Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 4 (2025)

The Failure of Social Media Platforms to Mitigate Cybercrime in India: Examining Algorithmic Gaps and Legal Responsibilities

Ms. Richa Sharma[1*]
[1]Research Scholar, School of Law, Sushant University Sector-55, Golf Course Road, Gurugram, Haryana- 122011, India
*Corresponding Email Id: richasharma.phd20@sushantuniversity.edu.in

Dr. Anil Dawra[2]
[2]Professor, School of Law, Sushant University Sector-55, Golf Course Road, Gurugram, Haryana- 122011, India
Email Id: anildawra@sushantuniversity.edu.in

Dr. Anjali Sehrawat[3]
[3]Associate Professor, School of Law, Sushant University Sector-55, Golf Course Road, Gurugram, Haryana- 122011, India
Email Id: anjalidabas@sushantuniversity.edu.in

ABSTRACT

There is increasing concern that the algorithmic architecture of social media platforms, particularly when utilized with insufficient human oversight, may exacerbate cybercrime rather than mitigate it. In India, hate speech, cyberbullying, phishing scams, non-consensual personal images, and financial theft have proliferated on platforms such as Instagram, Facebook, and X (previously Twitter). There has been significant public and governmental interest in content filtering; yet, research on how algorithmic amplification exacerbates these issues is limited. Indian law does not recognize platform design problems as a distinct legal harm, despite the stipulations of the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and their amendments in 2023. The study proposes that algorithmic negligence be recognized as a novel legal category within Indian cyber law, utilizing tort characteristics such as duty of care, breach, harm, and causation. The study demonstrates that nations globally are progressing towards more proactive governance by comparing the EU's Digital Services Act (**DSA**), U.S. Section 230 of the Communications Decency Act, 1996 (**Section 230**) jurisprudence, and Japan's content moderation regulations. This research proposes implementable enhancements such as obligatory algorithmic audits, tiered duty-of-care frameworks, and transparency requirements. It accomplishes this by doctrinal analysis, case studies, and cross-jurisdictional synthesis. It concludes by proposing a strategy to amend India's legislation to classify harmful algorithmic design as a legal violation.

Keywords: *Algorithmic negligence; legal accountability; social media intermediaries; cyber-crime mitigation; content moderation; comparative legal analysis; platform liability; Indian social media.*

INTRODUCTION

In India, social media platforms like Instagram, Facebook, and Snapchat, Youtube etc. hosts millions of active users daily, deeply influencing their everyday life. Over 820 million users are expected on these algorithmically regulated public platforms by 2025[1]. These platforms have become an essential component of contemporary communications infrastructure and public discourse. They have drastically reshaped the way we interact, share information and ideas. Social media platforms, with their algorithm system, selects, ranks and recommends contents to their users on the basis of their searches and interaction. National Crime Records Bureau (**NCRB**) reports a 24.4 % increase in cybercrime cases in India from 52,974 in 2021 to 65,893 in 2022, with frauds accounting for roughly 65% of the total instances[2]. In 2023, the Indian Computer Emergency Response Team (**CERT-IN**) observed an increase in deepfake frauds, targeted phishing, and non-consensual picture abuse[3]. Data shows that algorithmic recommendation systems without monitoring propagate harmful content and viral it faster than human moderation.

In recent years, there have been multiple documented incidents where algorithm-driven recommendation systems on social media platforms have been linked to the amplification of harmful content, thereby facilitating cybercrimes and offline violence. Following the tragic Southport murders in the United Kingdom on 29 July 2024, a UK Parliamentary report found that recommendation algorithms amplified false and hateful narratives, contributing to violent protests targeting Muslim and migrant communities[4]. In the United States, a multidistrict lawsuit has been brought against Meta (Instagram) and

TikTok by former users, including Caroline Koziol, alleging that their algorithms promoted harmful content that contributed to eating disorders, with courts allowing negligence and product liability claims to proceed[5]. Similarly, litigation arising from the 2022 Buffalo mass shooting alleges that the shooter was radicalised through extremist content promoted by algorithms on platforms such as Meta, Snap, Discord, Reddit, YouTube, and Amazon, with plaintiffs arguing that these systems constitute defective products[6]. Such cases underscore the emerging concept of "algorithmic negligence", where the automated curation of user feeds is not merely a neutral technological process but an active driver of harm, thereby raising serious questions regarding the legal responsibility of platforms in preventing the spread of unlawful and dangerous content.

