INTERPLAY BETWEEN THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND CRIMINAL DEFAMATION UNDER SECTION 356 OF THE BHARATIYA NYAYA SANHITA, 2023

Aarya Sachin Temgire, SVKM's Pravin Gandhi College of Law

ABSTRACT

The fastened expansion of digitalization in India has consistently increased blurring boundary between privacy of a person and personal expression. This paper thus, explores the relationship between the Digital Personal Data Protection Act, 2023 (DPDPA), which creates a framework for protecting digital personal data, and Section 356 of the Bharatiya Nyaya Sanhita, 2023 (BNS), which criminalises defamation. The paper examines how personal data, such as photographs, videos, and online social media profiles can be misused to harm the personal character of a person and defame them. Addressing raising concerns revolving around deepfake images and cyber defamation as reference points, this study shows how the consent-based architecture of the DPDP Act can function as an early safeguard against defamatory misuse of personal data, while the BNS continues to operate as the penalising backstop once defamation causes damage to reputation.

This paper also reflects on practical challenges, which include difficulties in enforcement of borderless digital spaces and the risk that defamation law may be invoked to strike down legitimate criticism. This paper further argues for a careful and harmonised reading of both statutes so that individual dignity is protected without unnecessarily curbing lawful expression in India's rapidly evolving digital eco-system.

Introduction

India is currently under a digital era where information flows instantly across social media platforms. The protection of reputation of a person and protection of individual privacy has become highly imporatant. In a country like India where population has reached 1.4 billion[1] as of 2024 and internet user base has exceeded to 1,002.85 million as of April–June 2025, the country finds itself in a difficult grey area where the need to protect personal data often clashes with the equally important need to protect an individual's reputation[2]. The Digital Personal Data Protection Act, 2023 (DPDPA) was enacted by the Ministry of Electronics and Information Technology to regulate the digital personal data of the citizens[3]. The DPDP Act, 2023 recognizes individuals' right to control their personal information while also allowing lawful uses of personal data by way of consent mechanisms[4]. The Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced the colonial – era Indian Penal Code, 1860, penalises criminal defamation under Section 356 by imprisonment for up to two years, a fine, or both, and community service, thus, re-examining traditional ideas of reputational harm so they make sense in today's digital world[5].

This interplay between the DPDP Act, 2023 and the definition of defamation under S. 356 of BNS is particularly remarkable in digital eco-spaces. As personal data of individuals can be manipulated through deepfake AI images, spread of misinformation, and/or unauthorized sharing of to defame individuals[6]. For example, the rise of synthetic media has enhanced the

[1] Press Information Bureau, *Understanding population-related issues, Tailoring solutions, and Driving progress*, Posted on 10 July 2024, available at: https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=151925&ModuleId=3&reg=3&lang=1 (last visited on 26 February 2026).

[2] Press Information Bureau. (2025, September 23). *Satellite internet in India: The future of internet above us* (Explainer ID: 155262). Government of India. Retrieved from https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155262&ModuleId=3&reg=3&lang=2

[3] Ministry of Electronics and Information Technology, *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*, Gazette of India, Extraordinary, Part II, Section 1, dated 11 August 2023, available at:https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on 26 February 2026).

[4] Ministry of Electronics and Information Technology, *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*, Gazette of India, Extraordinary, Part II, Section 1, dated 11 August 2023, available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on 26 February 2026).

[5] Ministry of Law and Justice, *The Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023)*, Gazette of India, Extraordinary, Part II, Section 1, dated 25 December 2023, available at: https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf (last visited on 26 February 2026).

[6] National e-Governance Division (NeGD), *Deepfakes in India: Legal Landscape, Judicial Responses, and a Practical Playbook for Enforcement*, Posted on 29 September 2025, available at: https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/ (last visited on 26 February 2026).

risks of fake images being circulated, as AI-generated fake images or videos can spread quickly and often being viral on social media platforms thus causing irreparable and irreversible damage to a person's reputation[7]. DPDP Act empowers data principals, as defined under DPD P Act "*means the individual to whom the personal data relates and where such individual is—(i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf*;"[8], with mechanisms like consent withdrawal and data erasure. The BNS Section 356 offers a criminal deterrent against intentional harm to reputation of a person. However, harmonising these laws require carefully working through the complex mechanisms involved due to constitutional tensions between Freedom of speech and expression under Article 19(1)(a)[9] and Right to Life under Article 21[10] of the Constitution of India.

