Information Disorders and their Regulation

By Torsha Sarkar, Shruti Trikanad, and Anoushka Soni
Edited and compiled by Vipul Kharbanda
Reviewed by Anubha Sinha
# Table of Contents

1. **Introduction**  
2. **Methodology and Scope**  
3. Conceptualising ‘Information Disorder’  
   3.1 What is an information disorder?  
4. **Tackling Information Disorders**  
   4.1 Information Disorders in the Digital Age  
   4.2 Guidance for Regulatory Responses  
5. The Indian State’s Responses Under General Laws  
   5.1 Notifications, Advisories, and other Communications  
   5.1.1 Notifications under the Epidemic Diseases Act, 1897  
   5.1.2 Advisories  
   5.2 Penal Provisions and Arrests  
   5.3 Judicial Decisions  
   5.3.1 What Is ‘Fake News’?  
   5.3.2 Official Versions of Events  
   5.3.3 Liability of WhatsApp Administrators  
6. State Responses under the Information Technology Act  
   6.1 Mechanism under Section 69A, IT Act  
   6.2 Mechanism under Section 79, IT Act  
   6.2.1 Who is Sending the Takedown Notices?  
   6.3 Common Strands in the Takedown Orders  
7. **Conclusion**
1 Introduction

The Indian media and digital sphere, perhaps a crude reflection of the socio-economic realities of the Indian political landscape, presents a unique and challenging setting for studying information disorders. In the last few years, ‘fake news’ has garnered interest across the political spectrum, as affiliates of both the ruling party and its opposition have seemingly partaken in its proliferation. The COVID-19 pandemic added to this phenomenon, allowing for xenophobic, communal narratives, and false information about health-protective behaviour to flourish, all with potentially deadly effects. This report maps and analyses the government’s regulatory approach to information disorders in India and makes suggestions for how to respond to the issue.

State efforts to address this problem have been imperfect. In 2020, for instance, the governments of Maharashtra and Assam announced measures – with the purported aim of preventing misinformation – which could be (mis)used to clamp down on the flow of information and threaten citizens’ rights to freedom of speech and expression. These attempts have percolated to social media platforms as well. The Ministry of Electronics and Information Technology (MeitY) has repeatedly issued advisories to social media platforms to curb ‘false news/misinformation’ related to the pandemic. This has culminated in the founding of fact-checking units conceptualised by the MeitY, raising concerns about censorship that circumvents established legal principles.

Questions raised in Parliament and their answers offer a glimpse into the fragmented nature of the government’s responses. In answer to repeated questions by members of the Lok Sabha about the regulatory responses adopted by the government to deal with the problem of ‘fake news’, the government has invoked various legislations including the Information Technology Act, the Cable Television Networks Act, and the Press Council Act.


as well as initiatives like the Press Information Bureau (PIB) fact-checking unit and the Information Security Education and Awareness (ISEA) portal.7

In addition to its measures being fractured, the government has not made any cohesive effort to understand what ‘fake news’ or ‘mis/disinformation’ consists of. This has meant that several regulations have come by way of local notifications under the Epidemic Diseases Act, an archaic and flawed legislation that does not clearly envisage the censorship of speech. Efforts have also involved overbroad techno-solutionism: BECIL, a public sector enterprise under the MeitY, floated an ‘expression of interest’ (EOI), inviting “Solution and Services related to fact verification and disinformation detection”.10 The scope of work of this proposal was alarmingly broad, including “geolocation identification and verification of visual content”, “Monitor[ing] the activities of Disinformation Uploaders across multiple Social Media platforms”, and “AI based Data classification and clustering”.

Coupled with this lack of legal clarity have been widespread and arbitrary arrests of citizens on grounds of spreading ‘fake news’.11 These citizens have been booked under the provisions of different legislations, including the Indian Penal Code (IPC) and the Epidemic Diseases Act.13 Arrests made on similar grounds have targeted journalists and dissenting voices.14

The intensity of the information disorder relating to the pandemic – the World Health Organization (WHO) termed it the ‘infodemic’ – created a strong case for analysing and reforming the regulatory measures for such disorders. In the absence of a suitable policy, even seemingly temporary and flawed solutions to stem the unprecedented flow of ‘fake news’, might become a permanent feature of our engagement with the internet.15

12 Dore, “Fake News”, Foreign Policy.
13 Dore, “Fake News”, Foreign Policy.
In this study, we gathered information by scouring general search engines, legal databases, and crime statistics databases to cull out data on a) regulations, notifications, ordinances, judgments, tender documents, and any other legal and quasi-legal materials that have attempted to regulate ‘fake news’ in any format; and b) news reports and accounts of arrests made for allegedly spreading ‘fake news’. Analysing this data allows us to determine the flaws and scope for misuse in the existing system. It also gives us a sense of the challenges associated with regulating this increasingly complicated issue while trying to avoid the pitfalls of the present system.
2 Methodology and Scope

At the outset, we recognise that Studies into ‘information disorders’ are fraught with the questions of definition. While some level of scholarly consensus exists on the definitions of ‘mis/dis/malinformation’, their operationalisation in regulatory responses has remained controversial. More contentious is the term ‘fake news’, which carries its own political charge, and has been used by authoritarian governments to quash critical or dissenting voices.16

To establish a consensus for this study, we conducted a literature review to identify the points of contention in these definitions, and fleshed out a conceptual framework for the terms ‘mis/disinformation’ and ‘information disorder’, used throughout the report.

From here, we moved on to culling out information about the Indian government's approach to ‘regulating’ information disorders. We define regulation as measures, initiatives, awareness programmes, or “binding legal norms created by a state organ that intends to shape the conduct of individuals and firms”.17 Using this definition allowed us to cast a wide net in selecting measures for our study, and to include acts from all three arms of the Indian government: the executive, judiciary, and legislature.

To locate information about these measures, we utilised a triangulation methodology, “using multiple data sources in an investigation to produce understanding”.18 We conducted searches of four databases – Google, Lumen, Indiankanoon, and the National Crime Records Bureau (NCRB) – to compile and gain a robust understanding of the various government measures. There are certain limitations associated with using these databases, particularly Indiankanoon and the NCRB – the available data is not comprehensive. As such, we do not claim that our compilation of the government’s measures is all-encompassing.

The report is divided into four parts. Chapter III uses a theoretical analysis to conceptualise and clarify the nomenclature of ‘information disorder’. Chapter IV discusses broad guidelines for tackling information disorders that have been suggested in academic research. Chapters V and VI look at the various types of government responses in India for dealing with such a complicated issue, and point out their drawbacks.


3 Conceptualising ‘Information Disorder’

Given the novelty and complexity of technology-mediated information disorders, it is important for regulatory solutions proposed to tackle these challenges to be rooted in research. Legislations and policy documents that seek to criminalise, prosecute, or otherwise sanction the production of various forms of harmful information often run the risk of being overbroad and censorious. Thus it is critical that these measures are backed by a conceptual framework and a vision about what comprises an information disorder.

Most scholarly work on the deluge of harmful, misleading, and problematic information seems conflicted about the exact contours of the concepts in question, or the relationships between them (mis/dis/malinformation, fake news, etc.). Some researchers, like Ethan Zuckerman and Danah Boyd, have warned against the use of ‘fake news’, since the term is vague and ambiguous, and encompasses vast amounts of information within its ambit, including information that people simply do not agree with, which may or may not be objectively true. Work by First Draft News has proven that a lot of content tentatively categorised as ‘fake news’ is neither fully fake (occasionally containing elements of weaponised truth) nor always ‘news’ in the traditional sense (sometimes including memes, rumours, and false ads). On the other hand, communication scholar Alice Marwick uses ‘fake news’ as a heuristic for public engagement with the term, while employing ‘problematic information’, devised by media historian Caroline Jack, as a catch-all term for all sorts of false and misleading information available online.