This raises a pertinent question of whether the platforms should bear the responsibility when their automated systems cause or contribute to such harms, a concept that can for this paper be termed as "Algorithmic Negligence".

In essence, algorithmic negligence can be referred as a failure of the platform to exercise a reasonable care in the design or operation of its algorithm to prevent any harm or injury like defamatory content, obscene material, to its users. These algorithms display prejudice by ranking content via public involvement, favouring sensational, emotionally charged, or misleading content[7]. Social media algorithms function as mathematical systems employing machine learning and heuristic reasoning to curate, prioritize, and recommend information tailored to individual users. These algorithms use behavioural data, including user interactions, relationships, and engagement metrics such as likes, clicks, and time spent on posts, to forecast which content will garner the most attention from users. For example, Facebook employs deep learning and collaborative filtering to customize its News Feed, whereas Twitter prioritizes material on its timeline by weighing its recency against user interest.

These algorithms are designed to maintain user engagement; yet, they frequently fail to mitigate illicit activity. A significant issue is their failure to comprehend the context, allowing perilous operations such as phishing or orchestrated online abuse to bypass filters if they resemble ordinary encounters[8]. Fraudsters have utilized Facebook groups to disseminate deceptive fundraising posts that appear authentic and are consequently endorsed by the platform. Another issue is that wrongdoers may use the system by employing bots or click farms to artificially enhance participation, so disseminating harmful content to a wider audience. Furthermore, these systems lack transparency, complicating the ability of both users and authorities to ascertain the criteria for takedowns or the logic behind detection, thereby hindering prompt and effective responses.

The Indian legal framework for the liability of social media platform does not, yet, directly deal with the issue of algorithm negligence. Section 79 of the Information Technology Act, 2000 (hereinafter referred as IT Act, 2000) provides platforms with some protections, or simply put a safe harbour, if they promptly address discovered information.[9] The 2021 Information Technology Rules incorporated more stringent criteria, such as traceability and local grievance redressal mechanisms. Platforms frequently defer compliance with regulations by asserting that technological or privacy concerns impede their adherence. For instance, WhatsApp declined to identify the origins of hate speech messages prior to the 2023 elections[10]. These laws were designed for instances where the social media platforms were seen as a passive hosts of the content posted by the third party. But Judicial bodies have begun to acknowledge that a platform bears the responsibility to use preventive technology, yet, the application of this legislation remains inconsistent. The disparity between algorithmic decision-making and regulatory frameworks persists, jeopardizing user safety in India's digital environment.

This paper undertakes a doctrinal analysis and highlights algorithmic neglect, utilizing tort characteristics such as duty of care, breach, harm, and causation, where social media companies poorly develop and deploy algorithmic systems that may harm its users. In order to ground this concept within the Indian legal framework, it is necessary to draw from Indian tort law, where negligence is established through four foundational elements: duty of care, breach, injury, and causation. In Shreya Singhal v. Union of India[11] (2015), Indian courts have evaluated intermediary liability, but not algorithm design negligence. The law emphasizes notification-based takedown procedures and fails to recognize platform design flaws as actionable damages. The absence of theory is concerning due to algorithmic structural issues. In contrast to discrete user acts, algorithmic curation is systemic and scalable. It causes damage faster and more than conventional regulatory structures can handle. WhatsApp impersonation schemes[12], Facebook political manipulation[13], and rising public interest litigations demanding algorithmic transparency and independent audits underscore the need for reform[14]. Even after the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and 2023 Amendments, Indian laws do not require platforms to analyze algorithmic system hazards. Also, in parallel, a comparative analysis of approaches in other countries

is also carried out in this paper. The European Union has recently overhauled its intermediary liability regime through Digital services Act (hereinafter referred as DSA), which inter alia, imposes transparency and risk mitigation obligations on the algorithmic systems of a platform.[15] As far as United States of America is concerned, it continues to shield the social media platforms under Section 230 of the Communications Decency Act (CDA), despite there being an issue regarding algorithmic recommendations. Japan has evolved in its approach and has aligned with the notice and takedown and safe harbour model and it also endorses immunity style provided by Section 230 of the CDA in its digital trade pact with the US.[16] The main aim of this article is to critically evaluate the strengths and shortcomings of India's current framework. The absence of explicit provisions or case laws on algorithmic accountability constitutes a legal vacuum, one which the platforms can exploit and leave the victims of algorithm driven harms without any clear remedies.

