

Media Law in the Digital Era: Regulatory Transformations, Judicial Safeguards, and Democratic Concerns in India

Dr. Komal Dahiya

Bennett University

ABSTRACT

Digital technology has changed the way India's media is done. The easy access to information that is provided through the Internet and smartphones has made information accessible to everyone, yet also posed new challenges. It has been answered by a large amount of regulations both in traditional media (such as broadcast/print) and in special digital legislation (such as the Information Technology Act 2000 and its rules) as well as data protection legislation. India's regulatory system is "fragmented" and recently partly "outdated" according to Professor Subhajit Basu, and has been in place for cable TV acts, film certification, IT law, and the newer codes that are being developed for the digital world.

In the following, this article systemically explores the concept of Media Law in the Digital Era in India. It starts by tracing the evolution of Indian media law from colonial Press to the information society and of the Constitutional provisions of Article 19(1)(a) rights and Article 19(2) restrictions. It reviews the pivotal legislations and regulations relating to digital media, such as the IT Act and its sections, including 66A, 69A and 79, the 2021 Intermediary Guidelines and Digital Media Ethics Code Rules, the new Digital Personal Data Protection Act 2023, and the laws relating to broadcasting, elections and telecom.

The study will look at the key decisions (Shreya Singhal, Puttaswamy, Anuradha Bhasin, Faheema Shirin and beyond to 2026), and their rulings and effects on expression. It discusses changes in regulation (such as digital news codes, content codes), enforcement, and platform liability/safe harbor rules. Important topics (content moderation, takedown regimes, grievance redress, misinformation and deepfakes, AI challenges, privacy-surveillance trade-offs, and democratic concerns (press freedom, censorship, political advertising, algorithmic amplification) are explored in detail.

INTRODUCTION

India's media landscape has been transformed by digital technology. Affordable internet and smartphones have democratized information access,

but also introduced new challenges for law and policy. The government has responded with extensive regulation: not only traditional broadcast/print laws but also special digital statutes (e.g. the Information Technology Act 2000 and its rules) and data protection laws. As Professor Subhajit Basu observes, India's regulatory framework is "fragmented" and partly "outdated," spanning cable TV acts, film certification, IT law, and emerging digital codes.

This article systematically examines Media Law in the Digital Era in India. It begins by charting the historical evolution of Indian media law (from colonial presses to the information society) and the constitutional framework (Article 19(1)(a) rights and Article 19(2) restrictions). It then analyzes the key statutes and rules governing digital media: the IT Act and its sections (including 66A, 69A, 79), the 2021 Intermediary Guidelines and Digital Media Ethics Code Rules, the new Digital Personal Data Protection Act 2023, as well as laws on broadcasting, elections, and telecom.

The study reviews landmark court judgments (e.g. Shreya Singhal, Puttaswamy, Anuradha Bhasin, Faheema Shirin, and others up to 2026), analyzing their holdings and impacts on expression. It explores regulatory transformations (e.g. digital news codes, content codes), enforcement mechanisms, and platform liability/safe harbor rules. Key issues – content moderation, takedown regimes, grievance redress, misinformation and deepfakes, AI challenges, privacy-surveillance trade-offs, and democratic concerns (press freedom, censorship, political advertising, algorithmic amplification) – are discussed in depth.

The analysis also offers a comparative perspective: how EU's Digital Services Act (2022), UK's Online Safety Act (2023), and US Section 230 approaches differ, and what lessons they offer for India. Finally, it proposes policy recommendations for reform (such as judicial oversight on takedowns, algorithmic transparency, data protection safeguards, and self-regulatory frameworks) to secure a free yet responsible media environment in India.

Historical Evolution of Indian Media Law:

Press in Colonial and early post-Independence era was regulated by the British laws (Press Acts 1799, 1835 and Vernacular Press Act 1878) which imposed wide censorship including ban on criticism of the British rulers. The sedition clause (IPC §124A, 1870)

outlawed “disaffection” towards the government. Constitution of India 1950 guarantees freedom of speech (Art. 19(1)(a)) after Independence. The earlier laws were the Cinematograph Act 1952 (Central Board of Film Certification), the Press Council of India Act 1978 (a statutory council of norms for the press) and the censorship rules during the Emergency (1975-77) which reiterated the press restrictions. Until the Cable Television Networks (Regulation) Act 1995, the cable television industry was not well regulated. Before the Cable Television Networks (Regulation) Act 1995, subversive/obscene content and registration of cable operators were not controlled.