3.1 What is an information disorder?

A review of 34 published articles on the topic of ‘fake news’ by Tandoc et al. finds that the term has been deployed in six settings: satire, parody, fabrication, manipulation, propaganda, and advertising. The study also identifies two domains in which this typology of ‘fake news’ can be mapped – facticity and intention. Facticity refers to the

---


extent to which a piece of information relies on facts, while intention is the degree to which the author of the information intends to mislead their audience.\textsuperscript{25}

The domains of facticity and intention, constituting a continuum,\textsuperscript{26} serve as useful tools for mapping the various types of false, misleading, and harmful content currently available online, including hoaxes, propaganda, and satire.\textsuperscript{27} In the work done by Claire Wardle and Hossein Derakhshan, these domains are operationalised. They identify three types of information disorders: misinformation, disinformation, and malinformation.\textsuperscript{28} Misinformation is information that is false, but not created with the intention to cause harm. Disinformation is information that is false and is created deliberately to harm. Malinformation is information that is based on reality, intended to harm.

The relationship between the work of Tandoc et al. and that of Wardle and Derakhshan is mapped in Table 1.

**Table 1: Mis/Dis/Malinformation and the Domains of Facticity and Intention**

<table>
<thead>
<tr>
<th>Domains</th>
<th>Facticity</th>
<th>Intention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misinformation</td>
<td>Not based on facts</td>
<td>No intention to harm</td>
</tr>
<tr>
<td>Disinformation</td>
<td>Not based on facts</td>
<td>Intention to harm</td>
</tr>
<tr>
<td>Malinformation</td>
<td>Based on facts</td>
<td>Intention to harm</td>
</tr>
</tbody>
</table>

A similar definition is adopted in the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Speech and Expression: “disinformation is understood as false information that is disseminated intentionally to cause serious social harm and misinformation as the dissemination of false information unknowingly”.\textsuperscript{29} The Special Rapporteur also cautions against using these terms interchangeably, since doing so compromises on the clarity and effectiveness of responses.\textsuperscript{30}

For this study, we adopted the conceptual framework for mis/dis/malinformation developed by Wardle and Derakhshan. In our discussion, these terms are not used interchangeably. While analysing the responses of governments and multilateral agencies in the subsequent sections, we replicate the terminologies used by the respective

\textsuperscript{26} Edson et al., “Fake News”, 137–153.
\textsuperscript{27} Jack, “Lexicon of Lies”, Data and Society Research Institute.
agencies to highlight the problem of non-uniform and ambiguous conceptual understandings in combating information disorder.
4 Tackling Information Disorders

Disinformation or fake news is not a new phenomenon – it has been around for a long time. Julius Caesar was involved in a fake news scandal way back in 44 BC, when he appointed himself dictator for life. Nazi propaganda machines used fake news to stoke anti-Semitic fervour in Europe. Similarly, In the 1890s, rival American newspaper publishers Joseph Pulitzer and William Hearst competed over the audience through sensationalism and reporting rumors as though they were facts, a practice that became known at the time as “yellow journalism.” Their incredulous news played a role in leading the US into the Spanish-American War of 1898. These are examples of information disorders that occurred (or began occurring) before the age of social media. Recognising the ubiquity of information disorders, the ancient Indian political text Arthashastra devoted time and space to a discussion of propaganda as a tool of statecraft.

In the absence of specific laws to deal with the issue, authorities have tried to use existing penal provisions to address information disorders: sections 124A, 153A, 153B, 171C, 171G, 269, 270, 499, 504, and 505 of the IPC, 1860; Section 54 of the Disaster Management Act, 2005; etc. Most of these provisions are concerned primarily with the consequences of the information. The limitations of using these provisions to deal with information disorders will become clear in the discussion that follows.

32 https://cits.ucsb.edu/fake-news/brief-history
35 Sedition.
36 Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony.
37 Imputations, assertions prejudicial to national integration.
38 Undue influence at elections.
39 False statement in connection with an election.
40 Negligent act likely to spread infection of disease dangerous to life.
41 Malignant act likely to spread infection of disease dangerous to life.
42 Defamation.
43 Intentional insult with intent to provoke breach of the peace.
44 Statements conducing to public mischief.
45 Punishment for false warning.
4.1 Information Disorders in the Digital Age

Even assuming that the aforementioned laws were sufficient to deal with information disorders in the analogue age, information disorders in the digital age have unique features which make it a different creature altogether. Primary among them are the following:

(i) Producing and spreading mis/dis/malinformation has become much cheaper and easier due to the availability of end-to-end digital infrastructure for information exchange. It has therefore become easy to circulate information to a much larger audience at a fraction of what it would have cost in a non-digital environment.

(ii) In the pre-internet age, only media outlets with sufficient resources could reach large audiences. These organisations had the means to invest in quality checks, which in turn improved their reputation and thus circulation. But due to the low-cost of production and the end-to-end infrastructure provided by the internet, today anyone can be a publisher with a potentially global reach even in the absence of sophisticated quality checking mechanisms. Indeed, since most news circulates free of charge and depends on the user bases of social media networks to do so, it has become uneconomical to invest in quality checks.

(iii) Information disorders are often amplified by algorithms used by social media companies. The algorithms are designed to provide personalised experiences which users are more likely to enjoy, thus reinforcing the worldviews of users within a safe ‘echo chamber’. Since there is nobody to challenge the ideas within these echo chambers, users are receptive to these messages and are likely to share and propagate the information themselves. Research also suggests that people are more likely to trust information they receive from someone they know. This is why mis/dis/malinformation disseminates so quickly – it travels in peer-to-peer networks which tend to have high trust quotients.

(iv) These personalised bubbles, though clearly problematic, are profitable for large tech companies as they enable them to retain users on their platforms for long periods. Tech companies then collect large amounts of information on individuals, allowing them to push targeted advertising to customers. This personalised messaging prompts users to keep returning to the platforms, thereby increasing the profits of the tech companies.

---


(v) Another peculiar feature of information disorders in the digital age is that the link between the content of the news and the means of communication is broken. Internet intermediaries have traditionally been shielded from taking responsibility for acts committed through, or on, their platforms by safe harbour provisions. Therefore, platforms have no real reason to take action against information disorders, which bring the desired traffic and, consequently, (advertising) revenue. Apart from the issues mentioned thus far, other factors contribute to the growth of information disorders. For instance, the struggling legacy media sector, absence of robust public information regimes, low digital and media literacy, social factors such as the frustrations and grievances of a growing number of people due to economic deprivation, market failures, political disenfranchisement, and social inequalities. All these factors make for a receptive audience which is susceptible to manipulation and mis/dis/malinformation.

### 4.2 Guidance for Regulatory Responses

Due to the peculiarities of information disorders in the digital age, states, and multilateral institutions all over the world are grappling with how to respond to this unique problem. The biggest challenge in responding to this phenomenon is to ensure a balance between curbing information disorders and respecting people’s right to free speech and expression. A response that shows too much deference to free speech may not be effective enough to manage information disorders. But, on the other hand, one has to be cautious about opportunistic governments suppressing dissent and criticism in the name of curbing information disorders.

The Broadband Commission for Sustainable Development, a joint initiative by the International Telecommunications Union (ITU) and UNESCO, in a report on countering digital disinformation, also recognises that the fight against disinformation should not lead to suppression of pluralism of information and opinions. To that end, the commission developed a framework with 23 reference points to assess legislative, regulatory, and policy responses to disinformation in accordance with human rights norms. The tool includes issues such as multi-stakeholder engagement, clear identification of the problem, effects on the freedom of speech and expression, a distinction between deliberate and unintentional misinformation, sufficient protection for journalists and civil society actors, oversight mechanisms, technological responses, engagement of civil

---

51 For example. Section 79 of the IT Act, 2000.


---

society actors, encouragement to counter disinformation work, recognition of specially vulnerable groups, and design as short-term or long-term measures. This framework could provide effective guidance for enacting or improving state responses to disinformation.

The United Nations Development Programme (UNDP), in its report on information pollution, suggests various methods to deal with disinformation. These include recommendations such as increasing participation by the non-government sector in the drafting of laws in the fight against disinformation, improving efforts that foster critical thinking, encouraging private institutions to invest in the media sector, and insisting on the corporate responsibility of social media companies. Just like the Broadband Commission’s report, the UNDP emphasises the need to ensure that responses to disinformation are developed using a human rights centric approach, and that freedom of speech and expression is respected.

In 2018, the European Union issued a communication which outlined its four-pronged approach to tackling disinformation: (i) improve transparency regarding the origin of information and the way it is produced, sponsored, disseminated, and targeted; (ii) promote diversity of information through support of high-quality journalism and media literacy; (iii) foster credibility of information by providing an indication of its trustworthiness, notably with the help of trusted flaggers; and (iv) fashion inclusive solutions, such as raising awareness, media literacy, stakeholder involvement, and cooperation of public authorities and online platforms. The communication emphasises that all action towards these objectives should strictly respect freedom of expression and include safeguards that prevent their misuse.