There is no doubt that India urgently needs a reform in its laws pertaining to cyber world. With millions of users on the social media platform, it is not just a part of our lives but is influencing our society at a deeper level. We have witnessed how with a single post rumors can spread dangerously, spark violence, how misinformation can sway elections etc. hence, the main research question of this paper is: "Can Indian law recognize algorithmic negligence as a form of platform liability? And if so, what doctrinal, regulatory, and comparative tools are needed to support this transformation? This research makes two important contributions. First, it defines algorithmic negligence in Indian tort law. Second, it defines structural obligations, such as algorithmic impact assessments, differentiated duties of care, and legal presumptions of causation for algorithmic exposure-related harm, to create a legislative framework for reform. It aims to move India's digital governance from reactive content regulation to proactive design-oriented responsibility.

This paper proceeds with literature review followed by discussion on theoretical framework of algorithmic negligence, examines how negligence doctrine in tort law might apply to algorithm driven services and hurdles in establishing duty, breach and causation in such cases. The next part focuses on the liability of platform in India and relevant case laws developments and discusses how they would intersect with or fail to cover algorithmic negligence. The paper also discusses the comparative international framework to highlight how other countries around the world are dealing with similar issues. Following this, how Indian courts are yet to take the area of algorithmic negligence as a concrete area that needs to be dealt separately from Section 79 of the IT Act approach is also discussed. Part 6 provides discussion and recommendations followed by conclusion.

LITERATURE REVIEW

The Information Technology Act, 2000, specifically Section 79, governs digital intermediaries in India. Online platforms receive conditional safe harbour[17]. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and 2023 revisions included complaint and content removal procedures[18]. Researchers think these methods are not enough to remedy algorithm design and structural damage[19]. Judicial guidance has been provided. Supreme Court ruled in Shreya Singhal v. Union of India (2015) that platforms are not liable for unmoderated posts if they do not have "actual knowledge" of illegal content. Gausen et al. (2024) note that the DSA can give digital governance "sociotechnical transparency" that Indian legislation lacks[20]. US controversy has increased about what Section 230 of the US Communications Decency Act entails[21]. Gonzalez v. Google LLC (2023) examined whether YouTube's algorithm fostered terrorism[22]. The Supreme Court did not hold Google accountable, but it established a clear distinction between passive hosting and active curating. According to legal theorists Pasquale (2015) and Balkin (2017), the state should regulate algorithms more[23]. They propose a legal system that views algorithms as infrastructures with legal repercussions, not just conveniences. Like Pareek & Sole (2021), Indian academic writing calls for platform intermediaries' obligations to be set down so they can be held accountable for indirect harms caused by algorithmic amplification[24].

Theoretical Framework of Algorithmic Negligence

Despite its growing importance in legal and policy discourse, Indian tort law fails to define "algorithmic negligence". Algorithmic negligence can be visualized as a branch of negligence law which deals with harms caused through automated decision making systems. In the traditional law on negligence in India which is a well-defined tort involving four

interwoven elements: a duty of care, a violation of that duty, harm or injury, and a causal relationship between the breach and the harm[25]. These are the four elements which a claimant must prove in order to prove tort of negligence. When the person making the decision is an algorithm, which is effectively a set of instructions created and maintained by humans, then applying this framework, though becomes challenging, but is necessary.