Telecom and internet era: The Indian Telegraph Act 1885 and the Wireless Telegraphy Act gave the government broad communication powers. In the 1990s–2000s, satellite TV proliferation led to self-regulation initiatives (e.g. Broadcast Content Complaint Council). A pivotal moment was the enactment of the Information Technology Act 2000 (amending the IPC for cyber offenses). The IT Act introduced new cyber crimes (offensive online content, privacy violations) and provided a safe harbor for online intermediaries. Over time, amendments and rules (e.g. Intermediary Guidelines 2011) expanded state control of digital content.

Recent decades: The 2010s saw fast digital growth (Digital India initiative in 2015) and corresponding laws: Aadhaar (2016), mobile internet surge, and new data/privacy debates. Courts began addressing digital free speech (see Section below). In 2021, the government introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, bringing social media, digital news portals, and OTT platforms under a tiered regulation. The Digital Personal Data Protection Act, 2023, was passed to regulate personal data processing. The broadcasting sector is also slated for overhaul via the Draft Broadcasting Services (Regulation) Bill, 2024. The analysis also provides a comparative perspective as to how the EU Digital Services Act (2022), UK Online Safety Act (2023) and US Section 230 are moving forward and what are the lessons for India. Last, it recommends policy measures for reform (e.g., judicial monitoring of takedowns, transparency of algorithms, data protection measures, and self-regulation) to ensure a free and responsible media space in India.

CONSTITUTIONAL FRAMEWORK:

“Freedom of speech and expression” is provided in the Constitution of India in Article 19(1) (a) and is subject to the “reasonable restrictions” enumerated in Article 19(2) of the Constitution of India. The framework upon which the media law will be built. Article 19(2) lists the grounds (sovereignty, security, public order, defamation, etc.) for restriction of speech. The Supreme Court has explained that any restriction has to pass the lawfulness, legitimate aim and proportionality tests. The Speech of Public Officials can be restricted

only on the narrow ground of Article 19(2) and not otherwise, as was held by a five-judge Bench in the case of *Kaushal Kishore v. State of U.P.* (2023).

Interestingly, the Constitution does not explicitly state “freedom of press”, the right is under the umbrella of Article 19(1)(a). The Press Council Act 1978 and other laws provide for balancing freedom of the press and responsibility, but only the Constitution itself is enforceable against the State (e.g. in the case of *Bennett Coleman v. Union of India* [1973] pre-publication censorship was declared unconstitutional).

Puttaswamy (2017) also marked an important constitutional development in that privacy was declared as fundamental right under Article 21 (life and liberty) by a nine-judge bench. Media and digital platforms are now affected by privacy, which regulates the unreasonable surveillance and the collection of data. Informational self-determination has been understood to be a right of privacy. For instance, the Kerala High Court in *Faheema Shirin* ruled that internet access (which forms part of education) would be covered by privacy.

Key Statutes & Regulations:

The Indian digital media is governed by a jigsaw of laws. The basis is the Information Technology Act, 2000 (No. 21 of 2000). It outlines cyber offenses (such as hacking, data theft) and provisions with content (sections 66A (offensive messages) was ruled unconstitutional). Section 69A gives the government the power to block online information for certain purposes (national security, public order etc.). Section 79 offers a safe harbor for intermediaries (ISPs, platforms) that if they comply with the duty of care, they are not liable if they remove illegal content upon receiving a notice.

Under the IT Act, rules can be framed. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (amended 2023) impose due diligence obligations on social media, news publishers, and OTT platforms. They require significant social media intermediaries to appoint grievance officers, trace originators of certain messages, and remove unlawful content within prescribed timelines. Digital news sites must adhere to a three-tier ethics code and set up self-regulatory bodies. Breach of these rules can strip a platform of safe harbor and invite penal action under the IT Act (e.g. jail under Sec. 87). Critics argue these rules undermine encryption and anonymity, though they aim to make platforms accountable.

Personal Data Law: The Digital Personal Data Protection Act, 2023 (No. 22 of 2023) is India’s first data protection statute. It regulates “digital personal data” (data processed by private entities) with rights and obligations, though it exempts government and offline data. Enforcement is by a new Data Protection Board. The Act’s penalty schedule imposes high fines – up to ₹250 crore for serious breaches (e.g. failure to

implement security safeguards) – signaling stringent compliance. This law enhances individuals’ data rights (consent, correction, erasure) but also imposes burdens on media (processing user data) and potential conflicts with surveillance laws.

