REGULATING SOCIAL COMMERCE IN INDIA: ARE EXISTING CORPORATE AND CONSUMER PROTECTION LAWS ADEQUATE?

Ashima Gupta, The ICFAI University

Dr. Susanta Kumar Sadangi, Associate Professor (Law), The ICFAI University

ABSTRACT

Social commerce is reshaping India's digital economy in ways that few anticipated even a decade ago. By weaving shopping directly into everyday social media use through platforms like Instagram, Facebook, and WhatsApp it has blurred the line between browsing and buying. A product can be discovered through a friend's post, recommended by a trusted influencer, and purchased without ever leaving the app. That seamlessness is its power. But it is also the source of its regulatory complexity.[1]

Unlike organized e-commerce platforms such as Amazon or Flipkart, social commerce thrives on informality. Many sellers are home-based entrepreneurs or micro-vendors with no formal business registration. Transactions often happen through private chats, Instagram DMs, or WhatsApp groups outside the reach of conventional marketplace rules. This informality creates real risks: misleading advertisements, counterfeit goods, data misuse, and near-impossible complaint redressal when something goes wrong.[2]

This paper asks a pointed question: do India's existing laws actually cover this? It looks carefully at the Consumer Protection Act, 2019, the Consumer Protection (E-commerce) Rules, 2020, the Companies Act, 2013, and the Information Technology Act, 2000 testing each against the realities of social commerce. The answer, in short, is that these laws offer a foundation but fall well short of what is needed.[3]

Targeted reforms are necessary. Clearer legal definitions for social commerce, firmer compliance duties for platforms, stronger complaint mechanisms, and alignment with forthcoming data protection law all of these

[1] Ministry of Electronics and Information Technology, Annual Report 2022–23 (Government of India, 2023). See also NASSCOM, India Digital Commerce Report 2023

[2] OECD, "Protecting Consumers in Peer Platform Markets" (OECD Digital Economy Papers No. 253, 2016).

[3] Prashant Reddy T, "Consumer Protection in Digital Markets" (2021) 6 Indian Journal of Law and Technology 45.

are essential if India wants social commerce to grow within a framework that genuinely protects consumers and holds participants accountable.

Keywords: Social Commerce, Digital Marketplace Regulation, Digital Economy, Consumer Protection, Corporate Governance, Informal Digital Sellers, Influencer Marketing, Intermediary Liability.

INTRODUCTION

Something has quietly changed about the way millions of Indians shop. They are not typing search queries into Amazon or browsing Flipkart catalogues they are scrolling through Instagram reels, joining WhatsApp groups run by local sellers, and buying products recommended by YouTubers they trust. This shift has a name: social commerce. And it is growing fast.[4]

The conditions for this growth have been building for years. Cheap mobile data, the spread of affordable smartphones, and the rise of UPI have collectively brought India's informal economy online in large numbers. Small sellers who once depended on physical markets or word-of-mouth now run product pages on social media, take orders through chat, and accept payment through digital wallets. No storefront, no warehouse, sometimes no formal registration just a phone and a following.[5]

That informality is the heart of the regulatory problem. When a buyer purchases a saree from a verified e-commerce seller, there is a paper trail: an invoice, a tracked delivery, a return policy, a grievance officer. When the same buyer orders from an Instagram account, there may be none of these. If the product never arrives, or turns out to be counterfeit, there is often no clear path to a remedy.[6]

India already has several laws that touch digital commerce. The Consumer Protection Act, 2019 extended consumer rights to online transactions. The E-commerce Rules, 2020 imposed specific obligations on marketplace operators. The IT Act, 2000 established the legal framework for digital transactions and set out when platforms could claim immunity for user-

[4] RedSeer Strategy Consultants, "Social Commerce in India" (2022) <https://redseer.com> accessed 12 March 2025.
[5] Telecom Regulatory Authority of India, Telecom Subscription Data (March 2024).
[6] Competition Commission of India, Market Study on E-Commerce in India (2020) 27

generated content. The Companies Act, 2013 governs corporate conduct for registered entities.[7]

The problem is that these laws were designed with organized digital marketplaces in mind. They assume identifiable sellers, documented transactions, and platforms that function as structured marketplaces rather than open communication networks. Social commerce does not fit that mould. A social media platform primarily built for communication does not sit comfortably in a regulatory category designed for Amazon.[8]

Influencer marketing adds another layer of complexity. When a content creator with two million followers recommends a skincare product in what looks like a personal opinion piece but is actually a paid promotion, consumers may have no idea they are being advertised to. The Advertising Standards Council of India has issued disclosure guidelines, but compliance is patchy and enforcement is harder still.[9]

This paper works through these issues systematically. It maps the current legal framework, identifies where the gaps lie, looks at how other countries are handling comparable challenges, and proposes reforms that are practical rather than merely aspirational. The underlying argument is straightforward: India's existing laws are not enough, and the gap between the law as written and the reality of social commerce is one that consumers often the most vulnerable participants in these transactions are currently paying for.

OBJECTIVE OF THE STUDY

This paper investigates whether India's current legal framework is genuinely fit for the task of regulating social commerce. The core question is existing corporate and consumer protection laws adequate? drives the analysis throughout.[10]

The specific objectives are:

- To trace the growth of social commerce in India and understand what makes it structurally different from traditional e-commerce.