Platforms deploy algorithms for content moderation (deciding which posts to remove or flag), content ranking (deciding which posts users see first), recommendations (suggesting new content or contacts), and advertisements targeting. If these algorithmic processes lead to injury – for instance, by systematically amplifying defamatory content, enabling illegal transactions, or creating an unsafe environment – one must ask: Can the platform be considered negligent? Following are the elements of negligence in order to analyse algorithmic negligence doctrinally:

1. Duty of Care: Are platforms legally obligated to operate their algorithms in a manner that mitigates the likelihood of harm? This is a primary inquiry. In such circumstances, courts have occasionally asserted that certain individuals bear obligations to those impacted by their products or acts (for instance, manufacturers are obligated to ensure the safety of their products for consumers[26]). A platform has an obligation to safeguard anyone who may be adversely affected by its material, including users and non-users who are targets of online harassment or offline victims of incitement, due to its active curation of information via algorithms. This is due to the probable dissemination of damaging information or incitement to violence. Nonetheless, establishing an individual's duty is challenging due to the extensive and ambiguous nature of potential victims, coupled with the right to free expression. Currently, no Indian legislation or judicial decision explicitly mandates that platforms bear this responsibility for their algorithmic functions. Indian law continues to classify platforms as "intermediaries" rather than publishers, historically resulting in diminished duties for them.
2. Breach of Duty (Standard of Care): If a duty were recognized, the subsequent inquiry pertains to the type of care algorithms that should be implemented. It may be feasible to establish an acceptable norm for platform operators. Would a prudent social media company have developed or monitored its algorithms in a manner that would have averted the harm? This requests evidence of industry standards, the technological viability of safer designs, and any prior alerts or recognized issues. For example, if it is recognized that a recommendation algorithm fosters "filter bubbles" or amplifies extreme content to enhance user engagement, a responsible operator would endeavour to mitigate these effects by modifying the algorithm or providing users with greater options. A breach could be established by demonstrating that the platform failed to implement technically and economically feasible measures that were widely recommended, or that it disregarded indications regarding the perilous nature of its algorithm.
3. Causation and Remoteness: A plaintiff must demonstrate that the algorithm's actions resulted in the harm, employing both factual causation (the "but-for" test) and legal causation (proximate cause). This is particularly challenging for algorithmic harm due of the multitude of potential factors involved. For instance, if a viral post incites an online mob assault, who bears responsibility? Was it the individual who published, the several individuals who disseminated it, or the algorithm that enhanced its visibility? The law of negligence posits that several causes may exist; nevertheless, a platform may assert that the chain of causation is disrupted by the independent actions of users, invoking the principle of novus actus interveniens. To ascertain proximate causation, one must assess whether the algorithm's design rendered the harm probable. If a recommendation engine presents adolescents with films depicting self-harm, resulting in injury, one could argue foreseeability exists, given prior cases and research linking such recommendations to harm. The capacity to foresee detriment from algorithmic decisions is a crucial aspect of both duty and causation analysis.
4. Damage: Algorithmic negligence can result in various forms of harm, including personal injury and psychological distress (such as suicide exacerbated by cyberbullying facilitated by algorithms, or mob lynching incited by online rumors) as well as financial detriment (for instance, defamation resulting in economic loss, or fraudulent schemes facilitated by platform algorithms). Indian tort law permits individuals to obtain compensation for several types of damages, including emotional distress and reputational harm, provided they can substantiate additional elements.

Platform Liability in India

The Indian legal framework does not specifically define internet intermediaries' algorithm design obligations. Intermediaries are protected from third-party content by Section 79 of the Information Technology Act, 2000[27]. However,

