The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

WHEN PRIVACY GOES VIRAL: RETHINKING FREEDOM OF SPEECH IN AGE OF YOUTUBE AND INSTAGRAM

~ Gunn Bhardwaj

Abstract:

Social networking sites, such as Facebook, are modern-day agoras, where public debate takes place. Social media freedom of speech has thus become a problem, and calls for better regulation have been made.[1] Public discourse is all about content moderation, as needed to remove harmful content by some, but censorship by others. What we have here is that we argue the modern debate is centrally focused on the speaking aspect of speech but overlooks a powerful way in which platforms have started invading free speech on the side of the audience. Rather than simply speaking to one's network of adherents, speech on social media is now organized by algorithms with the intent of maximizing user engagement and commercial appeal in the interest of targeted advertising. The result is that speech audiences are algorithmically determined, and it is a trend we term 'algorithmic audiencing'.

We introduce algorithmic audiencing as a discovery, a new trend gone unnoticed so far. We show that it impacts free speech in fresh and unforeseen ways not possible in pre-digital times, by amplifying or suppressing speech for profit, thus distorting free and equal exchange of ideas in public discourse. If black-boxed algorithms control who we talk to, the hurt parties, free speech shifts from 'what can be said' to 'what will be heard' and 'by whom'. We must problematize the audience side of speech urgently if we are to fully understand, and master,

[1] Kai Riemer & Sandra Peter, Algorithmic Audiencing: Why We Need to Rethink Free Speech on Social Media, 36 *J. Information Tech.* 3 (2021), https://doi.org/10.1177/02683962211013358.

free speech on social media. In the context of Information Systems research, algorithmic audiencing opens up entirely new research dimensions.

Introduction:

So what exactly is Algorithmic Amplification?

Have you ever thought about the Instagram reels you scroll through or the YouTube shorts, and believe how my feed has such relatable reels. But are you aware of the concepts like consent, privacy, etc that takes a backstage to make these reels more relatable and user friendly. Therefore let us take an example to understand the negligence in putting behind these sensitive areas just to make the reel look more attractive or rather more relatable.

a woman slips and falls on the sidewalk of a busy street. Someone in the crowd captures it on camera. A minute or two later, it's on Instagram. Hours later, it's on YouTube. It's a meme, a reel, a TikTok duet. Millions share, comment, laugh. She is the "face of the week"—without her name, her consent, or her awareness. The crowd has moved on, but her life is forever changed. It is the unseen crisis of our digital age—not trolls, not hackers, but algorithms.

Understanding Algorithmic Amplification :

Platforms like YouTube and Instagram use AI-driven algorithms to decide what shows up on your home feed, in search results, and especially in "For You," "Explore," or "Trending" categories.

Algorithmic amplification is the process by which social media platforms use auto-emphasizing mechanisms to showcase, recommend, and highlight particular content. Unlike a timeline feed, sites use engagement metrics to predict what will continue to be of interest to users. In doing this, sites don't just reflect public opinion; they actively create it through creating viral traction.

Status Quo on Grey Areas of Indian Legal System

There comes the grey area of law in India that technologies like AI tend to ignore, which is nothing but the concept of 'freedom of thought'. Though absolutely central, the freedom of thought ('FoT') coinciding with right to freedom of speech an expression yet is a right

underemphasized in both practice and discussion. Under Article 18 of the International Covenant on Civil and Political Rights ('ICCPR') and Article 9 of the European Convention on Human Rights ('ECHR'), the right is ambiguous and rarely invoked. In practice, FoT tends to be narrowed down to defending only the most provocative or fringe inner experiences, as is done, for instance, in U.S. court cases concerning gruesome but unbbidden thoughts. Indian legal systems, for instance, do not make any explicit mention of it and consider it as impliedly being a part of freedom of speech and expression[2].

A widening interpretation of Article 21 of the Indian Constitution - "No person shall be deprived of his life or personal liberty except according to procedure established by law" - has, in the course of time, comprised a range of implicit fundamental rights. Of them, mental privacy and freedom of thought can most surely be encompassed by way of judicial interpretation. In the landmark case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court affirmatively recognized privacy as a fundamental right under Article 21. The ruling noted that privacy is polyvalent and includes bodily privacy, informational privacy, and mental privacy. It determined that mental privacy is relevant in terms of surveillance, information gathering, behavior profiling, and neuro-technologies.