Information correction is perhaps the least intrusive method for dealing with fake news because it does not impinge upon freedom of expression. But it has been suggested that in circumstances where such measures prove ineffective and the stakes are sufficiently high, a more intrusive form of regulation, such as criminal sanction, may be effective due to its deterrent effect. Indeed, criminal sanctions that are customised and precisely implemented could be effective in tackling information disorders.

An overall analysis of the recommendations of various multilateral institutions suggests that most recommended responses to information disorders highlight the necessity to encourage critical thinking, invest in the media, and, most importantly, foster respect for freedom of speech and expression.

56 “Efforts to Counter Information Pollution”, United Nations Development Programme.

57 “Efforts to Counter Information Pollution”, United Nations Development Programme.


5 The Indian State’s Responses Under General Laws

India's responses to information disorders, under legislations other than the IT Act, 2000, have primarily targeted the actors involved in producing and transmitting the information, as well as the environments or media in which the information spreads. In the absence of a dedicated framework for dealing with information disorders, the state's response to this issue has been somewhat disjointed, with different authorities trying to address the issue with the tools available to them. This has led to the dispersal of regulatory responses across various notifications and advisories, and the use of penal provisions, content removal orders, voluntary self-regulation, judicial intervention, and fact-checking units. We now discuss these responses at length.

5.1 Notifications, Advisories, and other Communications

Notifications, advisories, and other communications allow governments to use their executive power to quickly respond to situations that need addressing. This governmental power was used extensively during the COVID-19 pandemic, particularly to curb incorrect medical information that was being circulated. The measures seemed to identify that while mis/dis/malinformation and its consequences were constant and unavoidable, there were some moments that warranted special attention, either because of increased potential for such information to spread (for instance, at a religious event) or awareness of the possible impacts (for instance, on COVID-19 treatments and/or resulting panic). In this section, we examine some of the regulatory measures initiated by the Indian government through notifications and advisories. We also consider the circumstances that led to their issuance, their effectiveness or impact, and potential consequences on free speech.

5.1.1 Notifications under the Epidemic Diseases Act, 1897

The Epidemic Diseases Act, 1897 is an archaic law which was enacted to deal with the spread of dangerous epidemic diseases. Section 2 of the act gives wide-ranging powers to the government to take steps and institute any regulations that it deems necessary for the prevention of an epidemic. During the COVID-19 pandemic, the administration frequently used this legislation to issue various notifications, including those to stop the flow of information. Some of the notifications are discussed as follows:

1. In March 2020, the Health and Welfare Department of Assam passed the Assam COVID-19 Regulations, 202060 under Section 2 of the Epidemic Diseases Act, 1897. Among other goals, it sought to prevent the spread of information on the disease. Regulation 6 stated that “No person/institution/organisation will use print or electronic or social media for dissemination of any information regarding COVID-19 without prior permission from the Health and Family Welfare Department, or the District Magistrate”. The notification primarily targeted healthcare facilities.

---

However, the provisions regarding the spread of information, targeted all persons/institutions and organisations. Specifically, it prevented all persons/institutions/organisations from spreading any information or materials in the management of the disease, or from using any print, electronic, or other media for COVID-19 without prior approval from the Ministry of Health and Family Welfare (MoHFW). The penalty for violating the regulation was provided under Section 188 of the IPC – one to six months of imprisonment. However, notwithstanding the prior restraint on speech that it had introduced, the notification failed to identify a reasonable procedure for seeking approval from the MoHFW. Notably, this provision did not prohibit the spread of false information, but merely of information concerning COVID-19.

2. Almost identically worded were the Delhi Epidemic Diseases (Mucormycosis) Regulations, 2021, which penalised the “spread [of] any information or material for management of Mucormycosis” or the “use [of] print/electronic or any other form of media for Mucormycosis” without prior permission from the Department of Health and Family Welfare, Government of Delhi. Following the notification, a committee was set up, under the chairmanship of the chief district medical officer (CDMO) in each district, with specialists of internal medicine, ophthalmology, ENT, and epidemiologists as members, to review any disobedience, which is also punishable under Section 188, IPC.

3. Similar regulations have been passed by Haryana, Punjab, Ladakh, and Chhattisgarh.

**5.1.2 Advisories**

Advisories, unlike notifications, have no statutory force. They are essentially clarifications which inform the public about various provisions of the law that already exist, in relation to the topic being discussed. Generally speaking, they do not have penal provisions for violations, but rather clarify other statutes, the violation of which might carry penalties:

1. One of the first few advisories concerning COVID-19 information was issued by the MoHFW. It aimed to address the misinformation that was allegedly rampant on social

---

61“Orders by Governor of Assam”, Government of Assam, paragraph 15.


64“Ladakh Epidemic Diseases (Mucormycosis) Regulation, 2021”, The Administration of Union Territory of Ladakh, 27 May 2021, [https://cdnbbsr.s3waas.gov.in/s395192c98732387165bf8e396c0f2dad2/uploads/2021/05/2021052769.pdf](https://cdnbbsr.s3waas.gov.in/s395192c98732387165bf8e396c0f2dad2/uploads/2021/05/2021052769.pdf).

media. Referring to the obligations of social media platforms under the Intermediary Guidelines, intermediaries were urged to do the following:

(i) initiate awareness campaigns on their platforms to discourage users from uploading/circulating false news/misinformation concerning the coronavirus, particularly if it was likely to create panic among public and disturb public order and social tranquillity;

(ii) take immediate action to disable/remove such content from their platforms on a priority basis; and

(iii) promote the dissemination of authentic information related to the coronavirus as far as possible.

A similar advisory was issued once again on 7 May 2021, with the same instructions to intermediaries as in the previous one, but with an additional direction to issue warnings to impostors who misuse the platforms and indulge in such fraudulent activities. These advisories were, however, unclear in their definitions of “false news/misinformation”. However, the reference to concerns about sharing “anonymous data”, and goals of preventing panic and ensuring “public order” have been interpreted by some as a desire to control the narrative of the pandemic and the government’s management of it. This is supported by reports of government requests sent to X (formerly Twitter), Facebook, and Instagram – that supposedly used the same language – to take down content regarding its (mis)handling of the pandemic, especially during the second wave, which hit India in April/May 2021.

2. As a continuation of the last few advisories requiring intermediaries to take action against misinformation on their platforms, the MeitY issued an advisory on 21 May

---


67 Information Technology (Intermediary Guidelines) Rules, 2011, which were in force when the advisory was issued.


69 The term ‘public order’ may have been specifically used to comply with the requirements of Article 19(2), which provides for exceptions wherein the right to freedom of speech and expression may be legitimately curbed.

70 Deep, “‘Fake News’ Advisory”, Medianama.


72 “Notification No. 16(1)/2020-CLES – 3”, Ministry of Electronics and Information Technology, Government of India, 21 May 2021,
2021 with a more specific scope: it asked all social media platforms to immediately “remove all the content that names, refers to, or implies ‘Indian variant’ of coronavirus” from their platforms. This was after a press release by the MoHFW which clarified that the WHO did not associate ‘Indian variant’ with B.1.617 in any of its reports or communications. Therefore, any reports that did so were unfounded and incorrect.73

3. During this period, the police also issued responses. In April 2020, the Maharashtra police, for instance, issued an advisory74 to WhatsApp users and administrators during the COVID-19 pandemic. Similar advisories were issued by the police in Goa,75 Jharkhand,76 Nagaland,77 and Arunachal Pradesh.78 These explained the best practices concerning the transmission of news on WhatsApp groups, and reminded users of the penal provisions that would be used against the speakers and administrators, should misinformation or other such news circulate on their groups. Notably, they seemed to attach criminal liability to “illegal” speech, not only for those who made or transmitted it, but also to the administrators of the groups, who did not take sufficient corrective action.79

4. In April, 2020, the MoHFW issued an advisory to address the social stigma associated with the COVID-19 pandemic, urging people not to label any community or area as associated with the spread of the novel coronavirus.80 This was,


74“Advisory for WhatsApp Users and Admins during the COVID-19 Pandemic”, Office of the Special Inspector General of Police,Maharashtra Cyber, 8 April 2020, https://drive.google.com/file/d/1qQQmBmoDgYyQqJvrM1L7bZiwLDJadPh/view.