Other relevant laws include the Cinematograph Act, 1952 (CBFC certification of films), the Cable Television Networks (Regulation) Act, 1995 (cable TV content and operator registration), and sectoral rules (e.g. broadcasting regulations by TRAI/I&B, telegraph and telecom laws). Election laws (RP Act, Section 126 of 1951) strictly limit political advertising and campaigning during the poll period. Criminal law (IPC) still applies for defamation, hate speech, sedition, and obscenity. Altogether, this multi-legislative regime defines what media can circulate in India, shaping the contours of speech.

Courts Decisions:

India’s courts have been pivotal in defining digital media freedoms. *Shreya Singhal v. Union of India* (2015) was landmark: a three-judge SC bench struck down IT Act Sec. 66A as unconstitutional. The Court held section 66A’s terms (“offensive”/“menacing” messages) were vague and violated Article 19(1)(a) without meeting Article 19(2) tests. This ended arbitrary internet arrests and underscored that speech online is as protected as offline. The Court also cautioned against broad takedown powers without judicial oversight. (Impact: removed a chilling law and affirmed robust free speech online.)

Anuradha Bhasin v. Union of India (2020) addressed Internet shutdowns. Following the 2019 Jammu & Kashmir revocation, non-Internet rule 144 orders suspended connectivity indefinitely. The SC (5:4) held that internet access is an integral part of Article 19(1)(a) free speech. The Court derived this from press freedom cases, noting the “fundamental proximity” between press and speech. It struck down indefinite orders lacking reasoned justification, insisting that suspension orders meet necessity and proportionality. (Impact: affirmed a right to Internet, set judicial review standards for shutdowns.)

Justice K.S. Puttaswamy v. Union of India (2017) was not a media case per se, but essential context: a nine-judge bench unanimously recognized privacy as a fundamental right under Article 21. It identified privacy as intrinsic to human dignity and autonomy. This has implications for media: it limits unwarranted state/data intrusions (e.g. government mass surveillance) and informs data protection (leading to the 2023 Act). For example, Puttaswamy’s emphasis on lawful, proportional intrusion lays groundwork for balancing press investigations against privacy. (Impact: enshrined privacy, influencing digital data debates.) *Faheema Shirin R.K. v. State of Kerala* (2019) (Kerala HC) extended privacy and education to internet access. A student challenged a hostel ban on night-time internet use, arguing her rights to education (Art.21) were infringed. The single-judge bench held the ban

unreasonable: quoting the UN Human Rights Council’s view that internet access is a basic human right, the court struck down the rule, ordering unlimited internet access during study hours. The judgment noted mobile/internet are “necessary part of life” and enhance educational opportunities. (Impact: a progressive recognition that internet access is essential for education and privacy.)

Other Supreme/High Court rulings: In *Google LLC v. Union of India* (2023), petitioners challenged the government’s temporary ban on porn websites; the SC upheld interim blocking orders, remarking that the 2023 Pornography Committee report (seeking 6-month ban) was a policy matter. The SC’s approach here was deferential; a challenge to the policy itself is pending. The *MediaOne* (Madhyamam) case (2023) saw a two-judge SC bench quash the I&B Ministry’s 2022 ban on the *MediaOne* TV channel. The government had alleged national security concerns (secrecy by sealed cover), but CJI Chandrachud’s bench found no evidence publicly shown to justify the ban. The Court held the license revocation arbitrary and insisted that secret evidence without showing facts to the affected party violates natural justice. (Impact: reaffirmed procedural fairness; government must substantiate speech restrictions.)

In *SG Vombatkere v. Union of India* (2023), the SC referred the constitutionality of sedition law (IPC §124A) to a Constitution Bench. Though sedition was not a press issue directly asked here, it highlights free speech tensions: the Court noted Article 14/21 evolution since *Kedarnath* (1962) and is considering whether sedition still passes muster.

In *Foundation for Media Professionals v. UOI* (2022–23), the SC is crafting guidelines on electronic search/seizure. The petitioners likened phones to human extension, invoking privacy (Art.21) and journalist-source privilege. In late 2023, a bench ordered the government to draft rules on device searches, signaling greater protection for digital data. (Impact: aims to protect journalistic privacy and prevent fishing expeditions by authorities.)

Other notable cases include *Subramanian Swamy v. CIL* (2016) (holding even legitimate encryption codes on phones must be provided under law, balancing code freedom against evidence needs), and *Struggle Forum* case (2021) where an NGO’s campus arrest by satyagraha-style protest for alleged anti-India social media posts was quashed, reinforcing that curbing speech requires credible evidence.