This leaves room for legal protection against coercive disclosure of beliefs or thoughts, mind control through technology (AI, neuro-imaging, brain-computer interface), and involuntary psychological profiling. Whereas freedom of religion and conscience is guaranteed in Article 25, freedom of thought per se is not mentioned in the Constitution. But freedom of thought is the quintessence of human dignity, and is indirectly guaranteed by Articles 19(1)(a) and 21. The Puttaswamy judgment established the philosophical and legal basis to argue that freedom of thought (cognitive liberty, i.e., freedom to think freely without coercion or monitoring) is intrinsic to privacy and hence enshrined under Article 21.

Not just privacy but the consent which is a major component of privacy lacks in the Indian legal framework especially when private momments are captured in public places (metro stations, roads, open markets, etc) and uploaded without consent, does implied consent apply just because a person was in private space. Does the law differentiate between consent to be seen in person and consent to go virally. The answer is simply no. If a person is singing on the streets or showing their talents to people doesn’t mean that they also give consent to make their

[2] Shruti Goswamy, *In the Age of Algorithm, We Must Revitalise the Conversation on the “Freedom of Thought”*, The Leaflet (June 2021), https://www.theleaflet.in/digital-rights/in-the-age-of-algorithm-we-must-revitalise-the-conversation-on-the-freedom-of-thought.

video and post it on Instagram or YouTube or to use it as a reel or meme. Though The Digital Personal Data Protection Act, 2023, supports the Puttaswamy mandate by imposing particular limitations on data use[3]. The Act, for example, requires that any processing of digital personal data collected in India be lawful and transparent. In essence, it sees data as an extension of mental privacy, which can only be violated with permission or for predefined, specific purposes but again implied consent becomes passive consent.

Section 79 – Intermediary Liability ("Safe Harbour" Provision)[4]
Grants immunity to online platforms (intermediaries) from liability for third-party content, provided they act like neutral hosts.
Section 79(3)(b): Intermediaries lose immunity if they fail to remove illegal content on notice by the government.

Here as we can understand, Section 79 of the IT Act,2000, protects intermediaries from user-generated content but social media apps actively promoting this content behind every user who provides their content is the same as shooting a gun through someone else's shoulder. The Indian Legal System is still silent on the passivity of AI algorithms, which takes a backseat.

International Status Quo:

EU (European Union)

EU General Data Protection Regulation (GDPR), now in place in respect of 25 May 2018[5], requires a mandatory legal basis for processing data - and aside from the general principles of fairness, accountability and transparency, the key principles of purpose, limitation and data minimisation, and these have implications for the creation, use

[3] Shruti Goswamy, *In the Age of Algorithm, We Must Revitalise the Conversation on the "Freedom of Thought"*, The Leaflet (June 2021), https://www.theleaflet.in/digital-rights/in-the-age-of-algorithm-we-must-revitalise-the-conversation-on-the-freedom-of-thought

[4] *Section 79 of the IT Act*, Vajiram & Ravi (2025), https://vajiramandravi.com/current-affairs/section-79-of-it-act/.

[5] Article 19, *Privacy and Freedom of Expression in the Age of Artificial Intelligence* (Apr. 2018), https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf.

and use of AI systems.

The GDPR also prohibits over-reliance on automated decision-making in certain circumstances, and requires individuals to be notified in regard to the fact of automated decision-making, the grounds therefor and the meaning and intended implications of the processing for the individual. The law imposes a blanket ban (subject to limited exceptions) to solely automated decisions where such decisions have legal or other significant effects.

Notably, the GDPR also defines profiling as the processing of data by automatic means in order to analyse or make predictions about personal aspects in relation to a person. The definition here recognizes the fact that personal data can be created by machine learning programs and other forms of profiling.

Finally, the GDPR also offers a range of provisions encouraging less privacy-invasive systems' design, some of which extend to AI more broadly. The obligation to incorporate data protection by design and by default tries to bring concepts of data protection into designing data processing operations.

The US

Malinowski's bill (bill that took away Section 230 immunity with respect to algorithmic recommendation), the Protecting Americans From Dangerous Algorithms Act[6], would take away Section 230 (3) (II) immunity for claims invoking certain civil rights and terrorism-related statutes if a platform "used an algorithm, model, or other computational process to rank, order, promote, recommend, amplify, or similarly alter the delivery or display of information."

[6] H.R. 2154, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/2154/text.

It contains exceptions, however, for algorithms that are "obvious, understandable, and transparent to a reasonable user," and it lists some examples that would fit the bill,[7] including reverse chronological feeds and ranking by popularity or user reviews. It would also seem to say that any website which does not present to all the exact same thing would forfeit Section 230 protections. Even presenting an individual someone else posts of individuals whom they follow arguably relies on data specific to someone.