79 The legal position relating to the liability of administrators of WhatsApp groups is discussed later in this paper.

presumably, to address the discrimination experienced by the Muslim community after a religious gathering of the Tablighi Jamaat sect was deemed to be a COVID-19 hotspot. What followed was a landslide of misinformation, including fake and engineered videos, and a demonising news cycle.\(^1\) The advisory identified that “certain communities and areas” were being “labelled purely based on false reports” floating around social media and elsewhere. It suggested “an urgent need to counter such prejudices”. Among a set of dos and don’ts, the advisory also urged against labelling any community or area as being responsible for the spread of COVID-19. However, this was easily disregarded as the MoHFW continued to focus on “hotspots” created by the Tablighi Jamaat gatherings, attributing a large percentage of the COVID-19 cases in India to the Tablighis.\(^2\) This triggered another news cycle of stigma, which was in stark contrast to what the MoHFW seemingly intended with its advisory.\(^3\)

From the state responses discussed here, we see two main categories or goals: a) preventing “false” news or making it inaccessible to people, and b) identifying “false” news and providing counter or correct information. A categorical analysis of the policy responses reveals the following broad themes:

1. **No further clarity on the definition of ‘fake news’** – Among the measures that sought to prevent false news, the majority used ‘negative’ measures to protect society and its right of access to information, by constraining the presence of destructive and harmful misinformation, and by functioning as a deterrent to repeat actions. However, what these responses collectively failed to establish was conceptual clarity on ‘fake news’. These notifications/advisories did not attempt to monitor or investigate mis/dis/malinformation campaigns, but simply served as reminders to comply with existing laws/regulations.

2. **Impact on the freedom of expression**– More concerning, however, were those policies that restricted not only ‘false’ news, but speech of any kind on a particular topic. Phrases like “any information or material for management of Mucormycosis”, “dissemination of any information regarding COVID-19”, and “comments...related to breaking of Corona transmission chain in an unrestrained manner” included in government directives were only some examples of the lack of concern about the impact on free speech. While some policy measures outright criminalised such speech, others required prior approval before posting information on certain topics. But there was no mechanism in place to secure such approval. Particularly when India was struggling with the second wave of COVID-19, this overbroad censorship had dire consequences since crucial information regarding the disease,

---


its treatment, and the availability of hospital beds and oxygen was being shared widely by citizens.

3. **Collaborative efforts with other actors** – One of the key goals these policy responses aimed to achieve was to identify fake news, and provide counter or correct information. However, there was an overemphasis on executing this in a top-down manner, with the government providing both services. Even here, the larger objective seemed to be to clarify fake news related to the government measures. While this was certainly an important part of informing the electorate, it addressed only one of many harms caused by mis/dis/malinformation, and was inadequate. Government measures could instead focus on endorsing or encouraging reliable fact-checking units.

4. **Effectiveness** – These policy measures were also lacking in any means to measure or evaluate their own efficacy. There was minimal oversight or accountability, and several of the regulations were poorly publicised, leaving the populace largely unaware of them. Even when questions were raised in Parliament, these measures were reiterated, without any more information on whether they were succeeding or failing.

## 5.2 Penal Provisions and Arrests

The state has sought to address information disorders using various regulatory responses, perhaps the most severe of which have been penal provisions under the IPC and other legislations. The pandemic led to a demonstrably large increase in the number of arrests, including a crackdown on journalists, activists, as well as negative reportage on the government’s handling of the pandemic. In the absence of any provisions to effectively deal with information disorders, the government resorted to a patchwork of legal provisions to carry out these arrests. Discussed next are some of the commonly used penal provisions in response to instances of alleged mis/dis/malinformation:

1. **Section 153A, IPC** *(Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony)* – This provision, which has often been used to curb information disorders, penalises the promotion of enmity between different groups. For instance, in West Bengal, there was an influx of over 500 fake posts regarding post-poll violence in Bengal, which made references to a “Hindu genocide”. But these posts were created using old videos from Bangladesh, Venezuela, etc. Four people were arrested in connection with these posts, for


sharing fake news that promoted enmity between groups. The Gujarat government has also in the past made use of Section 153A in connection with mob Lynchings and associated fake news on social media or other mediums, with the intention of cracking down on such incidents. Such posts came to the notice of the Supreme Court, which directed the centre and states to take immediate steps to stop the dissemination of such fake news, which whips up mobs into a frenzy.

2. **Section 124A, IPC (Sedition)** – In Chhattisgarh, an individual was taken into custody for posting a video on social media about power cuts, and was booked for sedition under sections 124A and 505 of the IPC (*Statements conducing to public mischief, etc.*), the latter of which deals with intention to cause fear and alarm. In a welcome but rare development, the Chhattisgarh Chief Minister Bhupesh Baghel made a statement to the effect that sedition law must not be invoked for social media posts that are critical of the government, and ordered the person’s release. His statement also cited pre-existing laws that deal with rumours, and urged that the addition of sedition charges was unnecessary. Sedition charges, among various others, were also imposed on a host of eminent personalities, including Congress MP Shashi Tharoor, for sharing news of a protestor who died during the farmers’ tractor parade. An eyewitness allegedly saw a tear gas canister fired by the police hit the individual on the head, causing him to lose control of his vehicle. Related tweets heavily implicated the police in the cause of the man’s death, but subsequent news reports (relying upon CCTV footage) suggested that it was an accident.


3. **Sections 499, 500, and 501, IPC (Defamation)** – Given that Defamation is viewed as a false statement which lowers someone’s reputation,\(^95\) Criminal defamation provisions such as Sections 499, 500, and 501 are, therefore, tools for the regulation of fake news that targets individuals. For instance, advocate Vibhor Anand was arrested for spreading conspiracy theories in the aftermath of the controversy surrounding the death of Sushant Singh Rajput, and was accused of violating the IPC and the IT Act, 2000.\(^96\) In cases where the reputations of individuals, or even companies, are attacked, defamation law has been employed to curb the resulting fake news.\(^97\) However, the trouble with using defamation laws is that they only cover a narrow portion of the regulation of fake news. This means that spreading fake news about a class of people – for instance, Muslims, which is an ongoing problem in countries like the US and India – is not covered under defamation laws because of the absence of reference to a plaintiff\(^98\) (it may, however, get covered under Section 153A of the IPC).

4. **Section 504, IPC (Intentional insult with intent to provoke breach of the peace)** – This provision may not see widespread usage, but it has the potential to be misused. It was used in the arrest of Sunil Brar, a reporter for the Dainik Bhaskar newspaper because he made an error in a report concerning the arrest of a terror suspect. The report supposedly created alarm among the public, since the error related to where the suspect was arrested. Brar was also charged with Section 153, which deals with provocation to cause a riot; Section 177, which deals with furnishing false information; and Section 505, discussed in the next point. However, the court held that nothing had been done which could create enmity between classes, and granted the journalist bail.\(^99\)

5. **Section 505, IPC (Statements conducing to public mischief, etc.)** – This section penalises the publication or circulation of any statement, rumour, or report which is intended or likely to cause fear or alarm among the public, such that any person is induced to commit an offence against the state or against public tranquillity.\(^100\)

---


\(^100\) Offences against the state fall under Chapter VI of the IPC, and include waging war against the state, collecting arms, assaulting the president, sedition, etc. Offences against public tranquillity...
Section 505(2) penalises statements or rumours that create or promote enmity between classes. Notably, an exception to this section clarifies that if the person making the statements has reasonable grounds to believe that the statement, rumour, or report is true, and publishes it in good faith, without any malicious intent, then this person would not be penalised under this section. However, the accepted practice seems to be for the police to impose the section without any regard for the exception. For instance, Pawan Kumar, a journalist who exposed the appalling state of the Uttar Pradesh government’s mid-day meal scheme, was accused, using Section 505, of spreading fake news and rumours to malign the image of the government, create enmity between groups, and incite violence. The misuse of Section 505 in this case does not even consider the misapplication, given that in exposing the scheme of the government, no bad faith on the part of the journalist was proven.