[7] Consumer Protection Act 2019; Information Technology Act 2000; Companies Act 2013; Consumer Protection (E-commerce) Rules 2020
[8] Usha Ramanathan, "Platforms and Liability in India" (2021) 33 National Law School of India Review 12.
[9] Advertising Standards Council of India, Guidelines for Influencer Advertising in Digital Media (2021).
[10] Indian Law Institute, Legal Research Methodology (ILI Press, 2019) ch 3

- To assess how consumer protection laws particularly the Consumer Protection Act, 2019 and the E-commerce Rules, 2020 apply (and fail to apply) to social commerce transactions.

- To examine the role of corporate governance frameworks in holding platform operators accountable.

- To identify the legal gaps that arise from the informal and decentralized nature of social commerce.

- To analyze intermediary liability under the IT Act, 2000 and consider whether the current safe harbor framework remains appropriate as platforms become more commercially active.

- To draw on comparative regulatory experience in the EU, China, the US, and other jurisdictions for lessons India can adapt.

- To propose concrete legal and policy reforms that would strengthen consumer protection without stifling innovation.

RESEARCH METHODOLOGY

This study uses a doctrinal and analytical research approach. It examines legal texts, regulatory instruments, judicial decisions, and academic literature to assess how well India's laws address social commerce. The research is qualitative in character and relies entirely on secondary sources.[11]

These sources include:

- Primary legislation: The Consumer Protection Act, 2019; the Consumer Protection (E-commerce) Rules, 2020; the Companies Act, 2013; the Information Technology Act, 2000; and the Competition Act, 2002.

- Case law and regulatory decisions from consumer courts, the Competition Commission

[11] S N Jain, "Doctrinal and Non-Doctrinal Research" in Indian Law Institute, Research Methods in Law (ILI Press, 2018) 17

of India, and relevant judicial bodies.

- Government reports and policy papers from the Ministry of Consumer Affairs and other regulatory bodies.
- Academic books, journal articles, and research papers on digital commerce, platform regulation, and consumer protection law.
- Reliable online sources, legal databases, and industry analyses tracking social commerce trends.

LEGAL FRAMEWORK GOVERNING SOCIAL COMMERCE IN INDIA

There is no single law in India that directly addresses social commerce. Instead, the regulatory landscape is assembled from several overlapping statutes consumer protection law, corporate law, information technology regulation, competition law, and advertising standards. Individually, each statute has a legitimate role. Together, they leave meaningful gaps when applied to the informal, conversation-driven world of social commerce.[12]

1. Consumer Protection Law

The Consumer Protection Act, 2019 is the most directly relevant statute. It updated India's consumer protection framework for the digital age, extending coverage to e-commerce transactions and introducing provisions against unfair trade practices in online markets including misleading advertisements, inaccurate product descriptions, and deceptive pricing.[13] The Act creates a tiered structure of Consumer Dispute Redressal Commissions at the district, state, and national levels. It also introduced the concept of product liability, allowing consumers to claim compensation when defective products cause harm a provision that can, in principle, reach social commerce sellers.[14]

A significant institutional development under the Act is the establishment of the Central Consumer Protection Authority (CCPA), which has power to investigate unfair trade practices, act against misleading advertisements, and mandate product recalls. In theory, the CCPA's

[12] Nandan Kamath, Law Relating to Computers, Internet and E-Commerce (Universal Law Publishing, 5th edn, 2020) 214.
[13] Consumer Protection Act 2019, ss 2(7), 2(47), 18, 21
[14] ibid, s 84 (product liability against manufacturers and sellers).

jurisdiction extends to social commerce. In practice, it faces serious enforcement challenges when sellers are unregistered, anonymous, or operating across state lines through informal channels.[15]

2. Consumer Protection (E-commerce) Rules, 2020

The E-commerce Rules, 2020 build on the Consumer Protection Act by setting out specific duties for online marketplace entities. These include obligations to display seller details, provide transparent pricing and return policies, appoint a grievance officer, and resolve consumer complaints within defined timeframes.[16]

These Rules work reasonably well for organized platforms where sellers register, list products through structured catalogues, and transact within a regulated environment. They are poorly matched to social commerce. A seller running a business through Instagram Stories or a WhatsApp broadcast list does not obviously fit the definition of an "e-commerce entity." The platform facilitating the transaction does not obviously qualify as a "marketplace entity" either it was built for communication, not commerce.[17]

This definitional ambiguity means that large swathes of social commerce activity fall between the Rules' categories, creating a practical enforcement gap that consumers currently bear the consequences of.

3. Information Technology Act, 2000, and Intermediary Liability

The IT Act, 2000 provides the foundational legal framework for digital transactions. It gives legal recognition to electronic records and contracts, enabling online commerce to operate within a legally accepted structure.[18]

Section 79 of the Act grants "safe harbor" immunity to intermediaries for third-party content on their platforms, provided they comply with due diligence requirements and do not themselves participate in or initiate the unlawful activity. Social media platforms Instagram,

[15] ibid, ss 10–15 (establishment and powers of the Central Consumer Protection Authority).
[16] Consumer Protection (E-commerce) Rules 2020, rr 4–5
[17] Apar Gupta, "E-Commerce Regulation and the Information Technology Act" (2020) 55 Economic and Political Weekly 34
[18] Information Technology Act 2000, ss 2, 10A (legal recognition of electronic records and contracts).