These decisions collectively show the courts’ efforts to safeguard fundamental speech rights while acknowledging state concerns. Generally, the trend is pro-speech: vague laws are struck down (*Shreya Singhal*), digital expression is protected (*Anuradha Bhasin*, *Faheema Shirin*), and privacy of digital communication is upheld (*Puttaswamy*, *FMP*). At the same time, the Supreme Court has signaled willingness

to review even established restrictions (sedition reference) and insisted on procedural fairness (Media One). The judicial dialogue thus continually refines India's digital media law in a rights-respecting direction.

Regulatory Transformations and Enforcement

Recent years have seen aggressive regulatory changes. The 2021 IT Rules marked a major transformation: for the first time, social media intermediaries and digital news portals are regulated similarly to broadcasters. Under these rules, platforms must comply within fixed timelines (e.g. remove unlawful content in 24–36 hours), appoint grievance officers, and enable users to appeal takedowns. Self-regulatory bodies oversee news publishers (Tier III) and OTT content (Tier II). The Ministry of Electronics & IT (MeitY) oversees social media compliance, while the Ministry of Information & Broadcasting (MIB) co-regulates digital news. Non-compliance can strip safe-harbor immunity and trigger sanctions (like fine or imprisonment) under Sec. 87 of the IT Act. This regime essentially deputizes platforms to police content, reflecting a policy of platform accountability.

Simultaneously, data protection enforcement is evolving. The Digital Personal Data Protection Act (2023) empowers a Data Protection Board to hear complaints and impose penalties (e.g. up to ₹250 crores as per the schedule). While enforcement mechanisms (e.g. appellate tribunals) have been streamlined (the 2023 Act does not have a separate tribunal), the Board can order data deletion or fines for breaches. Additionally, the government has signaled more surveillance powers: e.g. the 2023 Telecommunications Act and amended suspension rules limit how and how long Internet can be shut down.

Other enforcement bodies: The Press Council (autonomous) deals with press misconduct (no punitive power). The Cable Act tasks local authorities to enforce broadcast norms. TRAI oversees broadcast pricing and infrastructure, while the Election Commission tightly regulates political content during elections (poll silence days, bans on gifts/freebies in Trinamool case, etc.). Law enforcement agencies use IPC provisions (defamation, sedition) and telecom laws (IPC §377, Sec. 269–34 IPC) to prosecute online speech, though courts have often read these narrowly.

In practice, enforcement has been heavy-handed: India has been a leading user of internet shutdowns (over 1000 instances since 2012), and the govt frequently issues takedown orders under Sec.69A or sedition charges against online speakers. Courts have begun pushing back by requiring transparency (e.g. SC's 2020 Anuradha Bhasin rules require review committees for shutdowns and public justification). However, the substantive standards for content removal often remain broad.

In sum, India's regulatory apparatus has rapidly expanded to cover digital media. It now blends

executive powers (blocking, prosecution) with new platform regulation (IT Rules, DPDP Act) and established broadcast law. This creates a co-regulatory ecosystem: platforms are enlisted as gatekeepers, but ultimate authority (for takedowns, censorship) still rests with the government and its agencies. How effectively rules are enforced – fairly and in line with rights – remains a subject of legal and public debate.

Platform Liability and Intermediary Safe Harbor:

Under the IT Act, intermediaries (platforms) enjoy limited liability for user-generated content, subject to conditions. Section 79(1) provides a safe harbor: intermediaries “shall not be liable” for third-party content posted by users, provided they do not initiate or modify it. To retain this immunity, platforms must follow due-diligence rules (inform users of policies, expedite removal of illegal content when notified, preserve records for law enforcement). Subsection 79(3) clarifies that immunity fails if the intermediary had “actual knowledge” of illegal content or upon order, and did not act.

This framework balances free speech and accountability. It means platforms need not proactively monitor all content (avoiding prior restraint), encouraging a vibrant internet. However, critics point to the “notice-and-takedown” model's issues: vague government directives can pressure platforms to over-censor to maintain safe harbor, chilling speech. Shreya Singhal hinted at this, observing that takedown power without review creates risk of abuse. Indeed, after the 2021 Rules, some intermediaries have challenged mandates (e.g. on traceability impacting encryption), arguing that onerous duties erode user privacy and free expression.

Courts have respected the statutory immunity. They recognize Section 79(1) as conditional: platforms are shielded unless they flout their duties. For example, in *Bajaj Auto v. TV Today* (2015), the Supreme Court held that cable operators (then intermediaries) had no obligation to screen content beyond compliance with the Cable Act, citing the principle that preserving safe harbor encourages “free flow of information.” Post-Shreya Singhal, the SC noted that requiring judicial orders for takedowns (rather than summary executive deletions) is appropriate to protect intermediaries' immunity.