6. Sections 269 and 270, IPC (Negligent act and/or malignant act likely to spread infection of disease dangerous to life) – The COVID-19 pandemic prompted increased usage of disease-related provisions in the IPC to regulate information disorders. For instance, in Delhi, 25 people were arrested for questioning the Indian government’s vaccination policy. They had put up posters with this message: “Modiji humare bachon ka vaccine videsh kyon bhej diya?”. Similarly, the combined effect of sections 269 and 270 was felt by freelance journalist Zubair Ahmed, who was arrested for his tweet questioning why families were being placed in home quarantine after speaking to a COVID-19 patient over the phone. He was accused of spreading panic. However, the Calcutta High Court quashed the first information report (FIR) against him, calling it “absurd” and stating that criminal action against him for this reason would be a “sheer abuse of the process of law.” Section 270 was also invoked to arrest a TV journalist for his report that special trains would restart during the height of the migrant crisis in India during the first lockdown. His report elicited huge gatherings outside railway stations, where COVID-19 could easily spread.

are in Chapter VIII of the IPC and include unlawful assembly, rioting, assaulting a public servant, enmity between classes, etc.


7. **Section 336, IPC (Act endangering life or personal safety of others)** – Section 336 has been used in conjunction with Section 269 against journalists; for instance, in the case of Om Sharma, a Divya Himachal reporter who was accused of spreading of fake news showcasing the plight of migrants.\textsuperscript{106}Sharma was also charged for the publication of a report in Amar Ujala, a daily Hindi newspaper, on Facebook. He allegedly violated the provisions under sections 182, 188, 269, and 336.

8. **Section 144, CrPC (Power to issue order in urgent cases of nuisance or apprehended danger)** – This is one of the primary provisions of the Code of Criminal Procedure (CrPC), 1973 that was brought to the fore during the pandemic, demonstrating its extraordinarily large ambit.\textsuperscript{107} In cities such as Mumbai, which were hit hard by the pandemic, the police issued orders under Section 144, prohibiting individuals from disseminating information that was “incorrect” or factually distorted on social media platforms.\textsuperscript{108} These orders extended to the prohibition of the spread of statements that were inflammatory or discriminatory, as well as information that caused panic or confusion among the public. The order by the Mumbai police commissioner that held WhatsApp group administrators personally liable for the circulation of false or panic-inducing information on groups had the legal backing of Section 144.\textsuperscript{109} Similarly, the Office of the Collector and District Magistrate of Daman and Diu issued an order under Section 144, prohibiting the spread of fake news or rumours about COVID-19.\textsuperscript{110} As both these orders were issued under Section 144, the penal consequences for violation came from Section 188 of the IPC, which deals with disobedience of an order promulgated by a public servant. Given the widespread use of Section 144 during the pandemic, it is unsurprising that as per the latest ‘Crime in India’ report issued by the NCRB (referred to in the next paragraph), the number of cases registered under Section 188 rose exponentially, from 29,469 in 2019 to over 6,00,000 in 2020.\textsuperscript{111} An important aspect of Section 188 is

\textsuperscript{106}Tiwari, “Gagging the Media”, Newslaundry.


\textsuperscript{111}Bharti Jain, “28% Surge in Crimes in 2020, Fuelled by Violation of COVID Norms”, Times of India, 16 September 2021,
that mens rea is not part of the penalised offence; instead, mere contravention of the order with knowledge of it, and such contravention being likely to result or actually resulting in harm, is needed. In April 2021, the District Magistrate of Indore, Madhya Pradesh issued an order under Section 144, threatening criminal prosecution of those persons who made, or forwarded “comments on Social Media platform related to breaking of Corona transmission chain in an unrestrained manner”. It is worth noting that this was immediately contested because, among other things, it contradicted a previous Supreme Court order which observed that clamping down on information during an emergency situation such as COVID-19 was against state interest.

Although the foregoing discussion is illustrated by anecdotal evidence in news reports, it is also backed by the crime statistics in India, released by the NCRB. In the Crime in India report, the following table appeared, depicting a marked rise in fake news cases from 2018 to 2021.

<table>
<thead>
<tr>
<th>Crime Head</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circulate false/fake news/rumours</td>
<td>280</td>
<td>486</td>
<td>1,527</td>
<td>882</td>
</tr>
<tr>
<td>Crime Rate</td>
<td>0</td>
<td>0</td>
<td>0.1</td>
<td>0.1</td>
</tr>
</tbody>
</table>

Table: Crime Statistics

It is clear that since India has no direct provision for penalising fake news, the regulation of fake news often happens through the lens of its actual or perceived impact. For instance, using Section 153A, the impact is the creation of enmity between different


114 The NCRB, however, does not elaborate on what it refers to as ‘fake news’ and how all cases of circulation of fake news come under the ambit of Section 505 of the IPC, which requires specific mens rea or certain consequences, such as the statement inducing other persons to commit offences, to apply. As per the NCRB, to “circulate false/fake news/rumours” is a crime that is penalised by Section 505, read with the IT Act. However, there is no mention of which provisions of the IT Act are being utilised here. Further, Volume II of the report, without any justification or explanation, switches the head of the crime penalised under Section 505 from “circulate false/fake news/rumours” to “fake news on social media”, with no indication of what Section 505 has to do with social media. If Section 505 is interpreted to solely cover people who “circulate false/fake news/rumours”, then “fake news on social media” may be a subset of this category. But the NCRB data suggests that the latter is the only category.
groups. Therefore, while fake news causes the symptom of discord, the backing law does not directly address the core issue. Further, relying on the perception of the impact leads to instances such as the Cyber Police Station in Gurgaon booking a YouTube channel for spreading fake news surrounding the resignation of the Chief Minister of Haryana Manohar Lal Khattar. The channel Nation TV ran a news item titled “Master Stroke by Modi: Khattar Resigns, Anil Vij becomes the CM”. A complaint was filed on account of the “fake news” being shared with the intention to cause a riot and incite people. Hence, the case was filed under sections 153A and 505 of the IPC. Similarly the case of Sunil Brar, the Dainik Bhaskar journalist who was arrested under Section 504, evinces the need for a law that is not premised on the impact of the fake news, which here would be antagonism among classes. It also demonstrates the need for an exception for honest mistakes, especially since Brar issued a correction to the story the next day.

5.3 Judicial Decisions

It is with deep distress that we note that individuals seeking help on such (social media) platforms have been targeted, by alleging that the information posted by them is false and has only been posted in social media to create panic, defame the administration or damage the ‘national image’. – Supreme Court of India

In this section, we look at the judiciary’s involvement in the regulation of information disorders relating to the COVID-19 pandemic. Unlike with executive law-making, which has been adhoc, responses from the courts are expected to be more principled, and to delve into the doctrinal questions behind the principles discussed. However, as we will explore in this section, this has not always been the case.

5.3.1 What Is ‘Fake News’?

The Indian judiciary’s tryst with fake news has had an interesting correlation to the concerns of the citizenry at large. Majority of the notable decisions examined in this paper have resulted from writ petitions (WPs) and public interest litigations (PILs), which asked the court to take cognizance of ongoing issues on the ground. Take, for instance, Teheseen S. Poonawalla v. Union of India for which the Supreme Court considered a batch of WPs that urged the court to intervene on the issue of mob lynching and social media-mediated violence. In these petitions, the court laid down a series of guidelines for both the state and central governments:


a) to “take steps to prohibit instances of dissemination of offensive material through different social media platforms”,

b) to procure “intelligence reports about the people who are likely to commit such crimes or who are involved in spreading hate speeches, provocative statements and fake news”, and

c) for state and central governments to be obligated to “curb and stop dissemination of irresponsible and explosive messages, videos and other material on various social media platforms”.

Unfortunately the decision in *Teheen S. Poonawalla v. Union of India*, did not discuss the issue of what constitutes “fake news”, aside from the term being used in consonance with phrases like “hate speech” and “provocative statements”. In the absence of a clear definition of “fake news”, the discretion for how to interpret it on the ground lies with the executive. As with the examples of content takedown orders, this could allow the police and state officials to censor dissenting, critical, and unpopular voices.

Other petitions, urging the court to establish similar guidelines, have been less successful. For instance, in *Raju Ray v. Union of India*, the Calcutta High Court dismissed a petition for the court to direct the government to “take requisite steps to check broadcast of unwarranted, baseless and false news reports by media houses and to formulate and/or frame a policy or guideline for media house and TV news channels to regulate the content and punitive action for broadcasting fake news.”