Google India Pvt. Ltd. v. Visaka Industries[28] (2019) show that the judiciary scrutinizes this passive posture, especially where platform configuration causes injury. The court recognized the conditional immunity in para 149: "An intermediary is not liable for third party information if it proves that the offence or contravention was committed without its knowledge or that it had exercised all due diligence to prevent such commission. The safe harbour provision will not apply where the intermediary, upon receiving actual knowledge, fails to expeditiously remove or disable access to the unlawful material."
The Delhi High Court ruled in Visaka Industries that search algorithms regulate visibility and increase risk. This confuses passive hosting and active design. When automated curation affects user experience, an intermediary has a duty of care to victims under tort law. This obligation is specific to the platform's use of algorithms to change visibility based on engagement, regardless of content quality or harm. The platform is negligent if it fails to implement risk mitigation measures or continues to use optimization systems that algorithmically promote harmful content categories like scams, harassment, and graphic material despite public evidence of user harm.
Pain goes beyond financial loss here. Algorithmically amplified misinformation, online extortion, and impersonation fraud cause psychological, reputational, and physical harm. Indian courts have previously handled tort claims for emotional and reputational damages, therefore algorithms' impacts cannot be ignored. If there is enough evidence that the platform's algorithm caused the harm, causality can be established. The causal chain would be established if a platform's algorithm promoted fraudulent content despite internal concerns or complaints and damaged users. Instead of being a new tort, algorithmic negligence applies tort ideas to modern technology. It shows how typical negligence has evolved into systemic design-caused harm.
This study presents a typology of algorithmic defaults into passive, active, and opaque negligence to improve platform negligence use. Different levels of guilt and institutional authority affect legal liability in these groups. Passive algorithmic carelessness begins when platforms fail to monitor or analyze algorithm results. This includes cases when platforms ignore warning signs of dangerous trends like viral fraudulent ads, phishing targeting kids, and deepfake blackmail[29]. Inaction, failing to notice and avoid harm that a reasonable platform operator with internal analytics and moderation tools could have anticipated, is often negligence. Second, active algorithmic negligence.
It includes design choices that raise user vulnerability. This involves using algorithmic methods to achieve virality without blocking alteration or damage. Platforms that favor watch time or click-through rates over user safety encourage harmful content[30]. Often, the infraction is premeditated, making it nearly irresponsible. When a platform's architecture precludes users from observing or auditing its algorithms, opaque algorithmic carelessness arises. The platform is not responsible for the algorithms' content, but for its lack of transparency, which makes it harder for users, regulators, and courts to check diligence. Neglect violates accountability and requires a legal presumption of breach when an individual fails to collaborate or conceals information.

Comparative Doctrinal Models: Transplant Feasibility in India

This paper examines the European Union's Digital Services Act[31], the US's evolving view on Section 230 of the Communications Decency Act[32], and Japan's content moderation framework[33] to regulate algorithmic amplification and intermediary accountability. Despite their peculiarities, these strategies can help India overcome algorithmic curation in its judicial system.
The EU Digital Services Act shifts platforms from fixing concerns to preventing them. DSA requires Very Large Online Platforms (VLOPs) to conduct algorithmic risk assessments, submit transparency reports, and undergo scrutiny-based compliance verifications[34]. Misinformation, illicit content, and systemic manipulation are structural hazards that must be mitigated.
An ideologically driven DSA-like structure could boost structural accountability in India. For it to work, institutions, especially the Ministry of Electronics and Information Technology, must be improved. An autonomous statutory authority with legal and technological expertise must oversee risk audits, algorithmic disclosures, and enforcement actions in India.
Section 230 debates in the US show judicial-Congressional tensions. Section 230 shields internet sites from user-generated content liability. However, it is being criticised for protecting platforms even when their algorithms favor harmful content. The Gonzalez v. Google case examined whether algorithmic amplification varies from traditional publishing in immunity. The U.S. strategy is politically fractured and litigation-dependent, but it clearly states that algorithmic curation is not neutral and that platforms should not have protection when using algorithms for editorial decisions.

India should learn from the Section 230 scandal. Section 79 of the IT Act handles Indian intermediary liability like Section 230. U.S. courts grant platforms immunity, but Indian courts do not. They sometimes force platforms to respond to their knowledge. India may amend Section 79 of the IT Act, 2000 to exclude algorithmically prioritized material from platform safeguards, especially if platforms know about harmful practices. This would meet Section 230 reform goals. Japan, the third model, views regulation differently. The Ministry of Internal Affairs and Communications of Japan does not need comprehensive legislation to protect children and other vulnerable groups[35]. They issue immediate content moderation orders when needed. Administration, reaction, and fast risk mitigation characterize Japanese policy. It relies on the government to support state-platform self-regulation rather than the judiciary for law enforcement. India benefits from the Japanese model due to court backlogs and slow enforcement. Establishing ministerial oversight institutions that can collaborate with platforms in real time and provide non-binding but enforceable advise would require political will. Indian Press Information Bureau fact-checking units and MeitY alerts may provide a model for such systems.