In 2021, amendments to the Rules added explicit carve-outs: child sexual abuse material must be removed without delay, and anti-law enforcement obstructions (e.g. encryption hindrances) are penalized. These change the safe harbor calculus: platforms now risk liability if they fail to quickly delete such content. There is also proposed legislation (an Online Safety Code under discussion) that may further refine intermediaries' duties.

In practice, major platforms (Facebook, Twitter, YouTube) generally comply by having policies and grievance processes. A key debate is whether Section

79 should be liberalized or tightened. Supporters say strong immunity underpins free speech (as in the US Section 230 tradition). Opponents say it allows spread of disinformation unchecked. India's approach so far retains conditional immunity (unlike absolute US 230) but is moving towards greater oversight and more mandatory content removal.

Overall, India's intermediary regime attempts to protect platforms legally while subjecting them to due diligence. This has ensured platforms largely thrive, but it also makes them frontline regulators of speech – a contentious role in a democracy.

AI and algorithmic content:

There is no transparency requirement for social media algorithms in India in regard to AI and algorithmic content. The recommender systems of platforms can further sensationalize misinformation or polarization. Civil society has demanded regulation – for instance, disclosure of the targeting of political ads on platforms. The EU has introduced the DSA which calls for algorithmic transparency, but India has no such regime. But there has been a level of awareness of the government, which has floated the idea of licensing or regulating social media algorithms.

To conclude, there is a blend of existing tools (defamation, ICT laws, platform policies) and regulatory impulses to combat misinformation and AI-driven disinformation in India. The threats highlight the conflict between harms and free expression, and serve as a reminder of the need for sophisticated legal tools (such as definitions, due process for takedown of inaccuracies) in the future.

Digital media law is a hybrid of speech and privacy/surveillance law. The state uses security and order as an excuse to control internet communications and the Internet; on the other hand, people call for the protection of data and communications.

The Supreme Court in Puttaswamy's verdict (2017) had affirmed the existence of informational privacy in Article 21. This right limits the powers of the government in terms of data collection and surveillance. Yet, Indian law continues to restrict the Indian state with wide surveillance powers. In India, messages can be intercepted for security purposes with a warrant, under the Indian Telegraph Act 1885 and Telegraph Rules, which includes the "third party doctrine". The IT Act §69 gives the government powers to block websites or content based on the criteria of "sovereignty", "security", "public order" or "defamation". Such blocks have been challenged in court on a few occasions (Anuradha Bhasin) but most blocking orders are confidential and may be overly broad.

There are issues around privacy when investigating social media and searching devices. The SC noted that a smartphone has personal "intimacies" in Foundation for Media Professionals and issued directions for

lawful seizures. Likewise, the authorities and their usage of biometric surveillance (Aadhaar), the collection of metadata and facial recognition is facing criticism. The trouble is that the majority of enforcement actions (closing Internet in an area, requiring user information from the companies) occur without clear legal procedures, potentially exposing users to privacy concerns and "chilling effects" on speech.

In the area of data protection, the Indian law of 2023 will be a step forward. DPPDA 2023 gives the individual rights and mandates the proper handling of data by entities. The fines it imposes (such as ₹250 crore for severe violations) indicate a tough attitude. The Act, however, also includes wide exceptions: it excludes government data processing and includes "national security" exceptions. This has led to criticism from privacy advocates that "the President is exercising too much executive power." Further, the law is private and digital based and doesn't cover gaps (such as non-digital and foreign data).

These tensions are on display in practice. For instance, questions have been raised regarding anonymous accounts, both in terms of privacy and accountability. The policy of encryption is debatable: With the IT Rules 2021, there is a conflict between traceability and end-to-end encrypted services, which adds a layer of privacy concerns. All in all, although digital privacy is acknowledged as a right in India, many of the old surveillance powers still exist. There is still a lack of full convergence of government data protection requirements with police needs. Courts and civil society keep calling for privacy invades to adhere to proportionality requirements to not compromise free expression, in line with Puttaswamy's direction.

Democratic Concerns:

Media law and democracy intersect and questions arise. Freedom of speech and censorship is a constant issue. While the Constitution guarantees freedom of speech, governments sometimes use security legislation, defamation laws and sedition laws to suppress dissent. These are the threats that the Supreme Court has pointed to: "Public order or national security" is often a thinly veiled way to stifle criticism, say commentators. For example, journalists who have dissented have been arrested on fabricated charges. Internet shutdowns (more than 100 in recent years) disproportionately affect marginal communities, as well as hamper journalists' ability to provide news during protest events. Collective censorship occurs when such shutdowns "undermine free expression," says the IBA. Shutdowns have been defined by courts as "collective punishment" and have been subject to rigorous judicial review.