Facebook, WhatsApp are typically classified as intermediaries under this framework.[19]

The problem is that these platforms are no longer purely passive. They have built in-app shopping features, product tagging, influencer partnership tools, and targeted advertising algorithms that actively facilitate and profit from commercial transactions. At what point does a platform cease to be a neutral intermediary and become a marketplace operator with corresponding responsibilities? The current law provides no clear answer and courts have yet to settle it definitively.[20]

4. Corporate Governance: Companies Act, 2013

The Companies Act, 2013 governs corporate conduct for registered entities operating in India, including large digital platform companies. It imposes obligations concerning financial disclosure, board governance, and statutory compliance that promote transparency and accountability at the corporate level.[21]

The limitation is that the Act only reaches formal corporate entities. The vast majority of social commerce sellers are individuals, home-based vendors, or unregistered micro-enterprises who operate entirely outside its scope. For these sellers, there is no corporate governance framework, no mandatory disclosure, and no structured accountability mechanism. This leaves consumers dealing with informal vendors in a legal grey zone.[22]

5. Competition Law

The Competition Act, 2002 addresses anti-competitive conduct in digital markets, and the Competition Commission of India has scrutinized algorithmic bias, preferential treatment of sellers, and exclusionary practices in online marketplaces.[23]

Social commerce raises comparable concerns. When a platform's algorithm systematically favors certain sellers or products whether based on payment, affiliation, or opaque criteria it can distort competition in ways that harm both rival sellers and consumers. As social commerce

[19] ibid, s 79 (safe harbour for intermediaries).
[20] Shreya Singhal v Union of India (2015) 5 SCC 1 (Supreme Court of India, interpreting s 79 of the IT Act).
[21] Companies Act 2013, ss 134, 177 (financial disclosure and board oversight obligations).
[22] Competition Commission of India, Market Study on E-Commerce in India (n 6) 38.
[23] Competition Act 2002, ss 3, 4. See also In Re: Artificial Hiking of Prices on E-commerce Websites, Case No 99 of 2016 (CCI).

grows, competition law will need to engage more directly with these dynamics.

6. Data Protection

Social commerce is fundamentally data-driven. Platforms collect detailed personal information browsing patterns, purchase history, location data, social connections and use it to target consumers with personalized advertisements and product recommendations. The more granular the data, the more effective the marketing.[24]

Current data protection regulation under the IT Act, 2000 and its associated rules is widely regarded as inadequate for this environment. The Digital Personal Data Protection Act, 2023 represents a significant step forward, but its full implementation and the notification of relevant rules remain pending. Until a robust data protection framework is fully operational, consumers in social commerce have limited rights over how their personal information is collected, used, and shared.[25]

7. Advertising and Influencer Marketing

The Advertising Standards Council of India (ASCI) has issued guidelines requiring influencers to clearly disclose paid partnerships and sponsored content using labels such as #ad, #sponsored, or #collab. These guidelines represent a serious attempt to bring transparency to influencer marketing.[26]

Their effectiveness is constrained by several practical realities. Compliance is voluntary rather than legally mandated. Disclosure labels are often buried, minimized, or absent. Content disappears quickly on platforms built around ephemeral posts and Stories. And the sheer volume of sponsored content across thousands of influencers posting daily makes systematic monitoring by a single industry body nearly impossible.[27]

KEY REGULATORY CHALLENGES

Even a generous reading of India's existing legal framework reveals serious structural

[24] Saikat Datta, "Data Economy and Social Commerce" (2022) 19 NUJS Law Review 88.
[25] Digital Personal Data Protection Act 2023. As of the date of this paper, the secondary rules required for full operationalisation had not yet been notified
[26] ASCI, Guidelines for Influencer Advertising in Digital Media (n 9).
[27] Supra n 26; see also Advertising Standards Council of India, Annual Complaints Report 2022–23.

weaknesses when it comes to social commerce. The challenges are not merely technical they reflect a fundamental mismatch between rules designed for organized digital marketplaces and the informal, dispersed reality of social commerce.[28]

1. No Clear Legal Definition of Social Commerce

Perhaps the most basic problem is that social commerce has no legal definition in India. Existing e-commerce rules were drafted with structured, centralized platforms in mind. Social commerce operates through chat messages, influencer posts, private groups, and live streams activities that sit awkwardly in every existing regulatory category.[29]

Without a clear definition, it is difficult to determine who is regulated, under what rules, and to what standard. Platforms, sellers, and influencers can each credibly argue that they fall outside the relevant obligations. Consumers, who have the least legal sophistication, are left to navigate the consequences.

2. Anonymous and Unregistered Sellers

A structural feature of social commerce is the prevalence of sellers who operate without formal registration. Many run their businesses through personal social media accounts with no GST number, no business registration, and no traceable legal identity. If a buyer receives a defective product or nothing at all tracking down the seller can be effectively impossible.[30]

Unlike traditional e-commerce platforms that require seller onboarding and verification before a listing goes live, social media platforms impose no such requirement. A new account can begin selling within minutes of being created and disappear just as quickly once problems arise.