Looking the way forward:

Based on global best practices, the following policy recommendations can help India resolve the algorithmic amplification–privacy dilemma. They are as follows:

1. Expand the Requirements of Transparency[8]

Algorithmic risk must be monitored appropriately, but this is impeded by a lack of information about algorithm design. Article 24 (advertising) and Article 29 (recommender systems - Working Party being an advisory group consisting of a member from each of the EU Member States' data protection authorities, the European Data Protection Supervisor, and the European Commission) require minimal disclosures from such parties and – in advertising – do only advertisers' targeting attributes, and not the platform's selection. These should be lengthened to cover all the significant facts about the algorithm: the specific goals for which the algorithm is optimized (e.g., Youtube view time), the main parameters on which the system relies, how these influence what content is displayed, and how data on user activity affects recommendations and ad targeting.

2. Enlarge Access to Data to Civil Society and Journalists

Article 31 provides for regulators and properly qualified scholarship researchers' access to information at the level of the sole system so that audit can be performed of algorithmic processes and effects. The same provision needs to be extended to investigative reporters and watch groups, who have already proven invaluable in revealing harmful algorithmic effects and will continue to be vital in tracking the impact of such systems. Data access should be

Gilad Edelman, *Congress Takes Aim at the Algorithms*, Wired (Apr. 21, 2021), https://www.wired.com/story/congress-takes-aim-at-algorithms-section-230-reform/.

[8] Article 19, *EU: Civil Society Urges EU to Fix Algorithms*, Article 19 (Apr. 22, 2021), https://www.article19.org/resources/eu-civil-society-urges-eu-to-fix-algorithms/.

GDPR compliant with controls to minimize any privacy threat and prevent misutilization of data in Indian legal environment.

3. Subject Self-Assessments of Risk to Independent Audits

Under Article 26, the VLOPs should be required to conduct assessments of potential harms against all human rights and the social effects of their platforms. Self-assessments will be worth nothing if not audited by third parties, either public or licensed by the regulator. Supervisory bodies should require advice on the nature that these assessments and audits should take.

4. Protect Users By Default from Excessive Inferences and Dark Patterns

Users have to be safeguarded against coercive language by imposing a new requirement that the default mode of access to platform services should preclude use of personal data for recommendation and for advertising. Additionally, data use consent settings have to be available through an easy-to-use interface independent of the platform. Deceptively visually designed interfaces employed to influence or eliminate user choice, 'dark patterns', should be banned.

5. Enable Users to Make Changes to Recommendation Systems

Article 29 presently requires making provision for an option to choose a recommender system which does not involve profiling. As noted above, this opt-out has to be an opt in by default. Otherwise than that, sites can make available their existing algorithms on an all or nothing basis. But it has to be obligatory, and not optional, to enable user adjustment of the objectives and parameters of the algorithms.

Conclusion

As society establishes the boundary between rightful influence and undue manipulation, it poses a basic question: Should individuals have an absolute right to mental freedom from unwarranted interference? It is a question that becomes more relevant as technology advances to the point where it can subtly influence our minds and behaviors without our explicit

knowledge or consent. Clearly established ethical and legal limits are essential to protect cognitive liberty in the digital age.[9]

Technological design can be used to support mental autonomy. Humane tech initiatives, privacy-respecting search engines, and technologies that segment digital identities can empower users to maintain control of their cognitive space. Legal reforms can enshrine protections of externalised patterns of thought like search histories or personal notes within the definition of mental privacy. Now, in the age of algorithmic virality, when things go viral not by human design but by invisible digital logics, these distinctions between speech, platform, and privacy have crumbled. Platforms like YouTube and Instagram are no longer passive intermediaries, but are themselves actively shaping public discourse and private disclosure through recommendation algorithms that prioritize engagement over ethics.

To realize constitutional balance between Article 19(1)(a) (speech freedom) and Article 21 (right over privacy), India must move beyond traditional legal distinctions and recognize that algorithmic decisions are editorial judgments, and therefore, they need to be held accountable. Stricter data protection laws, disclosure requirements, independent audit processes, and remedies framed around the user are not policy options — they are constitutional necessities. As online spaces become the new public squares, safeguarding human dignity, informational autonomy, and consent must take precedence first over unrestricted virality. The future of Indian digital free speech rests on whether we can build a legal architecture that witnesses both the vigor of speech.

[9] Shruti Goswamy, *In the Age of Algorithm, We Must Revitalise the Conversation on the "Freedom of Thought"*, The Leaflet (June 2021), https://www.theleaflet.in/digital-rights/in-the-age-of-algorithm-we-must-revitalise-the-conversation-on-the-freedom-of-thought