This research aims to highlight where the DPDP Act, 2023 and S. 356 of BNS align and where they conflict with each other through a doctrinal analysis coupled with judicial precedents and scholarly commentary. This paper also proposes reforms to ensure more effective enforcement of the laws in force. Given that these laws were only implemented in the year 2024, this discussion is particularly relevant as at this early stage, interpretation and enforcement will significantly shape their long-term impact on the people residing in India. This research therefore seeks to contribute meaningfully to ongoing academic and policy conversations surrounding digital governance and regulatory reform.

Objective of the research paper

The paper aims to critically analyse the interplay between the Digital Personal Data Protection Act, 2023 and Section 356 of the Bharatiya Nyaya Sanhita, 2023 in addressing defamation on digital platforms.

Methodology

This research takes a doctrinal approach based on secondary data to explore the relationship between the Digital Personal Data Protection Act, 2023 and criminal defamation under Section

[7] CUTS International, *Reimagining Content Moderation Strategies in the Age of Generative AI*, 2024, available at: https://cuts-ccier.org/pdf/reimagining-content-moderation-strategies-in-the-age-of-generative-ai.pdf (last visited on 26 February 2026).
[8] *DPDP Act, 2023*, s. 2(j).
[9] *The Constitution of India*, 1950.
[10] Ibid.

356 of the Bharatiya Nyaya Sanhita, 2023. Since the focus is on interpreting the law, the research relies on existing materials rather than primary data. It primarily examines sources such as the Bare Acts, relevant constitutional provisions, parliamentary debates, and judicial decisions dealing with privacy, reputation, and defamation. These are further supported by Law Commission reports, academic writings, commentaries, and policy papers, which help place the legal analysis in a broader context.

This analysis is based on a close and careful reading of both of the statutes while comparing them side by side to spot where they overlap with each other, where tensions between them may arise, and where the law may still have gaps. The paper also considers judicial precedents and academic opinions to understand how these two legal frameworks are likely to work together in this digital age. This approach is well-suited to the study because it provides a clear and systematic way to examine a fast-evolving legal issue in a context where direct empirical data is still relatively limited.

Overview of the Digital Personal Data Protection Act, 2023

The DPDP Act, which got its assent on August 11, 2023, is India's first comprehensive data protection legislation. It is inspired by global standards like the EU's General Data Protection Regulation (GDPR).[6] It applies to the processing of digital personal data within India, whether collected online or digitized from offline sources.[7] Personal data is broadly defined as any information that relates to an identified or identifiable individual, encompassing names, emails, biometrics, and even inferred data[11].

The Digital Personal Data Protection Act, 2023 is structured around a set of safeguards that are meant to empower the individual's regarding their data and keep them in control of their personal data. At the very core of the law is the consent requirement under Section 6[12], which mandates that data fiduciaries, those are entities that determine the purpose and means of processing, must obtain consent that is free, informed, specific, and unambiguous from the data principal. Importantly, the Act recognises that consent is not permanent. Individuals retain the right to withdraw it at any time, and once such withdrawal occurs, the fiduciary is obligated to stop processing the data and take reasonable steps to erase it. At the same time, the statute

[11] The Digital Personal Data Protection Act, 2023
[12] The Digital Personal Data Protection Act, 2023, s. 6.

acknowledges certain "legitimate uses" under Section 7[13] where processing may occur without fresh consent, such as in cases of voluntary data disclosure by the individual, specific state functions, or certain employment-related purposes. Even in these situations, the processing must remain confined to clearly defined and lawful objectives.

The Act further strengthens individual autonomy by conferring enforceable rights on data principals under Sections 11 to 13[14]. These include the right to access information about how their data is being used, the right to seek correction or erasure of inaccurate or outdated data, and the right to nominate another person to exercise these rights in situations such as incapacity or death. To ensure that these obligations are not merely symbolic, the legislation establishes a dedicated Data Protection Board tasked with monitoring compliance and adjudicating violations. The enforcement framework carries significant financial consequences such as under Section 33[15], breaches of key obligations can attract monetary penalties that may extend up to ₹250 crores. This clarifies the legislature's intent to create strong deterrence and encourage responsible data governance.

