



This is an Open Access article distributed under the terms of the Creative Commons Attribution- Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

One Crime, Many Statutes: Complexity with Indian Cybercrime Regulations

Mansi Dadhich

ABSTRACT

A deepfake video puts words in a businessman's mouth, generated by a rival to defame him. That single act now triggers liability under three separate tracks: BNS defamation provisions, the IT Act's 2026 rules on synthetically generated information, and possibly the DPDP Act too. This paper traces why. BNS 2023 folded cyber offences into general criminal law rather than giving them a dedicated chapter, so forgery, cheating, and organised crime sections now carry electronic language stitched in, unevenly. Section 336 names "electronic records" outright. Section 356, the defamation provision that would actually catch Mr M's deepfake, says nothing about digital or synthetic media at all, leaving courts to stretch it case by case. India hasn't failed to legislate on cybercrime. It's legislated three times over, in three places that don't talk to each other.

BLOG

Mr M, a prominent business figure, appeared in a video that supposedly referred to a whole community as thieves, though later findings showed that the video was a deepfake, generated by his business nemesis to defame him. In this scenario, a single crime corresponds to two different sets of rules: BNS (defamation) and the IT Act's 2026 amendments on Synthetically Generated Information (SGI). ¹The real issue for India in 2026 is not the absence of enforcement, but the absence of a single law governing acts that create liability under multiple statutes at once. With the recent transitions from the IPC to BNS, efforts have been made to include cyber crimes as well, though still without a dedicated cybercrime framework of its own. The next step towards cybercrime regulation should be to build a systematic chain to link such acts, regulating the same crime. Is India's claim to technological advancement matched by equally advanced law?

To give legal recognition to electronic records and to criminalise computer-related offences, the IT Act 2000 ²was enacted as India's first purpose-built cyber governance act. But alongside this, the general criminal laws, the IPC, continued to apply. With BNS 2023, the whole IPC was rewritten. The scope of general criminal laws extended to computer-related crimes, such as forgery of "electronic records" (Section 336), cheating via electronic means (Section 318),

¹ Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Gazette Notification G.S.R. 120(E) (Feb. 10, 2026, effective Feb. 20, 2026).

² Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

and organised cybercrime (Section 111). These provisions remain scattered across categories of traditional offences: cheating, forgery, and organised crime, rather than being united as a dedicated chapter for computer-related crimes. The Digital Personal Data Protection Act, 2023³, stands as a third track; it adds civil and regulatory liabilities for data mishandling, meaning a single serious incident can trigger criminal charges under two statutes and regulatory penalties under the third. Most cybercrime FIRs in India cite BNS and IT Act provisions simultaneously, not because the crime is unclear, but because they remain live and overlapping. This becomes clearest when checking which BNS sections carry electronic language and how far they extend.

For instance: Section 318 deals with cheating; this covers online fraud, such as UPI scams, phishing, fake job offers, and digital impersonation to induce payment⁴. Broadly, these categories work under the definition of “cyber fraud”, but as explained in the provisions of BNS, these are in the general cheating section, with electronic acts simply falling within this category. Section 336 states forgery; this section explicitly names “electronic records” in its text.⁵ This becomes one of the most direct recognitions of digital forgery, unlike any other cybercrimes, which remain just an interpretive stretch. The definition of forgery is the making of a false document or *electronic record* with the intent to cause damage, support a false claim, or commit fraud. This section remains significantly important as “electronic” appears directly in the statutory language, unlike other provisions, where its application depends entirely on judicial interpretation.

Mr M’s case would fall squarely within the category of defamation, Section 356⁶. Though the section was written for traditional defamatory statements, spoken or published, Indian courts have already begun extending its application to social media posts, and the same logic needs to be stretched to capture a fabricated video depicting speech that was never actually made. Unlike Section 336’s explicit mention of “electronic records”, Section 356 doesn’t mention digital or synthetic media as such; the reach of this Section entirely depends on judicial interpretation, not statutory language.⁷

Sections 75 and 77-79 extend protection against stalking, voyeurism and non-consensual image circulation into digital space, further covering acts like repeated online monitoring, secretly recording someone, or circulating intimate pictures without consent of the affected person.⁸ These sections carry forward IPC-era protections and are stretched to cover digital methods, not offences as originally adapted with technology in mind. Section 111 covers organised crimes; this has been extended to organised ‘cybercrime’, relevant to coordinated phishing rings, romance-scam networks, and large-scale fraud operations organised by structured criminal groups rather than committed alone.⁹ As can be seen from all the sections, in the absence of any statutory explicit definitions, judicial interpretation becomes the only way to extend these crime definitions to cybercrimes, in the tech-advanced world. In sum, India

³ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁴ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India), § 318.

⁵ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India), § 336.

⁶ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India), § 356.

⁷ LawSection.in, *Cyber Crimes Under Bharatiya Nyaya Sanhita, 2023*, <https://lawsection.in/cyber-crimes-under-bharatiya-nyaya-sanhita-2023-bns/> (last visited July 23, 2026)

⁸ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India), §§ 75, 77-79.

⁹ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India), § 111.

requires a defined framework to work with these traditional crimes and cybercrimes simultaneously.

Mr M's case was not just a hypothetical scenario; it is what happens in the present, when a deepfake comes into existence: investigators and lawyers have to untangle BNS, the IT Act's SGI rules, and potentially DPDP, rather than opening one clear statute. This fragmentation is not what BNS fixed¹⁰; it remains a pattern that the Indian legal system has carried forward since the IT Act 2000, and BNS 2023, instead of resolving it, extended this fragmentation. India is advancing, so are its laws. But in pieces, not as a system. Until they converge, the answer to whether India's legal framework matches its technological ambitions remains unaddressed.

¹⁰ LawSection.in, *supra*.