3. Grievance Redressal in Practice

Consumer law gives buyers rights. But rights are only meaningful if there is a practical mechanism for enforcing them. In social commerce, that mechanism is often absent.[31]

Traditional e-commerce transactions generate digital evidence: order confirmations, invoices,

[28] OECD, "Protecting Consumers in Peer Platform Markets" (n 2) 8–12
[29] Pavan Duggal, "Social Commerce and the Regulatory Vacuum in India" (2022) 14 Journal of Cyberlaw 1
[30] National Consumer Disputes Redressal Commission, Annual Report 2022–23 (Government of India) 24 (reporting increase in e-commerce complaints with unidentifiable sellers).
[31] Consumer Protection Act 2019, s 36 (complaint procedure before district commissions).

delivery notifications, payment receipts. Social commerce transactions frequently leave none of these. A sale completed through WhatsApp voice messages and a bank transfer may be nearly impossible to document for the purposes of a consumer court complaint. Even where documentation exists, the consumer forum system is slow, under-resourced, and primarily designed for disputes with identifiable registered businesses.

4. Influencer Marketing and Deceptive Promotion

Influencer marketing is central to social commerce and is also its most visible accountability problem. When an influencer with a large following endorses a product enthusiastically, many followers will not know and will not think to ask whether the endorsement was paid for. The lines between personal recommendation and commercial advertisement are deliberately blurred.[32]

ASCI guidelines require disclosure, but compliance is inconsistent and enforcement is limited. Paid partnerships are sometimes flagged with small, obscure labels; sometimes not at all. Products are occasionally endorsed by influencers who have not used them or who make claims that could not survive legal scrutiny if made in a traditional advertisement.[33]

5. Platform Liability: Where Does Responsibility Lie?

One of the hardest questions in social commerce regulation is how much responsibility platforms should bear for commercial activity that takes place on their infrastructure. Under the current IT Act framework, the answer is: not much. The safe harbor provision of Section 79 largely insulates platforms from liability for third-party content provided they meet basic due diligence obligations.[34]

The difficulty is that major platforms are no longer passive. Facebook has Shops. Instagram has product tagging and checkout. WhatsApp Business enables commercial messaging at scale. These features generate revenue for the platforms and facilitate consumer harm when misused. There is a reasonable argument that platforms profiting from commercial activity on their infrastructure should bear proportionate responsibility for the quality of that activity but the

[32] Priyanka Srinivasan, "Influencer Marketing and Consumer Deception" (2021) 12 Indian Journal of Comparative Law 110
[33] Supra n 26
[34] Information Technology Act 2000, s 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

current law does not clearly impose this.

6. Data Privacy

The data practices of social commerce platforms raise genuine privacy concerns. Personal data collected through social engagement likes, searches, connections, time spent viewing content feeds into advertising algorithms that target consumers with increasing precision. Users generally have little visibility into how this data is collected, processed, or shared.[35]

The IT Act's data protection provisions were drafted before algorithmic targeting at this scale existed. The Digital Personal Data Protection Act, 2023 will eventually provide a more robust framework but until it is fully implemented, consumers remain inadequately protected against data exploitation in the social commerce context.

CASE STUDIES AND ENFORCEMENT INSTANCES

Abstract legal analysis only goes so far. Looking at actual enforcement activity cases that have been investigated, complaints that have been filed, and regulatory actions that have been taken gives a more grounded picture of how the current framework operates in practice.[36]

1. Competition Commission of India: E-commerce Investigations

In 2020, the CCI launched an inquiry into the commercial practices of Amazon India and Flipkart, examining allegations of anti-competitive conduct including preferential treatment for certain sellers, exclusive product arrangements, and aggressive discounting strategies that may have damaged competition in the online retail market.[37]

The direct focus was traditional e-commerce, but the implications extend to social commerce. Social commerce sellers frequently use the same logistics networks and payment systems as organized marketplace sellers. As social commerce platforms integrate in-app shopping and product discovery features, the competition concerns that arose in the Amazon/Flipkart context algorithmic favoritism, data advantages, market foreclosure are increasingly relevant here too.

[35] Internet Freedom Foundation, "Data and Discrimination in the Digital Economy" (IFF Working Paper, 2022).
[36] Indian Law Institute, Law and Social Research (ILI Press, 2016) 89 (on the use of case studies in legal analysis).
[37] In Re: Alleged Anti-Competitive Practices by Amazon Seller Services and Flipkart Internet, Case Nos 40 and 41 of 2019 (CCI, order of 13 January 2020).

2. Consumer Fraud via Social Media Accounts

Consumer courts and police cybercrime units across India have dealt with a significant and growing volume of complaints involving fraudulent social media sellers. The pattern is typically consistent: a social media account often on Instagram or Facebook advertises attractive products at low prices. Buyers pay through UPI or bank transfer. The seller either delivers counterfeit goods or disappears without delivering anything.[38]

Under the Consumer Protection Act, 2019, affected buyers technically have the right to file a complaint with a consumer dispute redressal commission. In practice, these cases are difficult to pursue. The seller is often untraceable. There is no invoice. The transaction has no paper trail. The platform claims intermediary immunity. The consumer, having lost perhaps a few hundred or a few thousand rupees, frequently has no practical path to a remedy.[39]

This is not an edge case or an exceptional situation. It is a routine feature of social commerce transactions in India, and it represents a systematic failure of consumer protection.