A large part of the court’s reason for dismissal was based on the observation that it was not the court’s place to determine whether or not any statement published by the print/audiovisual media was false.

Contrast this with the Supreme Court’s decision in relation to broadcasts on a TV channel. On 28 August 2020, petitioner Firoz Iqbal Khan approached the court, hoping for an urgent intervention with regard to an upcoming programme on Sudarshan News. The petition placed on record a 40-second transcript of the show, stating that it contained statements that would deter the entry of Indian Muslims into the civil services. However, the court refused to issue a pre-broadcast injunction, and referred the case to the competent authorities. On the same day as the Supreme Court’s order, however, a single judge bench in the Delhi High Court stopped the channel from broadcasting the programme, and directed the Ministry of Information and Broadcasting (MIB) to determine whether there had been a violation of the Programme Code under the Cable Television Networks (Regulation) Act, 1995. The union government then sent a communication to the channel on 9 September 2020. Meanwhile, four episodes of the programme were broadcast.

Following this, on 15 September 2020, the Supreme Court was once again called to consider an injunction. The petitioner placed on record a series of clips from the

---

119“Writ Petition (Civil) No. 754”, Supreme Court of India.


121Raju Ray v. Union of India.

122Raju Ray v. Union of India.

broadcast, to argue that alongside the hate speech directed at the Muslim community, the programme also contained statements that were “palpably false”.\(^{124}\) This time around, the court found that *prima facie* the statements made in the case were not only “palpably erroneous but have been made in wanton disregard of the truth”.\(^ {125}\) It therefore issued the injunction originally requested.

Unlike the deference shown in *Tehseen S. Poonawalla v. Union of India*, and the abstention in *Raju Ray v. Union of India*, in this case, the court enter into the debate about whether the statements made in the concerned programme were false. Arguably, this determination was relatively simple, since the programme did contain statements that were factually incorrect.\(^ {126}\)

### 5.3.2 Official Versions of Events

The judiciary’s tendency to intervene saw a substantial uptick during the pandemic, and seemed to be largely in reaction to the government’s policies and regulations. Take, for instance, *Alakh Srivastava v. Union of India* (2020),\(^ {127}\) a PIL filed during the peak of the migrant crisis in March 2020. The government submitted before the Supreme Court that the migrant crisis had been triggered by “fake news”, and prayed that the court direct the media to prevent “fake and inaccurate reporting”, whether intended or not, that would cause “panic in the society”. But the court did not permit such a blanket censorship regime. Having denied the government’s request, the court nevertheless expected the media to maintain “a strong sense of responsibility”, and avoid broadcasting “unverified news capable of causing panic”. The government was obligated to publish a daily bulletin “to clear the doubts of people”, and while the court did not want to interfere in free discussions about the pandemic, it did direct the media to “refer to and publish the official version about the developments”.\(^ {128}\) The court also took note of Section 54 of the Disaster Management Act, 2005, which penalised the spread of false information, and stated that the advisories issued under the provision constituted “orders” under Section 188 of the IPC. Accordingly, faithful compliance to them was expected of state governments, public authorities, and citizens. Ultimately, the decision in *Alakh Srivastava v. Union of India* showed immense deference to the government’s assertion that the migration of labourers was caused by “fake news”.\(^ {129}\) Moreover, the court did not concern itself with assessing either the veracity of the claim or the proportionality of any of the government’s measures. Similar to *Tehseen Poonawalla v. Union of India*, there was no

---

\(^{124}\) *Writ Petition(s) (Civil) No(s). 956*, Supreme Court of India.

\(^{125}\) *Writ Petition(s) (Civil) No(s). 956*, Supreme Court of India.

\(^{126}\) The programme insisted that the upper age limit for entering civil services was different for the different religions, and that more attempts at the civil services exam were available to Indian Muslims. Both of these statements are factually incorrect.


\(^{128}\) *Writ Petition (C) No. 76*, Supreme Court of India.


---
attempt by the court to define “false information” or “fake news”. It must be pointed out, however, that these orders were issued during the height of the pandemic, when the threat of the crisis repeating itself was still very much alive. It is then perhaps understandable that the court placed greater emphasis on instructions for how to avoid a similar situation rather than getting into the jurisprudence of what constituted “fake news”.

In Vinod Dua v. Union of India, the Supreme Court was called upon to quash an FIR for sedition against journalist Vinod Dua, who had criticised the government’s handling of the pandemic. The prosecution relied upon the decision in Alakh Srivastava v. Union of India to argue that it was “the fake and inaccurate reporting [of Vinod Dua] that triggered the migration of workers”. However, in this case, the court turned the argument of the prosecution on its head, holding that the decision in Alakh Srivastava v. Union of India was evidence that a large number of migrant labourers were already travelling towards their homes. Therefore, it could not be said that statements made by Dua were the reason for this movement. The court also found that Dua was within his rights to comment on issues of public import, and his comments could not be construed to create a criminal proceeding against him. On these grounds the court dismissed the FIR against him.

### 5.3.3 Liability of WhatsApp Administrators

The question of whether WhatsApp group administrators can be made liable for content shared on groups has been addressed several times by different courts. In Kishor v. State of Maharashtra an application under Section 482 of the CrPC was filed before the Nagpur Bench of the Bombay High Court, challenging the charge sheet that named the applicant as an accused. The applicant was charged for being the administrator of a WhatsApp group in which a member allegedly made sexually coloured remarks towards another member. The court held, however, that

> A group administrator cannot be held vicariously liable for an act of a member of the group, who posts objectionable content, unless it is shown that there was common intention or pre-arranged plan acting in concert pursuant to such plan by such member of a WhatsApp group and the administrator.

In other words, a WhatsApp administrator does not incur liability solely on the grounds that they hold such a position within the group. Thus, even if the administrator does not remove the member who posted objectionable content on the group, they are still not

---


liable. A similar view has been held by the Madras High Court\textsuperscript{133} and the Delhi High Court in *Ashish Bhalla v. Suresh Chawdhary*,\textsuperscript{134} According to the Delhi High Court:

*When an online platform is created, the creator thereof cannot expect any of the members thereof to indulge in defamation and defamatory statements made by any member of the group cannot make the Administrator liable therefor. It is not as if without the Administrator’s approval of each of the statements, the statements cannot be posted by any of the members of the Group on the said platform.*


\textsuperscript{134}https://www.casemine.com/judgement/in/5a65cbac4a932633207777d4
6 State Responses under the Information Technology Act

The IT Act, 2000 gives the state the power to issue content takedown orders via government requests to social media platforms and other online intermediaries to remove or block speech that violates the laws of the country. In the absence of any clear conceptual definition of what false information needs to be regulated, takedown measures have the potential to become a tool for the government to censor dissenting and unpopular views online.\textsuperscript{135} As we will see, the legal regime making provisions for these measures is inconsistent and largely driven by the executive. With the COVID-19 pandemic, these censoring tendencies have only increased. Although police authorities have occasionally tried to issue content takedown orders under provisions of the CrPC,\textsuperscript{136} the primary legislation dealing with content takedown orders is the IT Act, 2000 and the rules framed under sections 69A and 79 therein.