The Act's extraterritorial reach extends to foreign entities processing Indian data, thus, emphasizing the existence of sovereignty in digital affairs[16]. However, critics have noted lighter regulatory burden of DPDP Act, 2023 compared to GDPR, thus, inferring that DPDP Act potentially favours business interests over robust privacy safeguards[17]. In the context of defamation, DPDP Act's focus on preventing unauthorized data use can pre-empt the dissemination of harmful content derived from personal information.

Overview of Criminal Defamation under Section 356 of the Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita (BNS), which came into force on 1 July 2024[18], reorganises India's criminal law framework while substantially preserving the earlier law on defamation.

[13] The Digital Personal Data Protection Act, 2023, s. 7.
[14] The Digital Personal Data Protection Act, 2023, ss. 11–13.
[15] The Digital Personal Data Protection Act, 2023, s. 33.
[16] CyberPeace, *Extraterritorial Application in Data Privacy: Lessons for India's DPDP Act*, Posted on 6 March 2025, available at: http://cyberpeace.org/resources/blogs/extraterritorial-application-in-data-privacy-lessons-for-indias-dpdp-act (last visited on 27 February 2026).
[17] Shivam Tripathi & Ritu Sharma, *Reimagining Content Moderation Strategies in the Age of Generative AI*, Computer Law & Security Review, Vol. 53 (2024), Article 105933, available at: https://www.sciencedirect.com/science/article/pii/S0267364924000992 (last visited on 27 February 2026).
[18] The Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023).

Section 356 of the BNS carries forward the core substance of the former Section 499 of the Indian Penal Code. Under Section 356(1), defamation is defined, "*Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes in any manner, any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person."*[19] . The provision is deliberately wide in scope. It extends not only to statements concerning living individuals but also to imputations about deceased persons where the statement would injure the feelings or reputation of surviving relatives. Similarly, reputational harm caused to companies, associations, or collections of persons is also recognised within the offence.

In terms of consequences, Section 356(2) prescribes punishment in the form of simple imprisonment that may extend up to two years, or fine, or both. A notable addition in the BNS framework is the explicit inclusion of community service as an alternative sentencing option, signalling a gradual shift towards incorporating elements of restorative and rehabilitative justice within criminal law. At the same time, the provision continues to retain the traditional ten exceptions which protect speech made in good faith and in the public interest. These include, among others, imputations that are true and made for the public good, fair comment on the public conduct of public servants or public figures, and substantially accurate reporting of judicial proceedings.

In the contemporary digital environment, the scope of "publication" under defamation law has naturally expanded.[20] Courts have increasingly treated online posts, forwards, and shares as capable of satisfying the publication requirement where reputational harm can be demonstrated. The constitutional validity of criminal defamation itself was affirmed by the Supreme Court in Subramanian Swamy v. Union of India (2016)[21], where the Court held that protecting an individual's reputation is a legitimate state interest and that criminal defamation operates as a reasonable restriction on the freedom of speech and expression. Taken together, Section 356 of the BNS reflects both continuity with established defamation principles and a

[19] *The Bharatiya Nyaya Sanhita, 2023*, s. 356.
[20] Melisa Zukić & Abdurrahman Zukić, *Defamation Law and Media: Challenges of the Digital Age*, MAP Education and Humanities, Vol. 5, Issue 1 (2024), pp. 98–109, available at: https://www.researchgate.net/publication/385487183_Defamation_Law_and_Media_Challenges_of_the_Digital_Age (last visited on 27 February 2026).
[21] *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221.

cautious adaptation to evolving modes of communication and punishment.

The Intersection between DPDP Act, 2023 and S. 356 BNS.

The intersection between the Digital Personal Data Protection Act, 2023 and Section 356 of the Bharatiya Nyaya Sanhita becomes particularly pronounced in cases of cyber defamation, where misuse of personal data directly enables reputational harm. In the digital ecosystem, harmful speech is often not created in isolation, it is built using someone's personal information, images, or biometric data[22]. This is most evident in the growing use of deepfake technology, where artificial intelligence is employed to manipulate a person's likeness and falsely depict them engaging in acts they never committed[23]. Such content does not merely distort reality but it simultaneously raises concerns of privacy invasion, unlawful data processing, and reputational injury.