3. ASCI Action Against Influencer Non-Disclosure

The Advertising Standards Council of India has become increasingly active in monitoring influencer advertising. It has issued notices and warnings to influencers and brands that failed to disclose paid partnerships or made unsubstantiated product claims particularly in sectors like health supplements, beauty products, and financial services.[40]

ASCI's Influencer Advertising Guidelines require clear labelling of sponsored content. But compliance remains uneven. Monitoring a small number of well-known influencers is manageable; systematically monitoring tens of thousands of micro- and Nano-influencers posting across multiple platforms is not. And because ASCI's powers are advisory rather than statutory, the consequences of non-compliance are limited.[41]

4. Cybercrime Cases Involving Social Commerce Scams

Police cybercrime divisions have recorded a steady rise in complaints related to fake social

[38] National Cybercrime Reporting Portal, Annual Statistics 2022–23 (Ministry of Home Affairs, 2023
[39] Consumer Protection Act 2019, s 2(1)(d) (definition of "consumer" applicable to digital purchases).
[40] ASCI, "Violations Report: Influencer Marketing" (2022–23 Quarterly Monitoring Report).
[41] ibid. For the limits of self-regulatory enforcement, see generally Christopher Marsden, Internet Co-Regulation (Cambridge University Press, 2011) 45

media shops. Fraudsters create pages mimicking legitimate brands, offer products at unrealistically low prices, collect payments through digital platforms, and vanish. WhatsApp is commonly used to manage customer interactions in these schemes, since its private chat format makes monitoring by authorities extremely difficult.[42]

Awareness campaigns have been run, and some arrests have been made, but the enforcement challenge is significant. Fraudulent accounts can be created quickly, operated briefly, and abandoned without leaving meaningful traces. The speed at which social commerce operates is also the speed at which fraud within it can be committed.

5. Platform-Enabled Social Commerce: The Meesho Model

The growth of platforms like Meesho illustrates both the potential and the regulatory complexity of structured social commerce. Meesho enables individuals to act as resellers by sharing product catalogues through social media earning a margin on each sale without holding inventory. The platform handles logistics, payment processing, and returns.[43]

This model has empowered millions of people, particularly women in smaller towns and cities, to earn income through digital commerce. But it also raises regulatory questions. Does Meesho function as an e-commerce marketplace (and therefore fall under the E-commerce Rules, 2020) or as an intermediary? The classification matters enormously for consumer protection obligations and it is not yet definitively resolved.[44]

ANALYSIS: ARE EXISTING LAWS ADEQUATE?

The honest answer is: not adequately. India's current legal framework provides a partial response to the challenges of social commerce. It covers some situations, reaches some actors, and offers some remedies. But the coverage is patchy, the enforcement is weak, and the framework was not designed with social commerce in mind.[45]

1. Consumer Protection Act, 2019

The Act is conceptually sound. It extended consumer rights to digital transactions, introduced

[42] Cyber Peace Foundation, "Social Media and Online Fraud in India" (Research Report, 2023).
[43] Meesho, Annual Report 2022–23 <https://meesho.com/about> accessed 12 March 2025
[44] Consumer Protection (E-commerce) Rules 2020, r 2(c) (definition of "marketplace e-commerce entity").
[45] Comparative analysis drawing on OECD, Consumer Protection Enforcement in a Global Digital Marketplace (2018).

product liability, and created the CCPA. In a world where social commerce sellers are identifiable and transactions are documented, it would provide meaningful protection.[46]

The world of social commerce is often not that world. The Act assumes that you can find the seller, that you have a receipt, and that there is a grievance officer to complain to. In practice, social commerce transactions frequently tick none of these boxes. The law exists on paper, but the preconditions for using it are often absent.

2. E-commerce Rules, 2020

The Rules work for Amazon. They work less well for a seller running a business through Instagram DMs. The Rules were drafted for organized marketplaces with registered sellers, structured product listings, and defined complaint mechanisms. Social commerce sellers operating through personal accounts, private groups, and messaging apps are not obviously captured by the Rules' definitions.[47]

Key obligations under the Rules seller verification, transparent pricing, accessible grievance mechanisms are absent or unenforced in much of the social commerce ecosystem. The regulatory void is significant.[48]

3. IT Act, 2000: The Safe Harbor Problem

Section 79's safe harbor was designed for a generation of platforms that primarily hosted user-generated content without financial involvement in its commercial exploitation. That design assumption no longer holds. Platforms now build and monetize commercial features; their algorithms actively steer consumer attention toward products and sellers; their infrastructure is the marketplace, not merely the medium.[49]

The question of whether a platform that profits from enabling commerce should retain full safe harbor immunity is not one the current law answers satisfactorily. An update to the intermediary liability framework one that conditions immunity on the nature and extent of the

[46] Consumer Protection Act 2019, s 2(7) (definition of "consumer" inclusive of digital transactions).
[47] Consumer Protection (E-commerce) Rules 2020, rr 4–5; see analysis in CCI, Market Study on E-Commerce (n 6) 45–50
[48] ibid
[49] Information Technology Act 2000, s 79; cf European Commission, Digital Services Act (Regulation (EU) 2022/2065), arts 5–9 (tiered liability for platforms).

platform's commercial involvement is overdue.

4. Companies Act, 2013

Corporate governance obligations reach platform companies but not the individual sellers who constitute the commercial layer of social commerce. For most consumer disputes in social commerce, the Companies Act is simply irrelevant. The sellers who cause harm are not corporate entities subject to its requirements.[50]

This is a structural gap, not a drafting oversight. The Act was built for a corporate economy; social commerce operates significantly outside it.