Table 1. Comparative Legal Framework

Jurisdiction	Model/Framework	Key Features	Legal Philosophy	Transplant Feasibility in India
European Union	**Digital Services Act (DSA)**	- Mandates algorithmic risk assessments and independent audits- Imposes heightened obligations on Very Large Online Platforms (VLOPs)- Requires transparency in content moderation and systemic risk mitigation	Proactive, rights-based regulation focused on systemic accountability	**Moderately feasible**: Aligns with India's evolving public law doctrine. Requires statutory reform, a new regulatory body, and enforcement capacity. Conceptually robust for India but administratively intensive.
United States	**Section 230 (Reform Debates)**	- Originally provides broad immunity to platforms for third-party content- Reform efforts seek to limit immunity for algorithmic amplification- Courts exploring whether algorithmic design = editorial function	Litigation-driven, speech-protective, reactive in nature	**Partially adoptable**: Offers a doctrinal warning against overbroad safe harbour. India could amend Section 79 to exclude immunity where platforms curate harmful content knowingly. Less dependent on full-scale institutional change.
Japan	**Ministry-Led Content Oversight**	- Fast-track moderation advisories from Ministry of Internal Affairs- Focus on real-time removal, especially of harm to minors- Co-regulation between state and platforms	Administrative and preventive, centered on user protection	**Operationally feasible**: India can adapt this through MeitY-issued advisories and quick-response cyber cells. Works well within India's executive-driven regulatory style. Useful for time-sensitive threats like phishing or deepfakes.

Judicial And Legal Vaccum in India

India's legislative and judicial engagement with intermediary liability and content regulation has advanced in the previous decade, but it lacks a unified framework to handle algorithm-driven harms. A doctrinal study of significant court precedents and forthcoming regulatory episodes show that platforms' algorithmic architecture is increasingly separating them from legal accountability for harms. This section discusses algorithmic negligence legally.

In re Suo Motu Proceedings Regarding Circulation of Deepfake Content[36] (Delhi High Court, 2023), the Court addressed social media and Telegram deepfake pornography involving women prominent figures. The Court ordered platforms to remove such content and cooperate with law enforcement, concerned about the lack of algorithmic filters or AI-based safeguards. It criticized the platforms' persistent usage of user-driven abuse reporting despite their technological capabilities. Passive negligence in not using prophylactic algorithmic moderation is seen in this situation. The Bombay High Court heard deepfake-enabled KYC fraud petitions in 2023–24, concentrating on Meta-owned platform ads[37]. Petitioners showed that platforms' automated targeting algorithms showed scam adverts to vulnerable customers

despite repeated complaints. These systems profiled consumers using behavioral data and used trust-building visualizations like blue-tick badges and pseudo-official insignia. Even after notification, the platforms failed to recalibrate these algorithmic tools, demonstrating active algorithmic negligence; where design choices cause known damages. The Court directed the Ministry of Electronics and Information Technology (MeitY) but did not hold the platform directly liable due to statutory uncertainty under Section 79 of the IT Act, 2000.

A digital rights organization filed Writ Petition (Civil) No. 411 of 2022[38] with the Supreme Court of India, calling for systemic platform regulation improvements. Mandatory algorithmic audits, content governance policy disclosure, and recommendation engine transparency. The petition claims that unaccountable algorithmic prejudice fosters digital discrimination and violates fundamental rights under Articles 14 and 21. The forthcoming case may set a precedent for design-based liability in courts.

The Delhi High Court also found that search engines and algorithmic algorithms prioritize content, which could lead to liability[39]. While algorithmic curation changes the visibility and virality of damaging material, the Court ruled that liability cannot be imposed without legal modification. The intermediary liability framework, based on manual content control and post-facto compliance, cannot address automated risk transmission. The law must enforce an ex ante duty of care when platforms build, run, and profit from algorithms that influence public behavior and jeopardize user safety.

Recommendations

Indian intermediary liability law, particularly the Information Technology Act of 2000 and the Intermediary Guidelines of 2021 (amended in 2023), is reactive. These frameworks assumed that user-generated content caused most digital harm, thus notice-and-takedown procedures were implemented to remove harmful information after publication[40]. Modern challenges from platform algorithms' automated content amplification, profiling, and virality make this technique worthless. Existing technique ignores that design decisions might affect users without user participation.