6.1 Mechanism under Section 69A, IT Act

Section 69A of the IT Act empowers the government to block access to any content or information on the grounds of

\textit{the interest of the sovereignty and integrity of India, defence of India, the security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to the above.}

The government enacted procedural rules to implement this provision in the form of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. These rules specify that a central government officer not below the rank of joint secretary, either on receipt of a court order or a request by nodal officers of designated organisations, may order an intermediary or a government agency to block access to any content. Further, before sending such a request, there must be a hearing before a committee (consisting of the designated officer and officers not below the rank of joint secretary from the Ministry of Law and Justice, Home Ministry, MeitY and the Indian Computer Emergency Response Team [CERT-In]) to determine whether an order may be issued to block the content. There is also an emergency procedure whereby the designated officer may forward the request to the secretary of the Department of Information Technology, who may in turn issue a blocking order as an interim measure, to be followed by the review committee process as a post facto measure. The blocking rules also mandate maintaining “strict confidentiality” around the entire blocking procedure.\textsuperscript{137}


When the Rules of 2009 were challenged as unconstitutional in *Shreya Singhal v. Union of India*, the Supreme Court upheld them on the basis that Section 69A was narrowly drawn and had sufficient procedural safeguards, including the grounds of issuance of a blocking order being specifically drawn (and relatable to Article 19(2), reasons for blocking have to be recorded in writing and can be challenged by a WP under Article 226 of the Constitution.\(^{138}\) The court was also influenced by the fact that the review committee gives an opportunity of hearing to the intermediary and the originator of the information –only after these procedural safeguards are met can a blocking order be passed.\(^{139}\)

### 6.2 Mechanism under Section 79, IT Act

Section 79 of the IT Act, 2000 deals with intermediary liability and creates a safe harbour for intermediaries as long as they exercise due diligence and comply with the guidelines issued by the government in this regard. The earlier guidelines issued by the government in 2011 were superseded by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Rules). Rule 3(1)(b) therein provides that an intermediary shall make independent efforts and inform its users not to host or share any information that “deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature”. Any user may send a request to the grievance officer for content listed in Rule 3(1)(b)\(^{140}\) to be removed; this request has to be resolved within 72 hours. Although this sub-clause appears to be aimed at curbing mis/dis/malinformation, its wording is too wide –it could include within its ambit any untrue information. It also makes no exceptions for satire or social commentary, which often use patently false premises to get a point across. This provision, therefore, appears to err too much on the side of caution. As such, it could very well be used to stifle free speech.

A complaint must be acted upon within 24 hours if it is regarding material which “exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual.”\(^{141}\)

Any person who is not satisfied by the grievance officer’s decision or whose complaint is not resolved within the specified time has the right to approach the Grievance Redressal Committee formed under the Intermediary Rules.\(^{142}\) In January 2023, the central government established three Grievance Appellate Committees consisting of members from the administration and industry. Not a single member with judicial experience was appointed to any of the three committees.\(^{143}\)

---


139 Shreya Singhal v. Union of India.

140 Except those listed in sub-clauses (i), (iv), and (ix).

141 Rule 3(2)(b), Intermediary Rules.

142 Rule 3A, Intermediary Rules.

143 “Three Grievance Appellate Committees (GACs) Notified on the Recently Amended IT Rules 2021”, Ministry of Electronics and Information Technology, Press Information Bureau, 28 January 2023,
Apart from this, the intermediary is also required to remove content within 36 hours from receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the appropriate government or its agency under Clause (b) of Sub-section (3) of Section 79 of the Act.\textsuperscript{144} In keeping with the directions given by the Supreme Court in \textit{Shreya Singhal v. Union of India}, the provision clarifies that such content has to relate to “the interest of the sovereignty and integrity of India; security of the state; friendly relations with foreign states; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force.”

These are constitutionally recognised exceptions to the right to free speech and expression under Indian law.

The Intermediary Rules also envisaged a fact-checking unit; initially the unit was a non-statutory body whose role was to watch for themes or stories promoting false and misleading information, especially related to the government. Besides reviewing content and raising alarms about false news or misinformation, the unit was supposed to publish appropriate content to counter the narratives in question, the report said. In April 2023, the government amended the Intermediary Rules, giving statutory recognition to the fact-checking unit and increasing the scope of information prohibited under Rule 3(1)(b) to include information “in respect of any business of the Central Government, is identified as fake or false or misleading by such fact check unit of the Central Government”.\textsuperscript{145}

The Intermediary Rules thus established a primarily user-generated content takedown mechanism, where the state specified the type of content that was prohibited – Rule 3(1)(b) –and allowed users to register complaints with intermediaries about such information. The rules also allow intermediaries to develop appropriate safeguards to prevent users from misusing this provision.

\textbf{6.2.1 Who is Sending the Takedown Notices?}

The Lumen database, maintained by the Berkman Klein Center for Internet and Society, keeps a repository of takedown notices that are received by social media intermediaries across the world. These notices are voluntarily submitted to the database by the intermediaries themselves, provided that disclosure is not forbidden by law. The Lumen database holds evidence of various governmental authorities sending takedown notices to X (formerly Twitter) and Google between 2017 and 2021, demanding that specific accounts be suspended, particular tweets be taken down, or specific searchlinks be delisted. Authorities have deployed diverse legal provisions to demand the removal of content. And, as not all of these provisions are directly relevant to the regulation of information disorders, their usage is a testament to the confusing nature of content takedown laws in India.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{144} Such an order can only be made regarding information which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the state; friendly relations with foreign states; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the aforementioned, or any information which is prohibited under any law for the time being in force.
\item \textsuperscript{145} GSR 275(E), 6 April 2023.
\end{itemize}
\end{footnotesize}
Among the orders extracted from the database, the two authorities that sent the highest number were MeitY and the Election Commission of India (ECI), which issued the orders under the IT Act and IPC, respectively.

1. **Ministry of Electronics and Information Technology** – Very little is known about the orders that were sent under the IT Act, as the Government of India does not make such information publicly available. Aside from generally circumventing public accountability, this also means it is hard to ascertain whether any of the takedown orders sent under the IT Act aimed to remove “false” information. Further, while some of the orders issued under the IT Act quoted Section 69A as the supporting provision, other orders cited the entirety of the legislation. Early in 2021, X (formerly Twitter) took down about 52 tweets that were critical of government handling of the second wave of the pandemic. The tweets taken down included those by an opposition MP, an opposition MLA, and a former journalist and actor. Similar takedowns have also been effected by Facebook and Instagram. Subsequently, the government issued a statement saying that the X (formerly Twitter) takedown request was made because the tweets were spreading “fake news”, and not because they had criticised the government. Interestingly, while denying a right to information (RTI) application seeking access to the X (formerly Twitter) takedown orders, the government confirmed that the takedowns were effected under Section 69A.

Of course, this one instance does not tell us the exact number of orders that have been issued for removing information that the government has considered “fake news”. Indeed, the government has previously used takedown orders to censor legitimate content, including a satirical website critiquing the social custom of

---


dowry and an environmental activism website.\textsuperscript{152} Given these examples, therefore, one may wonder how many takedown orders have been issued to censor “fake news”, simply comprising views, opinions, and facts that the government does not agree with. Take, for instance, popular cartoonist Manjul, who was informed by X (formerly Twitter) that the government had requested that action be taken against his account since it “violates the laws of India”. Manjul had tweeted cartoons criticising the government’s handling of the pandemic.\textsuperscript{153} Similarly vague government notices have also been served to Alt News co-founder Mohammad Zubair.\textsuperscript{154}

Did these instances of action occur under the guise of “regulating fake news”? What about the information shared/created by these users did the government find to be “false”? Were the takedown orders sent to X (formerly Twitter) under Section 69A? There is no way of ascertaining this, beyond making educated guesses based on the little publicly available information.

Problems also become clear when we consider the legal procedures surrounding the process of content removal, which is executive driven\textsuperscript{155} and involves little judicial intervention. Affording such unfettered discretion to the executive ensures that the government’s judgment about what constitutes fake news continues to be effectively beyond reproach.

2. Election Commission of India – In March 2019, a month before India’s Parliamentary Elections, a group of social media platforms and the industry body Internet and Mobile Association of India (IAMAI) presented a Voluntary Code of Ethics, which was to govern information flow during the election period. Among the obligations undertaken by these social media platforms, a channel of communication was to be established with the ECI. Through this channel, the ECI would have the power to send notifications to the platforms, informing them about potential violations of provisions of the Representation of the People Act (ROPA), 1950, as well as “other applicable electoral laws”.\textsuperscript{156} All notifications were to be acted upon within three hours. This channel, while voluntary for platforms, ultimately created another pathway for government authorities to route takedown orders, including instances


of mis/dis/malinformation. This alternate system was also purely executive driven, with no judicial oversight.

In July 2019, in response to a parliamentary question, the minister of law and justice stated that a total of 154 cases in which the ECI had directed social media platforms to remove “fake/false news/misinformation” had been observed.157 News reports claimed that all of these reported (and removed) pieces of “fake news” were about the ECI, concerning the ostensible manipulation of electronic voting machines (EVMs) over the course of the election.158 Separate fact-checking efforts undertaken in the run-up to the General Elections of 2019 pointed out a host of “misinformation” efforts,159 which were nebulously disruptive and included communal, extremist, and politically sensitive narratives.160

In the absence of any clear reasoning about why a certain piece of news is tagged as “misinformation”, or “fake”, the ECI system for content takedown runs into similar problems as the Section 69A procedure – absolute discretion with no in-built accountability mechanisms. While the importance of maintaining a healthy information ecosystem during elections cannot be overstated, the legal mechanism set up to achieve this end has, ultimately, been flawed.