The media is not only being censored, it's being censored too. Political influence is a frequent feature of film and news censorship. There is extensive self-censorship, and a number of film and book bans (Lipstick Under My Burkha, Padmaavat originally)

have received criticism. There are concerns about neutrality when targeted takedowns of anti-government information, real or perpetrated as “misinformation”, occur online. The Bombay HC (2024) rules which struck down the Fact Check amendments pointed to concerns about the government creating a propaganda unit that will determine truth.

Political advertising and election regulation are also in focus. The Election Commission's model code restricts political ads and gifts to voters on TV and there is uneven compliance. The Supreme Court in *Trinamool Congress v. West Bengal* (2023) has indeed declared that giving “freebies” (hugs/food) to voters is unconstitutional and the demand for “level playing field”. Unlike several countries, India has no laws in place related to micro-targeting and political ads online. Social media content funded by foreign nationals is subject to regulation by FCRA/IT Rules while political ads remain not clear about anonymous content.

The algorithmic amplification is a new Democratic worry. Extreme ideology or echo chambers can be reinforced by social media algorithms. There is no Indian requirement for algorithmic transparency or for research access (unlike the EU's DSA mandating data access). Civil society has said that opaque recommendation systems are bad for an informed public discourse. The Kerala HC in *Faheema Shirin* gave a nod in the same direction, that access to internet is vital for education and knowledge.

Finally, media pluralism and ownership affect democracy. There are dangers of homogenized views from the large media conglomerates and cross-ownership. There have been recent digital mergers (Zee-Sony) that have been brought under the anti-trust spotlight. Press Council and BBFC have little ability to promote diversity of the media.

Multitude, freedom and responsibility of the media are important preconditions for a democratic health. The laws govern the balance that India wants but it is tilted towards control. When critical speech is “incipient disorder,” debate is replaced by police power, as legal scholar Subhajit Basu cautions. Media regulation must not quash dissent of any kind if democracy is to be sustained. Policy changes (see below) need to ensure transparency, independence of the media and definite boundaries of censorship to safeguard the democratic values of India.

Comparative Perspective:

India has a digital media regime that is sandwiched between multiple models in the world. One comparator is the EU Digital Services Act (2022). The DSA is an EU regulation regarding platform accountability: It keeps the current conditional liability exemption: intermediaries are only liable when notified of illegal content – and new obligations for large platforms: risk management, transparency, independent audits. It requires a complaint system for users and tells them

what they can do if they have a complaint (e.g. appeal moderation decisions). Interestingly, platforms can be fined up to the equivalent of 6% of global turnover for DSA infringements. The EU has also established a regulator to review algorithms, and demanded “notice-and-action” procedures, which are not in India's policy. The DSA's focus on transparency and systemic-risk assessment has lessons: Indian law has a takedown mandate, but not an algorithmic one or a mandate for data sharing for research.

The UK Online Safety Act (2023) has a child safety focus. It puts a “duty of care” responsibility on user-to-user services to address the dissemination of illegal content (CSAM, terrorism, extremist content) and establishes guidelines for harm reduction to minors. It will be enforced by Ofcom. The consequences of failing to comply are high (up to £18 million or 10% of turnover), and executives can face criminal charges for non-compliance. The Act includes the requirements for risk assessment, rule-of-thumb filtering of child content and elimination of illegal content. While there is no similar direct duty of care regime in India (only general duty of care), an express duty of care regime might be considered. But, critics say that UK's method has created privacy issues, such as age-verification for adult content. A balance would have to be carefully struck in any Indian adoption.

In contrast, the Communications Decency Act (CDA) section 230 of the United States provides broad immunity: the platforms are not considered publishers of user-generated content unless they make a specific effort to encourage illegal activity. This has been said to allow for free innovation and for free speech to flourish on the internet, and has been called for to be reformed because of hate speech and misinformation. India's model is different: it offers conditional immunity, and is tilting towards increased platform responsibility. The Indian law did not provide a strong safe harbor (as in the US) was intentionally so to be regulated more. What India learns is that no immunity should fetter accountability, but too much liability can chill online expression – some balance is required.

