

The portal specifically allows reporting of online sexually explicit content and certain forms of rape/gang-rape content. It also provides a broader cybercrime category covering online and social-media crimes.

This is a positive development because it reduces dependence upon physical police stations. However, the effectiveness of an online reporting mechanism ultimately depends upon what happens **after the complaint is filed**.

A reporting portal should not become merely a digital substitute for a complaint register.

It must be connected to:

1. Trained investigators;
2. Evidence-preservation mechanisms;
3. Platform liaison systems;
4. Prosecutorial authorities;
5. Victim support services; and
6. Measurable response timelines.

XI. INTERMEDIARY ACCOUNTABILITY

Social-media platforms occupy a central position in the online violence ecosystem.

Platforms control important technological functions including:

- Content moderation;
- Account suspension;
- Reporting mechanisms;
- Recommendation systems;
- Preservation of data; and
- Responses to law-enforcement requests.

The challenge is to determine how far intermediary responsibility should extend.

A platform should not be treated as automatically responsible for every unlawful act committed by its users. Such an approach could negatively affect innovation and legitimate expression.

However, platforms should have heightened responsibilities where:

- Unlawful content is specifically reported;
- The platform has actual knowledge through a valid mechanism;
- The content involves intimate imagery;
- The victim faces an immediate risk of harm; or
- The platform's own systems materially amplify harmful content.

The 2026 SGI amendments move in this direction by imposing specific technical obligations on intermediaries that facilitate synthetic-content generation.

XII. PRIVACY-PRESERVING JUSTICE

One of the paradoxes of online gender-based violence is that seeking legal protection can itself expose the victim to further publicity.

A victim may have to submit intimate photographs, private communications or other sensitive material as evidence.

The legal system must therefore prevent the remedy from becoming another source of harm. Victims of sexual offences are already protected against disclosure of their identity under Indian law, and the Supreme Court has repeatedly emphasised the importance of protecting the privacy and dignity of victims of sexual offences.

The same principle should inform digital proceedings.

Courts and investigative agencies should:

- Restrict unnecessary disclosure of intimate evidence;
- Use secure methods for electronic evidence;
- Avoid reproducing intimate material unnecessarily in pleadings;
- Protect victim identity;
- Limit access to sensitive digital exhibits; and
- Adopt trauma-informed procedures.

Privacy must therefore be treated as part of the remedy, not merely as an abstract constitutional value.

XIII. THE ENFORCEMENT GAP: A STRUCTURAL PROBLEM

The enforcement gap can be represented through five stages:

Reporting → Preservation → Removal → Investigation → Prosecution

A failure at any stage can undermine the entire process.

Reporting failure

Victims may not know where to complain.

Preservation failure

Evidence may disappear before investigators secure it.

Removal failure

Harmful material may continue circulating.

Investigation failure

Authorities may lack technical resources or expertise.

Prosecution failure

Even when a perpetrator is identified, evidentiary or procedural difficulties may prevent successful prosecution.

This demonstrates that legal reform cannot focus exclusively on creating new offences.

The more important question is whether the entire enforcement chain functions effectively.

XIV. RECOMMENDATIONS

1. Establish a Unified Digital Gender-Violence Reporting Mechanism

The existing National Cyber Crime Reporting Portal should evolve towards a comprehensive victim-facing system in which a complainant can report cyberstalking, image-based abuse, threats, impersonation, doxxing and AI-generated sexual abuse through a single interface. The current portal already provides separate pathways for women/children-related crimes and other cybercrimes.

2. Create Specialised Cyber Units

Every State should have adequately staffed cybercrime units with expertise in:

- Digital forensics;
- Social-media investigations;
- Cryptocurrency and payment tracing;

- Ai-generated content;
- Evidence preservation; and
- Victim-sensitive investigation.

3. Introduce Emergency Removal Procedures

Where credible evidence establishes non-consensual intimate imagery or comparable high-risk material, platforms should have rapid-response mechanisms independent of the time required for final criminal adjudication.

4. Strengthen Victim Assistance

Legal remedies should be accompanied by:

- Free legal assistance;
- Counselling referrals;
- Digital-security guidance;
- Evidence-preservation guidance; and
- Assistance in communicating with platforms.

5. Strengthen AI-Generated Content Detection

The emergence of synthetic intimate imagery requires technical systems capable of identifying manipulated or AI-generated content.

The 2026 IT Rules provide an important starting point, but implementation should include transparent standards and independent auditing.

6. Protect Digital Evidence

Investigators should receive specialised training regarding preservation, authentication and chain of custody of digital evidence.

7. Improve Platform Transparency

Large platforms should publish periodic information concerning:

- Complaints received;
- Average response times;
- Removal rates;
- Appeals;
- Repeat offenders; and
- Cooperation with lawful investigation.

8. Strengthen Legal Literacy

Law schools, universities and women's organisations should conduct digital-rights awareness programmes explaining how victims can preserve evidence and access the National Cyber Crime Reporting Portal.