From the perspective of the Digital Personal Data Protection Act, the unauthorised creation or circulation of deepfake material may amount to unlawful processing of personal and biometric data, particularly where it occurs without the data principal's valid consent. In such situations, the data fiduciary, or any entity responsible for determining the means and purpose of processing, may be in breach of statutory obligations. The affected individual is then entitled to invoke rights such as seeking erasure of the manipulated content and triggering regulatory action, including monetary penalties. The Act therefore offers a civil-regulatory pathway focused on data misuse and informational autonomy.

Section 356 of the Bharatiya Nyaya Sanhita addresses the reputational dimension of the same conduct. Where the deepfake or manipulated content contains imputations that are false and demonstrably harmful to a person's reputation, and where the requisite intention or knowledge can be established, criminal defamation may be attracted. In practice, therefore, a single act, such as generating and circulating a defamatory deepfake, can engage both protections i.e., the data protection framework responding to the unlawful handling of personal data, and the

[22] Pablo Madriaza et al., *Exposure to Hate in Online and Traditional Media: A Systematic Review and Meta-Analysis of the Impact of This Exposure on Individuals and Communities*, Campbell Systematic Reviews, Vol. 21 (2025), Article e70018, available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC11736891/ (last visited on 27 February 2026).

[23] Furizal et al., *Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review*, Social Sciences & Humanities Open, Vol. 12 (2025), Article 101882, available at: http://sciencedirect.com/science/article/pii/S2590291125006102 (last visited on 27 February 2026).

criminal law responding to the injury to reputation. This overlap illustrates how modern digital harms rarely fit neatly within traditional legal silos. Instead, they operate at the intersection of privacy, data governance, and reputational protection, requiring courts and regulators to carefully navigate the concurrent application of both statutes.

The Digital Personal Data Protection Act, 2023 also plays an important preventive and supportive role in situations that may otherwise escalate into criminal defamation. One such way is insisting on valid, informed consent before personal data is processed, the Act has the potential to curb the creation and circulation of harmful content at an early stage. Digital platforms and other data fiduciaries are expected to build compliance safeguards into their systems, which can indirectly reduce instances of "publication" that might attract liability under Section 356 of the Bharatiya Nyaya Sanhita. At the same time, the rights granted to data principals, particularly the right to access information about how their data has been used, can significantly strengthen a victim's position in defamation proceedings. Thus, enabling individuals to trace the origin and flow of their personal data, the DPDPA helps generate a clearer evidentiary trail, which may prove crucial in establishing unauthorised use and supporting a claim of reputational harm.

Case Studies and Judicial Insights

Judicial interpretation has played a decisive role in shaping how Indian law responds to digital harms. In Shreya Singhal v. Union of India[24], the Supreme Court struck down Section 66A of the Information Technology Act for vagueness and overbreadth, firmly establishing that restrictions on online speech must satisfy the test of proportionality and constitutional precision. This decision continues to influence how courts approach the emerging overlap between data protection and criminal defamation. In the post-DPDPA landscape, courts dealing with deepfake controversies, particularly cases involving morphed celebrity videos, have increasingly relied on a combination of intermediary due-diligence obligations under the IT Rules, 2021 and privacy principles reinforced by the Digital Personal Data Protection Act, 2023 to direct prompt takedowns of harmful content[25].

High Courts have also begun to build procedural safeguards against misuse of defamation law

[24] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[25] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Digital Personal Data Protection Act, 2023.

in the social media context. Notably, the Telangana High Court has emphasised that defamation FIRs arising out of online speech should not be registered mechanically and has required prior magisterial scrutiny in appropriate cases, recognising the chilling effect that criminal process itself can produce, this was further affirmed by Hon'ble Supreme Court.[26] Similarly, the Delhi High Court, in matters involving cyber harassment and non-consensual circulation of personal material, has drawn an explicit connection between privacy violations and reputational harm, signalling that data protection norms can meaningfully strengthen victim remedies alongside traditional defamation law.[27]

Comparative developments further illuminate India's policy choices. The United Kingdom, through the Defamation Act 2013, moved toward decriminalising libel and raising the threshold for actionable harm, reflecting a stronger tilt toward speech protection[28]. India's decision to retain criminal defamation, now under the Bharatiya Nyaya Sanhita, may operate as a deterrent against egregious digital abuse, but it also raises continuing concerns about over-criminalisation and chilling effects in the online sphere. The tension is visible in cases such as Ramdev v. Facebook[29], where the court ordered global takedown of defamatory content containing personal data, demonstrating how reputation, platform regulation, and data protection are becoming increasingly intertwined. Together, these judicial trends suggest that while Indian courts are moving toward a more integrated digital rights framework, careful doctrinal calibration will be essential to preserve both dignity and free expression in the evolving online ecosystem.