The concept of negligence in Indian tort law focuses on people acting incorrectly. There must be a duty of care, a breach that causes injury, and a clear causal connection. There is no doctrinal consensus that platform-managed algorithmic systems can behave as risk agents. Thus, recommendation engines, automated targeting, and AI-driven content evaluation injuries constitute non-actionable carelessness.

Indian law must recognize algorithmic recklessness. Platforms should be required to identify and minimize automated system risks, especially those that disproportionately affect minors, women, and other vulnerable populations, under the Information Technology Act[41]. Systemic design flaws, algorithmic bias, and failing to reveal content governance criteria should be considered "negligence." This rule would bridge the gap between tort responsibility and automated platform harm. Second, the law must require algorithmic audits and transparency disclosures by an independent, legal-backed agency. This regulatory authority must enforce design standards, uncover algorithmic flaws, and order fixes. The courts must rethink carelessness in light of technology mediation. Judicial bodies must understand that algorithmic curation and amplification platforms cannot avoid culpability for predictable harm. As digital platforms influence public discussion and private experiences, the legal system must improve safety, transparency, and accountability.

CONCLUSION

This study examined how the indiscriminate application of algorithms by social media platforms such as Instagram and Facebook exacerbates criminality in India. The IT Act and the 2021 Intermediary Rules exemplify current legal instruments that emphasize takedown procedures. Nevertheless, they inadequately address the systemic function of algorithms in disseminating detrimental content. The EU's Digital Services Act, the recent judicial interpretations of Section 230 in the U.S., and Japan's audit-centric methodology collectively demonstrate that enhanced regulatory oversight is both feasible and necessary.

India must transition from a reactive approach to governance to a proactive one. This entails mandating algorithmic audits, ensuring transparency in recommendation algorithms, and establishing a tiered duty-of-care framework commensurate with the platform's scale and influence. Recognizing flaws in algorithmic design as legal liabilities is crucial to prevent platforms from facilitating cybercriminal activities. Enhancing these regulations will more effectively protect consumers, increase accountability in democracy, and align India with evolving global standards.