Other jurisdictions provide more direct parallels: e.g. the Australia's Online Safety Act (2021) and Singapore's POFMA law demonstrate that governments require content takedowns (usually with a short window to comply). India's 2021 Rules are in the same spirit (short takedown deadlines), but less legal. The world is heading in the direction of more regulation rather than less and India should take note of that. Democratic countries struggle to balance protection of speech with limitation of harms. As is the case in Europe, India can implement transparency measures, like platform reporting and appeals while maintaining the essential free-speech protections. For example, India could implement transparency reporting on content removal and appeals (which DSA does) or an external audit on algorithms. India's Supreme court has said that any acts that seek to criminalise speech and/or extend the powers of the

state must be open to judicial review, as some countries have done. It is very important to uphold good constitutional norms (Art.19 proportionality). Last but not least, some experience in a different country indicates that self-regulation by industry combined with independent supervision (as in the UK child-safety codes or EU co-regulatory systems) may be more effective at preserving democracy than onerous censorship.

Policy Recommendations and Future Reforms:

India needs to take a step in that direction by making changes across several fronts to ensure that freedom of expression and responsibility go hand in hand. Clarity and limits: Vague provisions should be made more precise (e.g. “fake news” or “terrorism-related content” should be clearly defined) to avoid abuse.

There should be procedural safeguards to prevent arbitrary censorship of takedown powers (Sec.69A, IT Rules) such as prior notice or post takedown court review. There would be no abuse because of mandatory transparency (public logs of takedowns and shutdowns).

Algorithmic and platform transparency: Mandate transparency reports (on actions taken on content, origin of orders) and disclosure of simple logic of recommendation algorithms, like EU requirements. Increase the powers of an independent regulator/ombud (may be part of TRP Authority or Telecom Regulator) to audit compliance.

Enhance data rights: establish an independent and powerful Data Protection Board; perhaps constitutional right to privacy, in addition to statute. Avoid loopholes for surveillance in the DPDP Act by limiting state exceptions. Acknowledge that there is a certain “right to be forgotten” when using a deepfake or defamatory material.

Promote media pluralism: Apply anti-trust and cross-ownership rules for media. Support independent public television/radio. Enhance Press Council’s powers for digital media ethics.

Emphasize media literacy and hold accountable: invest in information literacy campaigns to enable citizens to recognize misinformation. Support and incentivize facts checking (public-private partnership, not government censorship). In the recently struck down Fact-Check Unit, we have seen that independent checkers are best for the public interest.

Speech restrictions should continue to be subject of close scrutiny by courts (as in Anuradha Bhasin and others). Restrictive laws should be sunset or reviewed from time to time by legislators. Civil society should be vigilant, strategic litigation (as recommended by IBA experts) can establish precedents in the protection of speech.

CONCLUSION

The media law in India today is at a critical juncture in the digital era. It has a broad and robust free speech guarantee underlying the system, but newer technologies have caught up with the legal frameworks which are no longer keeping pace. While courts have gone to great lengths to extend constitutional protections online, legislative and executive measures frequently take it too far in restricting it. The difficulty is to develop a regulatory system that is able to address the actual negative effects (violence, fraud, hate, privacy violation) while allowing debate and dissent. There is a proven track record of international experience in establishing a democratic information ecosystem through transparency, accountability and well-defined roles, not in total censorship. Any future changes to the media law in India should be based on constitutional protection and ensure social media and digital news continues to support India's pluralistic democracy and protects citizens from the threats of the "new age". India can create a free and responsible digital media environment by establishing clear guidelines and ensuring that the courts remain on the watch for innovation, individual rights and social harmony.

REFERENCES

1. Constitution of India. (1950). Article 19(1)(a), (2). Retrieved from <https://legislative.gov.in/constitution-of-india>
2. Cable Television Networks (Regulation) Act, 1995 (India), Act No. 7 of 1995. Retrieved from India Code (<https://www.indiacode.nic.in>).
3. Central Board of Film Certification v. Unit (Cinematograph Act, 1952) (India). Cinematograph Act, 1952 (India).
4. Cinematograph Act, 1952 (India), Act No. 37 of 1952. Retrieved from India Code (<https://www.indiacode.nic.in>).
5. Deepfakes, Misinformation and Role of Technology: Legal Responses and Restrictions (Lawjournals.org, 2026). Retrieved from <https://www.lawjournals.org/assets/archives/2026/vol12issue2/12117.pdf> [65].
6. Digital Personal Data Protection Act 2023, (No. 22 of 2023) (India). Retrieved from Ministry of Electronics & IT (<https://www.meity.gov.in>).
7. “Exemption from liability of intermediary.” Information Technology Act, 2000 § 79(1)–(3) (India).
8. Faheema Shirin R.K. v. State of Kerala, W.P.(C) No. 19716/2019 (Ker. H. C.) (2019). Retrieved from <https://indiankanoon.org/doc/49257562/>.
9. Freedom on the Net 2024: India. (2024). Freedom House. Retrieved from <https://freedomhouse.org>
10. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India). Retrieved from Ministry of Electronics & IT (<https://www.meity.gov.in>).