5. Data Privacy

The data protection deficit is acute. Social commerce platforms harvest detailed personal data to power targeted advertising and algorithmic recommendations. The IT Act's protections are minimal. The Digital Personal Data Protection Act, 2023 offers a more appropriate framework, but until it is fully operative with detailed rules and active enforcement, the gap remains.[51]

6. Enforcement Capability

Even where the law is theoretically adequate, enforcement faces practical barriers. Millions of social commerce transactions occur daily across dozens of platforms. Consumer forums are backlogged. Cybercrime units are stretched. Advertising regulators lack statutory powers. Regulators do not have the real-time digital monitoring tools that effective enforcement in this space requires.[52]

The conclusion of this analysis is that India's regulatory framework for social commerce is not merely incomplete in specific provisions—it is structurally misaligned with the activity it is supposed to govern.

INTERNATIONAL COMPARATIVE INSIGHTS

Other jurisdictions are grappling with the same challenges, and some have developed

[50] Companies Act 2013, s 2(20) (definition of "company" confined to registered corporate bodies).
[51] Digital Personal Data Protection Act 2023 (n 25
[52] National Consumer Helpline, Complaint Data Analysis 2022–23 (Ministry of Consumer Affairs, 2023).

regulatory responses that India can learn from. No model is perfectly transferable the scale of India's informal economy, its regulatory capacity, and its constitutional structure are distinctive. But the direction of travel in more advanced regulatory systems offers useful guidance.[53]

1. European Union: Rights-Based Platform Regulation

The EU has built the most comprehensive digital regulatory architecture currently in operation, centered on the Digital Services Act (DSA) and the Digital Markets Act (DMA).[54]

The DSA establishes a tiered framework in which obligations scale with platform size. Very Large Online Platforms must conduct mandatory risk assessments, implement risk mitigation measures, submit to independent audits, and provide users with alternatives to personalized recommendations. The Know Your Business Customer requirement obligates platforms to verify the identity of traders selling through their infrastructure.[55]

The DMA targets platforms designated as "gatekeepers" large digital intermediaries with structural market power and imposes ex-ante obligations on them, including prohibitions on self-preferencing, data portability requirements, and interoperability mandates.[56]

Underpinning both instruments is the General Data Protection Regulation (GDPR), which gives consumers meaningful rights over their personal data including rights of access, erasure, and portability, with strict consent requirements for data collection and use.[57]

The EU model is demanding in its compliance requirements, and there are legitimate concerns about its burden on smaller platforms. But its core insight that platform size should determine regulatory obligation, and that data protection and consumer protection need to be integrated offers a sound template for India to adapt.

2. China: Sector-Specific Direct Regulation

China has taken a more interventionist approach, particularly in relation to live-streaming

[53] Indian Law Institute, Comparative Law and Legal Research (ILI Press, 2017) 33.
[54] Digital Services Act (EU) 2022/2065; Digital Markets Act (EU) 2022/1925
[55] Digital Services Act (n 54), arts 26–35 (obligations for very large online platforms).
[56] Digital Markets Act (n 54), arts 5–7 (obligations for designated gatekeepers).
[57] General Data Protection Regulation (EU) 2016/679, arts 7, 17, 20 (consent, erasure, and portability).

commerce, which closely mirrors India's social commerce landscape in many respects.[58]

Chinese regulation explicitly recognizes live-streaming and social commerce as distinct commercial sectors subject to dedicated rules rather than general e-commerce legislation. Liability is clearly allocated among platforms, sellers, and hosts and influencers. Platforms must monitor live streams in real time, remove non-compliant content promptly, and maintain transaction records for audit purposes. Algorithmic discrimination and data-driven price manipulation are explicitly prohibited.[59] The enforcement record in China is substantially stronger than in India, though this partly reflects a political and institutional context that is not replicable. The structural lessons clear definitions, explicit liability allocation, mandatory transaction documentation are nevertheless relevant.

3. United States: Market-Led with Targeted Enforcement

The US approach is more permissive in design, reflecting a policy preference for innovation and limited regulatory intervention. Section 230 of the Communications Decency Act provides platforms with broad immunity for third-party content, similar in effect (though broader in scope) to India's Section 79.[60]

The Federal Trade Commission plays an active enforcement role, particularly in relation to deceptive advertising and influencer disclosure. The FTC has pursued both brands and individual influencers for failure to disclose paid partnerships and for making unsubstantiated product claims, creating a deterrent effect that ASCI's advisory-only model cannot match.[61]

The US model has been criticized for under protecting consumers relative to the EU. But its FTC enforcement approach targeted, evidence-driven, with statutory penalties offers India a model for strengthening advertising regulation without requiring comprehensive legislative reform.