REFRENCES

1. Internet and Mobile Association of India (IAMAI), Digital in India: State of Internet 2025, (2024)".
2. "National Crime Records Bureau, Crime in India 2019 data summary (reported by NDTV, 30 Sep 2020); Business Standard, "11% jump in cyber crime in 2022" (11 Feb 2022).
3. Press Information Bureau, CERT-IN issues advisory on AI-based cyber threats, (Government of India, May 2023).
4. UK House of Commons Science, Innovation and Technology Committee, Online Harms and the Role of Social Media Algorithms (HC 441, 2024) https://publications.parliament.uk/pa/cm5901/cmselect/cmsctech/441/report.html.
5. 'Court Allows Social Media Harm Lawsuits to Proceed' Time (28 June 2025) https://time.com/7295323/social-media-case-instagram-tiktok/.
6. Nate Raymond, 'Reddit, YouTube must face lawsuits claiming they enabled Buffalo mass shooter' Reuters (19 March 2024) https://www.reuters.com/legal/reddit-youtube-must-face-lawsuits-claiming-they-enabled-buffalo-mass-shooter-2024-03-19/.
7. UK House of Commons Science, Innovation and Technology Committee, Second Report of Session 2024–25: Social Media, Misinformation and Harmful Algorithms, HC 441 (2024) §§ Summary and Introduction.
8. Smitha Milli et al., Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media (pre-registered algorithmic audit on Twitter) (2023), available at: https://arxiv.org/abs/2305.16941, The Guardian, "Social Media Algorithms 'Amplifying Misogynistic Content'" (2024), available at: https://www.theguardian.com/media/2024/feb/06/social-media-algorithms-amplifying-misogynistic-content.
9. Daniel Castro and Ash Johnson, How Other Countries Have Dealt With Intermediary Liability, Information Technology and Innovation Foundation, 22 February 2021.
10. India News Explained: WhatsApp vs Indian Government on New IT Rules, Outlook India, 26 May 2021.
11. Shreya Singhal v. Union of India, (2015) 5 SCC 1".
12. "Global Witness, Facebook's Political Ad Failures in India: A Technical Assessment, 2023, https://www.globalwitness.org/en/campaigns/digital-threats/facebook-political-ads-india/ (last accessed 11 July 2025).
13. Ibid.
14. In Re: Regulation of Algorithmic Bias in Social Media Platforms, Writ Petition (Civil) No. 411 of 2022, pending before the Supreme Court of India.
15. Daniel Castro and Ash Johnson, How Other Countries Have Dealt With Intermediary Liability, Information Technology and Innovation Foundation, 22 February 2021.
16. Ibid.
17. The Information Technology Act, 2000, s. 79".
18. "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023.
19. S. Khan, 'Algorithmic Accountability in India: Bridging the Gap between Regulation and Reality' (2024) 14 Indian Journal of Law and Technology 22, R. Singh, J. Cobbe and L. Norval, 'Clarifying and Mapping the Roles of Transparency in Accountability Mechanisms for Algorithmic Decision-Making' (2018) 31 Philosophy & Technology 1.
20. Gausen, L., Hempel, L., Klenk, M. and Leistert, O., 'Transparency as Regulation: The Digital Services Act and the Promises of Sociotechnical Oversight', Internet Policy Review, 13(1), 2024.
21. Communications Decency Act, 47 U.S.C. § 230 (1996).
22. Gonzalez v. Google LLC, 598 U.S. ___ (2023), Supreme Court of the United States.
23. Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015); J.M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2017) 51 UC Davis Law Review 1149.
24. Pareek, A. and Sole, M**.,** "Amplification and Accountability: Rethinking Platform Liability under Indian Law", Indian Journal of Law and Technology, Vol. 17, 2021.
25. Donoghue v Stevenson [1932] AC 562 (HL); Municipal Corporation of Delhi v Subhagwanti AIR 1966 SC 1750; Ratanlal and Dhirajlal, The Law of Torts (LexisNexis 2022) 400–405".
26. M/s Spring Meadows Hospital v. Harjol Ahluwalia, (1998) 4 SCC 39.
27. "Information Technology Act 2000, s 79; Shreya Singhal v Union of India (2015) 5 SCC 1.
28. Google India Pvt. Ltd. v. Visaka Industries, 2019 SCC OnLine TS 206.
29. Ramesh Subramanian and Eddan Katz, The Negligence Liability of Internet Intermediaries (UNESCO 2016) 11–14; Tal Zarsky, 'A Duty to Monitor? Algorithmic Harm and Intermediary Responsibility' (2021) 34(3) Harvard Journal of Law & Technology 257".

30. "Parliamentary Standing Committee on Information Technology, Report on Safeguarding Citizens' Rights and Preventing Misuse of Social Media Platforms, Seventeenth Lok Sabha, 2021, Ministry of Electronics and Information Technology, Government of India.
31. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1, arts 26–27.
32. Communications Decency Act, 47 U.S.C. § 230 (1996).
33. Ministry of Internal Affairs and Communications (Japan), Overview of the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Sender (2023); MIC Japan, 'AI Moderation Evaluation Framework Launched', Press Release, 14 July 2023.
34. Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) [2022] OJ L277/1, arts 15–30".
35. "Ministry of Internal Affairs and Communications (Japan), Final Report on Platform Service Governance—Ensuring Safe and Secure Use of Digital Platforms, 2022, available at https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/2204_report.pdf"
36. "In re Suo Motu Proceedings Regarding Circulation of Deepfake Content, Suo Motu W.P. (Crl.) No. 2794 of 2023, decided on 7 November 2023 (Delhi HC).
37. Praja Foundation v Union of India, PIL (L) No. 3201 of 2023, decided on 18 December 2023 (Bombay HC).
38. Internet Freedom Foundation v Union of India, Writ Petition (Civil) No. 411 of 2022".
39. "Google India Pvt. Ltd. v Visaka Industries Ltd., 2019 SCC OnLine Del 8494.
40. Khan, A., "Algorithmic Accountability in India: Rethinking Due Diligence in Platform Governance," Indian Journal of Law and Technology, Vol. 19, 2024.
41. Information Technology Act, 2000, ss 66E, 67B, 69A; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr 3(1)(b), 3(1)(j), and 4(4)."