XV. BALANCING PRIVACY, SAFETY AND FREEDOM OF EXPRESSION

Any comprehensive framework must avoid excessive censorship.

Online gender-based violence regulation must not become a mechanism for suppressing:

- Political criticism;
- Satire;
- Journalism;
- Legitimate artistic expression;
- Academic discussion; or
- Lawful disagreement.

The constitutional objective should therefore be **targeted protection rather than broad censorship**.

The legal system should distinguish between content that is merely offensive and conduct that constitutes harassment, intimidation, sexual abuse, privacy invasion or another recognised legal wrong.

This balance is particularly important because intermediary platforms operate at enormous scale.

Automated moderation systems may incorrectly remove legitimate speech, while under-inclusive systems may fail to detect abuse.

A combination of automated detection, human review, victim reporting and transparent appeal mechanisms is therefore preferable.

XVI. CONCLUSION

Online gender-based violence represents one of the most significant emerging challenges to equality, privacy and dignity in India's digital society.

The legal framework has evolved considerably. The BNS recognises stalking through electronic communication, voyeurism, sexual harassment and intrusion upon women's privacy. The IT Act provides offences relating to privacy violations and sexually explicit electronic material. The IT Rules establish intermediary grievance mechanisms and expedited

treatment for certain non-consensual intimate content. The National Cyber Crime Reporting Portal provides a dedicated reporting mechanism for women and children-related cybercrime. The 2026 amendments to the IT Rules are particularly significant because they recognise the emerging threat posed by synthetically generated information and expressly address categories such as non-consensual intimate imagery and privacy-invasive synthetic content. Nevertheless, the existence of multiple legal provisions does not automatically produce effective protection.

The principal enforcement gap lies in the distance between **law on paper and justice in practice**.

A victim may know that her privacy has been violated but may not know which legal provision applies. Even after reporting, content may continue to circulate. Evidence may disappear. Anonymous perpetrators may be difficult to identify. Investigations may be delayed. And the victim may face further privacy violations while pursuing the complaint. The solution therefore does not necessarily lie in creating a completely new offence for every form of online abuse.

India instead requires a **coordinated, victim-centred enforcement architecture**.

Such an architecture should combine the criminal provisions of the BNS and IT Act with effective intermediary regulation, data protection, cyber-forensic investigation and accessible reporting mechanisms. It should also recognise that artificial intelligence has changed the nature of image-based abuse and requires technological as well as legal responses.

Most importantly, the legal system must recognise that online violence is not less serious merely because it occurs through a screen.

A digitally disseminated intimate image can cause real-world humiliation. A cyberstalking campaign can create genuine fear. A fabricated AI-generated image can damage a person's reputation even when every element of the image is artificial.

The constitutional values of **equality, dignity, autonomy and privacy** must therefore extend fully into digital spaces.

The ultimate objective should not be to make women safer by asking them to withdraw from the internet. It should be to create a digital environment in which women can participate freely, equally and safely.

India's next phase of cyber-law reform should therefore move beyond asking whether a legal remedy exists.

The more important question is:

Can a victim obtain that remedy quickly, safely, affordably and effectively?

Until the answer is consistently yes, the enforcement gap will remain the central weakness in India's response to online gender-based violence.

REFERENCES

A. Constitutional and Statutory Materials

1. Constitution of India, 1950.
2. Information Technology Act, 2000.
3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
4. Bharatiya Nyaya Sanhita, 2023.
5. Bharatiya Nagarik Suraksha Sanhita, 2023.
6. Bharatiya Sakshya Adhiniyam, 2023.
7. Digital Personal Data Protection Act, 2023.
8. Digital Personal Data Protection Rules, 2025.
9. Protection of Children from Sexual Offences Act, 2012.
10. Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.

The official India Code record identifies the BNS provisions dealing with sexual harassment, voyeurism, stalking and intrusion upon women's privacy. The IT Act's relevant provisions include Sections 66E, 67, 67A and 67B.

B. Judicial Authorities

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
2. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
3. *Vishaka v. State of Rajasthan*, (1997) 6 SCC 241.
4. *Nipun Saxena v. Union of India*, (2019) 2 SCC 703.
5. *In Re: Prajwala*, Supreme Court of India.
6. *State of West Bengal v. Animesh Boxi*, judicial decision concerning non-consensual intimate imagery and online sexual abuse.
7. *Aureliano Fernandes v. State of Goa*, (2024) 1 SCC 632.

C. Government and Institutional Sources

1. Ministry of Electronics and Information Technology, Government of India, Information Technology Rules, 2021 and amendments.
2. Ministry of Electronics and Information Technology, explanatory material concerning the 2026 amendments relating to synthetically generated information.
3. Ministry of Home Affairs / Indian Cybercrime Coordination Centre, National Cyber Crime Reporting Portal.
4. India Code, Digital Personal Data Protection Act, 2023.
5. India Code, Bharatiya Nyaya Sanhita, 2023.