4. UK and Singapore

The UK is developing an Online Safety framework that focuses on platform accountability for harmful content, integrating elements of EU-style platform responsibility with national

[58] Measures for the Administration of Live-Streaming Marketing Activities (China, 2021).
[59] ibid, arts 14–16 (liability of hosts, sellers, and platforms).
[60] Communications Decency Act 1996 (US), s 230
[61] Federal Trade Commission, Endorsement Guides: What People Are Asking (FTC, 2023).

enforcement flexibility. Singapore's approach emphasizes regulatory clarity and proportionality, using plain guidance and predictable rules to encourage compliance rather than relying primarily on penalties.[62]

5. What India Lacks

The comparative picture highlights four significant gaps in India's approach. First, there is no dedicated legal framework for social commerce as a distinct commercial activity. Second, the safe harbor framework is more protective of platforms than the EU model and lacks the conditionality that platform responsibility demands. Third, enforcement mechanisms in terms of monitoring capacity, penalty severity, and inter-agency coordination are inadequate for the scale of the problem. Fourth, data protection integration, essential to any modern digital commerce framework, remains incomplete.[63]

POLICY RECOMMENDATIONS

Reform is necessary, and the shape of reform is reasonably clear. The following recommendations are grounded in the analysis in this paper and informed by comparative experience. They aim to strengthen consumer protection and platform accountability without unnecessarily burdening smaller sellers or impeding digital innovation.[64]

1. Define Social Commerce in Law

The most fundamental step is to define social commerce as a distinct legal category. A clear statutory definition covering transactions conducted through social media platforms, messaging applications, influencer promotion, and live-streaming would establish the regulatory perimeter and remove the definitional ambiguity that currently allows multiple actors to argue they fall outside the relevant obligations.[65]

This definition should identify and differentiate the relevant stakeholders: platform operators, individual sellers, influencers and content creators, and consumers. Each category should have

[62] Online Safety Act 2023 (UK); Singapore, E-Commerce Booster Package (Infocomm Media Development Authority, 2022).
[63] See consolidated comparative analysis in UNCTAD, Digital Economy Report 2021 (United Nations, 2021) ch 6
[64] Indian Law Institute, Legislative Drafting (ILI Press, 2020) 78 (on principles of regulatory design).
[65] Consumer Protection Act 2019, s 2 (on definitional clarity in consumer law).

corresponding rights and duties.

2. Update Intermediary Liability

Section 79 of the IT Act should be amended to introduce a graduated liability model. Platforms that passively host user content should retain broad safe harbor protection. Platforms that actively facilitate, promote, or profit from commercial transactions on their infrastructure should bear proportionate accountability for consumer protection failures that occur within that commercial activity.[66]

A conditional safe harbor analogous to the EU's DSA model would preserve protection for genuinely passive intermediaries while ensuring that platforms profiting from social commerce cannot insulate themselves entirely from its consequences.

3. Mandatory Seller Verification

Every account used for commercial purposes on a social media platform should be subject to a Know Your Seller (KYS) verification requirement. This should include verified identity, contact information, and business registration details where applicable. Platforms facilitating commercial transactions should be required to maintain accessible seller records that can be made available to consumers and regulators in the event of a dispute.[67]

4. Legally Binding Influencer Disclosure Rules

ASCI guidelines on influencer disclosure should be given statutory force. Clear, mandatory labelling requirements for paid promotions should be legally enforceable, with penalties for non-compliance that create a genuine deterrent. A registration or certification system for influencers above defined follower thresholds could be considered, creating a category of accountable commercial actors with specific legal obligations.[68]

5. Implement a Robust Data Protection Framework

The Digital Personal Data Protection Act, 2023 should be brought into full operation without further delay. Secondary rules should specifically address data practices in social commerce,

[66] Digital Services Act (n 54), arts 5–8; see Usha Ramanathan (n 8) 22–25.
[67] Digital Services Act (n 54), art 30 (Know Your Business Customer requirements for online marketplaces).
[68] Federal Trade Commission, Endorsement Guides (n 61); ASCI, Guidelines for Influencer Advertising (n 9).

including algorithmic profiling, targeted advertising, and cross-platform data sharing. Consumers should have meaningful, practically accessible rights over their personal data not merely rights that exist in theory but require legal proceedings to enforce.[69]

6. Strengthen Enforcement Capacity

Better laws without better enforcement will not solve the problem. Investment is needed in AI-assisted monitoring tools capable of operating at digital scale. Regulatory staff need digital literacy training. Formal coordination mechanisms between the Ministry of Consumer Affairs, the CCPA, the CCI, data protection authorities, and cybercrime units would allow agencies to pool intelligence and coordinate action rather than operating in silos.[70]

7. Streamlined Complaint Redressal for Social Commerce

Consumer courts and grievance mechanisms need to be adapted for disputes that arise from informal, undocumented social commerce transactions. Simplified evidentiary standards recognizing screenshots, chat logs, and payment records as adequate documentation would make formal dispute resolution accessible to consumers who currently have no practical path to a remedy.[71]

8. Support Formalization of Informal Sellers

Rather than simply imposing legal obligations on unregistered sellers and waiting for non-compliance, a more effective strategy would combine regulatory requirements with practical support for formalization. Simplified registration processes, awareness programmes explaining the legal consequences of informal operation, and digital literacy initiatives for micro-entrepreneurs would bring a larger segment of the social commerce ecosystem within the regulatory framework over time.[72]

9. Competition Oversight of Algorithmic Practices

The CCI should develop clear guidelines on algorithmic self-preferencing, data advantages,

[69] Digital Personal Data Protection Act 2023 (n 25).
[70] Competition Commission of India, Annual Report 2022–23 (CCI, 2023) 45
[71] Consumer Protection Act 2019, s 36 (complaint process); cf Online Dispute Resolution Policy, Ministry of Consumer Affairs (2023).
[72] Meesho, Social Commerce Impact Report (2022) (data on micro-entrepreneurship through social commerce platforms).