Recommendations:

1. Criminal defamation under the Bharatiya Nyaya Sanhita, 2023 should be redefined for the digital defamation by making it harder to prove real harm and deliberate bad intent, and by nudging most routine online disputes toward civil remedies instead of criminal cases. This would help strike a more reasonable balance between protecting a person's

[26] Furizal et al., *Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review*, Social Sciences & Humanities Open, Vol. 12 (2025), Article 101882, available at: http://sciencedirect.com/science/article/pii/S2590291125006102 (last visited on 27 February 2026).
[27] *McDonald's Corporation & Anr. v. National Internet Exchange of India & Ors.*, CS (COMM) 324/2020, decided on 24 December 2025 (Delhi High Court), available at: https://delhihighcourt.nic.in/app/showFileJudgment/PMS24122025SC3242020_181821.pdf (last visited on 27 February 2026).
[28] Defamation Act 2013 (UK).
[29] Ramdev v. Facebook Inc., 2019 SCC OnLine Del 10701.

reputation and safeguarding free speech under Article 19(1)(a), in keeping with the proportionality principle as recognised in Subramanian Swamy v. Union of India[30].

2. A formal coordination mechanism should be established between the Data Protection Board under the Digital Personal Data Protection Act, 2023 and cyber police units to enable joint investigations, faster evidence preservation, and effective takedowns. Such integration would strengthen the State's positive obligation to protect informational privacy recognised in K.S. Puttaswamy v. Union of India[31].

3. Governments should mandate digital literacy programmes and sector-specific AI ethics guidelines, such as watermarking and traceability, to prevent deepfake misuse. Preventive safeguards of this kind reflect the constitutional duty to protect privacy and dignity.

4. Courts should evolve harmonising guidelines between the Digital Personal Data Protection Act, 2023 and the Bharatiya Nyaya Sanhita, 2023 using the four-part proportionality test laid down in K.S. Puttaswamy v. Union of India[32].

Conclusion

The relationship between the Digital Personal Data Protection Act, 2023 and Section 356 of the Bharatiya Nyaya Sanhita clearly shows attempts by India to address the digital harms meaningfully. The DPDP Act certainly strengthens the protection of personal data and helps prevent misuse of digital data that can cause harm to a person's reputation, but Section 356 of the BNS also ensures that genuinely malicious conduct does not go unchecked. Both the Act and the provision when read together showcases potential to create a more a more practical and easy-to-follow system of accountability for the digital platforms. However, if these provisions are applied mechanically or without addressing the context of use, they may also may end up making access to justice even more unequal, especially for people who lack digital awareness or the resources to seek legal help. Moving ahead, what is needed to harmonise is a clearly rights-oriented approach grounded in proportionality and public interest, so that privacy protection does not come at the cost of legitimate expression, and vice versa.

[30] Subramanian Swamy v. Union of India, (2016) 7 SCC 221.
[31] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[32] Ibid.

References:

1. The Constitution of India
2. Bharatiya Nyaya Sanhita, 2023
3. Digital Personal Data Protection Act, 2023
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Digital Personal Data Protection Act, 2023.
5. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
6. Subramanian Swamy v. Union of India, (2016) 7 SCC 221.
7. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
8. Defamation Act 2013 (UK).
9. Ramdev v. Facebook Inc., 2019 SCC OnLine Del 10701.
10. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=151925&ModuleId=3&reg=3&lang=1
11. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
12. https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf
13. https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/
14. https://cuts-ccier.org/pdf/reimagining-content-moderation-strategies-in-the-age-of-generative-ai.pdf
15. http://cyberpeace.org/resources/blogs/extraterritorial-application-in-data-privacy-lessons-for-indias-dpdp-act

16. https://www.sciencedirect.com/science/article/pii/S0267364924000992

17. https://www.researchgate.net/publication/385487183_Defamation_Law_and_Media_Challenges_of_the_Digital_Age

18. https://pmc.ncbi.nlm.nih.gov/articles/PMC11736891/

19. http://sciencedirect.com/science/article/pii/S2590291125006102

20. https://delhihighcourt.nic.in/app/showFileJudgment/PMS24122025SC3242020_181821.pdf