11. Information Technology Act, 2000 (India), Act No. 21 of 2000. Retrieved from India Code (<https://www.indiacode.nic.in>).
12. Interim Report on Fake News: Committee to Propose Measures for Combatting Fake News (Government of India, 2023). (Proposed. Not adopted.)
13. Kaushal Kishore v. State of Uttar Pradesh, (2023) S.C.C. 1 (India).
14. Kenneth Kenula Saro v. Union of India, AIR 2015 SC 1523 (India). Shreya Singhal v. Union of India.
15. Madhyamam Broadcasting Ltd. v. Union of India (MediaOne case), (2023) 9 SCC 1 (India).
16. Mediya v. Kerala (Faheema Shirin case), W.P.(C) No. 19716/2019 (Kerala High Court, 2019).
17. Nayak, N. (2025, Dec 16). Freedom of expression: removal of online content by Indian authorities raises serious concerns. International Bar Association. Retrieved from <https://www.ibanet.org/Removal-of-online-content-and-internet-shutdowns-threaten-freedom-of-expression-in-India>.
18. Online Safety Act 2023 (United Kingdom). Retrieved from <https://www.gov.uk> (covers UK measures on platform duties).
19. Press Council Act, 1978 (India), Act No. 37 of 1978. Retrieved from Press Council of India (<https://www.presscouncil.nic.in>).
20. Representation of the People Act, 1951 (India), Act No. 43 of 1951. Retrieved from India Code.
21. Regulation (EU) 2022/2065 (Digital Services Act). Official Journal of the European Union L 277 (19 Oct 2022), 1–102.
22. Scott C. Observer. (2024, January 3). Supreme Court Review 2023: Freedom of Speech. Retrieved from <https://www.scobserver.in/journal/supreme-court-review-2023-freedom-of-speech/>.
23. Section 230, Communications Decency Act, 47 U.S.C. § 230 (1996).
24. Singhal v. Union of India, (2015) 5 SCC 1 (India).
25. Subramanian Swamy v. Cellular Operators Assoc., (2016) 4 SCC 385 (India).
26. Technologies (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
27. 'The Digital Services Act explained'. (n.d.). European Commission – Digital Strategy. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>.
28. The Electronic Telegraph Act, 1885 (India). Retrieved from India Code.
29. The Telecommunications Act, 2023 (India), Act No. 44 of 2023. Retrieved from egazette.gov.in.
30. Vishwanath, A. (2020, January 11). Explained: the laws being used to suspend internet, and what the SC laid down. Indian Express. Retrieved from [https://indianexpress.com/article/explained/kashmi-r-supreme-court-interne t-suspension-6368739/](https://indianexpress.com/article/explained/kashmi-r-supreme-court-interne-t-suspension-6368739/).
31. Vijay Productions v. Govt of India (C.B.F.C.), (1975) 2 SCC 212 (India) (film certification).
32. Basu, S. (2024). Regulating broadcasting in the digital age: A critical comparative perspective. NUJS Journal of Regulatory Studies, 3(1), 67–102.
33. Kaushik, M., & Khurana, U. (2025). Digital public policy and the future of Indian newsrooms. International Research Journal of Journalism and Mass Communication, 9(5).
34. Law Journals (2026). Deepfake, misinformation and role of technology: legal responses and restrictions in India. Retrieved from <https://www.lawjournals.org/assets/archives/2026/vol12issue2/12117.pdf>.
35. Lawyered. (2020, April 14). Right to access internet is part of right to privacy & education: Kerala HC. Retrieved from <https://www.lawyered.in/legal-disrupt/articles/right-access-internet-part-right-privacy-right-education-kerala-hc/>.
36. Observer Research Foundation (ORF) – Digital Media Ethics Code (Commentary) (analysis).
37. Press Council of India. (2023). Norms of Journalistic Conduct. Retrieved from <https://www.presscouncil.nic.in>.
38. SCObserver. (2024). Kaushal Kishore v. State of U.P.: No restriction beyond Article 19(2).
39. Telecom Suspension Rules (Public Emergency), 2017 (India). Retrieved from Department of Telecommunications.
40. UN Human Rights Council. (2011). Report on the promotion and protection of the right to freedom of opinion and expression. (Not a law, but context).