and market foreclosure in social commerce contexts. As platforms integrate more commercial functionality, competition concerns particularly around how algorithms affect product visibility and consumer choice will intensify. Proactive regulatory guidance is preferable to retrospective enforcement after harm is entrenched.[73]

10. Engage International Regulatory Forums

Digital commerce is inherently cross-border. India should actively engage with international regulatory bodies and bilateral partnerships to develop common standards on seller verification, influencer disclosure, and data portability. Cross-border enforcement agreements would strengthen India's ability to act against platforms and sellers operating from foreign jurisdictions.[74]

CONCLUSION

Social commerce in India is not a niche phenomenon. It is already a substantial part of how millions of people buy and sell goods, and it is growing rapidly. The informality, reach, and speed that make it attractive are also what make it difficult to regulate and what make the consequences of inadequate regulation so serious for consumers.[75]

This paper has argued that India's existing legal framework the Consumer Protection Act, 2019, the E-commerce Rules, 2020, the IT Act, 2000, and the Companies Act, 2013 provides a partial response at best. Each statute has genuine relevance to some aspects of social commerce. But none was designed with social commerce in mind, and together they leave significant gaps: no clear definition, no systematic seller verification, limited platform accountability, inadequate influencer oversight, incomplete data protection, and enforcement mechanisms that are not equipped for the scale of the problem.[76]

The international evidence suggests what a better framework looks like. The EU's risk-proportionate, rights-based model; China's sector-specific regulation with explicit liability allocation; the US's enforcement-driven approach to advertising accountability each offers elements that India can adapt. The common thread is clarity: clear definitions, clear

[73] Competition Act 2002, s 4; CCI, Market Study on E-Commerce (n 6) 62–65
[74] UNCTAD, International Consumer Protection Enforcement Network: Annual Report (2023).
[75] RedSeer Strategy Consultants (n 4).
[76] See consolidated analysis in ss V–VI above

responsibilities, and clear consequences for non-compliance.[77]

Reform does not require starting from scratch. India already has the institutional architecture consumer courts, the CCPA, the CCI, cybercrime units, and ASCI needed to regulate social commerce. What is required is updating the legal framework to reflect the reality of social commerce, giving these institutions the resources and coordination mechanisms to enforce it effectively, and ensuring that the framework supports rather than stifles the entrepreneurial energy that social commerce has released.[78]

The goal is not to regulate social commerce out of existence. It is to make it work fairly for sellers, platforms, influencers, and especially for the consumers who are currently bearing the costs of a regulatory gap that the law has not yet closed.

[77] OECD, Consumer Protection Enforcement in a Global Digital Marketplace (n 45).
[78] Indian Law Institute, Regulatory Governance in India (ILI Press, 2021) 55

REFERENCES

Primary Legislation

1. Consumer Protection Act, 2019.
2. Consumer Protection (E-commerce) Rules, 2020.
3. Companies Act, 2013.
4. Information Technology Act, 2000.
5. Competition Act, 2002.
6. Digital Personal Data Protection Act, 2023.

European and Foreign Instruments

7. Digital Services Act (Regulation (EU) 2022/2065).
8. Digital Markets Act (Regulation (EU) 2022/1925).
9. General Data Protection Regulation (EU) 2016/679.
10. Communications Decency Act 1996 (United States), s 230.
11. Measures for the Administration of Live-Streaming Marketing Activities (China, 2021).
12. Online Safety Act 2023 (United Kingdom).

Cases

13. Shreya Singhal v Union of India (2015) 5 SCC 1.
14. In Re: Alleged Anti-Competitive Practices by Amazon Seller Services and Flipkart Internet, Case Nos 40 and 41 of 2019 (Competition Commission of India).
15. In Re: Artificial Hiking of Prices on E-commerce Websites, Case No 99 of 2016 (Competition Commission of India).

Books and Reports

16. Indian Law Institute, Legal Research Methodology (ILI Press, 2019).
17. Indian Law Institute, Regulatory Governance in India (ILI Press, 2021).

18. Nandan Kamath, Law Relating to Computers, Internet and E-Commerce (Universal Law Publishing, 5th edn, 2020).

19. Competition Commission of India, Market Study on E-Commerce in India (2020).

20. OECD, Protecting Consumers in Peer Platform Markets (OECD Digital Economy Papers No 253, 2016).

21. UNCTAD, Digital Economy Report 2021 (United Nations, 2021).

22. RedSeer Strategy Consultants, Social Commerce in India (2022).

Journal Articles

23. Prashant Reddy T, "Consumer Protection in Digital Markets" (2021) 6 Indian Journal of Law and Technology 45.

24. Usha Ramanathan, "Platforms and Liability in India" (2021) 33 National Law School of India Review 12.

25. Apar Gupta, "E-Commerce Regulation and the Information Technology Act" (2020) 55 Economic and Political Weekly 34.

26. Priyanka Srinivasan, "Influencer Marketing and Consumer Deception" (2021) 12 Indian Journal of Comparative Law 110.

27. Pavan Duggal, "Social Commerce and the Regulatory Vacuum in India" (2022) 14 Journal of Cyberlaw 1.

Online Sources

28. Advertising Standards Council of India: www.ascionline.in

29. Competition Commission of India: www.cci.gov.in

30. National Consumer Helpline: www.consumerhelpline.gov.in

31. Internet Freedom Foundation: www.internetfreedom