3. Police Departments – Beyond arresting people on the charge of spreading “fake news”, various police departments have written to social media platforms to request the removal of content that was “highly misleading, baseless and had potential to trigger panic among people”.161 Early in the pandemic, the Mumbai police, for instance, reportedly deployed a team of officials to constantly monitor content on social media platforms. Once any “problematic” content was detected, the police then wrote to the concerned service providers to have it removed.162 These requests were not made under the IT Act and rules thereunder, but under Section 91, CrPC.163 It must be pointed out here that Section 91 of the CrPC empowers law enforcement agencies to issue a written order/summons to produce a document or other thing which is necessary for the purpose of investigation, inquiry, trial, or other proceeding. It has been used in the past for

---


162 Yadav, ”Misleading Social Media Posts”, Hindustan Times.

163 Yadav, ”Misleading Social Media Posts”, Hindustan Times.
interception,\textsuperscript{164} however, using this provision to issue content takedown orders is a relatively new phenomenon, and is as yet legally untested.

Another news article reported that the Maharashtra police had sent 55 takedown notices to prevent “the spread of hateful messages and rumour-mongering on social media vis-a-vis the coronavirus situation”. These notices were sent to the social media platforms themselves, under Section 149 of the CrPC, which empowers the police to prevent a cognizable offence.\textsuperscript{165} However, there is ambiguity about who the intended recipients of these notices were. Indeed, a separate news report about the Maharashtra police mentioned that the Section 149 notices were sent to the users who had created/posted the content in the first place.\textsuperscript{166} The same report also mentions that the police had gotten in touch with social media platforms, requesting them to remove 138 posts that related to “fake news on COVID-19”.\textsuperscript{167}

The Calcutta police and Bengal Criminal Investigation Department (CID) also reportedly contacted prominent social media platforms to remove over 500 posts and user accounts that were supposedly spreading fake content about the political unrest following the 2021 West Bengal Elections.\textsuperscript{168} The news report, however, did not mention the legal provisions used to request this takedown.

6.3 Common Strands in the Takedown Orders

One characteristic that immediately stands out in all the cases mentioned is the ad-hoc nature of the regulatory process. Among the three governmental authorities studied, three legislations and five separate legal provisions were invoked to tackle online information disorders. In the news reports and the original documentation for these takedowns, the authorities provided nearly no reasoning for why any of the content removed was designated as “fake news”. Ground realities suggest that content being taken down using Section 69A is not as limited as the law envisages. Conversations with one popular intermediary revealed that the government prefers to use its powers under Section 69A, possibly because of the opaque nature of the procedure.\textsuperscript{169}


\textsuperscript{169}Sarkar and Grover, “Content Takedown and Users’ Rights”, Centre for Internet and Society.
The inconsistent way in which legal provisions are invoked also begs the following questions: to what extent are any of these laws equipped to effectively deal with the problem of false information? Are these laws being applied to target information that goes beyond the original ambit of the laws? Table 1 provides a comparison between the text of the laws and the contexts of their applications.

### Table: Legal Provisions and their Scopes

<table>
<thead>
<tr>
<th>Legal Provision</th>
<th>Original Ambit</th>
<th>Context in which it is being used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 69A, IT Act</td>
<td>“In the interest of sovereignty and integrity of India, defence of India,</td>
<td>The content being removed under this provision does not always conform to the strict grounds</td>
</tr>
<tr>
<td></td>
<td>security of the State, friendly relations with foreign States or public order</td>
<td>mentioned in the provision.</td>
</tr>
<tr>
<td></td>
<td>or for preventing incitement to the commission of any cognizable offence</td>
<td></td>
</tr>
<tr>
<td></td>
<td>relating to above.”</td>
<td></td>
</tr>
<tr>
<td>Section 79, IT Act, read with</td>
<td>An intermediary shall not host information that “deceives or misleads the</td>
<td>The provision is widely drafted and does not contain any exceptions for bona fide content which</td>
</tr>
<tr>
<td>the Intermediary Guidelines, 2011</td>
<td>addressee about the origin of the message or knowingly and intentionally</td>
<td>may not be untrue, such as satire.</td>
</tr>
<tr>
<td></td>
<td>communicates any misinformation or information which is patently false and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>misleading in nature”.</td>
<td></td>
</tr>
<tr>
<td>Section 91, Cr.P.C.</td>
<td>Summons to produce documents.</td>
<td>This section is used to removed content that is “highly misleading”. It is not immediately</td>
</tr>
<tr>
<td></td>
<td></td>
<td>clear how content takedown orders are amassed within the ambit of Section 91, Cr.P.C. since this</td>
</tr>
<tr>
<td></td>
<td></td>
<td>section only talks about the production of a document or thing before the police, rather than</td>
</tr>
<tr>
<td></td>
<td></td>
<td>removal of such an item.</td>
</tr>
<tr>
<td>Section 149, Cr.P.C.</td>
<td>The prevention of any cognizable offences.</td>
<td>This section is invoked to censor “rumour-mongering” and “fake news” related to the pandemic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Compared to the IPC provisions, Section 149 of the Cr.P.C. casts a</td>
</tr>
</tbody>
</table>
wider ambit, empowering the police to perform a variety of actions. An essential aspect of this provision is that action should aim to prevent cognizable offences, which are defined in the First Schedule of the Cr.P.C., and are separate from offences defined under the IPC and under other laws. From the news reports gathered, however, it is not clear which legal provisions had been violated by the spread of the impugned information.
7 Conclusion

To prevent regulatory measures dealing with information disorders from being overbroad and censorious, it is imperative that these measures are backed by a conceptual framework and a vision of what comprises an information disorder. This is especially important for information disorders in the digital age, due to the unique challenges they present, including the ease of circulation, lack of editorial oversight, algorithmic amplification, and creation of personalised bubbles.

These features necessitate regulatory responses that are specific and calibrated. The Indian state’s responses so far can be categorised thus: (i) pre-emptive notifications prohibiting citizens from circulating information of a certain type (primarily during the COVID-19 outbreak), including advisories which reinforce obligations under other statutes; (ii) action under various penal statutes; and (iii) content takedown orders under the IT Act. In all three categories, the responses of the state seem to have been too heavy-handed. For example, notifications issued during the COVID-19 pandemic prohibited people from sharing any information regarding the pandemic, rather than only false information. Similarly, law enforcement authorities have been criticised for enforcing penal statutes to suppress negative publicity or news which may be critical of the administration, while claiming to tackle misinformation.

The response of the judiciary has been, perhaps understandably, restrained, as far as laying out a comprehensive framework to deal with information disorders is concerned. This is because in our three-tiered government system the primary role of the judiciary is to interpret and implement laws, not to promulgate and enact them. Therefore, although courts may have stepped in and interfered in certain circumstances (such as the Sudarshan TV case and the Vinod Dua case), any expectation of the judiciary to deal with a complex issue such as information disorders would be misplaced.

The government’s preferred method for takedowns in India is the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 because of the confidentiality clause which allows authorities to ensure very little or no transparency regarding the orders. The alternative takedown mechanism – the Intermediary Rules, 2021 – which is supposed to be primarily user driven, has wide provisions for dealing with misinformation. Therefore, the Intermediary Rules could accommodate satire and legitimate social and/or political commentary.

The inadequacy of the responses thus far is only to be expected, as the state is using legislations that were not enacted to deal with the complicated phenomenon of information disorders in the digital age. Although the Intermediary Rules, 2021 mention “misinformation or information which is patently false and untrue or misleading”, there is no nuance in how they deal with the issue. Regulatory responses to information disorders in the digital age have to be carefully crafted to ensure a delicate balance between stopping mis/dis/malinformation and related harms and ensuring freedom of speech and expression. Any regulatory response, therefore, cannot be too liberal (favouring freedom of speech and expression too much) so as to become ineffective. At the same time, it should not be so conservative as to become a means of suppressing free speech and critical opinions.

A recent trend in regulatory responses towards misinformation has been to place greater obligation on intermediaries to take steps to mitigate misinformation; this is reflected in
the Intermediary Guidelines, 2021. While reports available from various multilateral agencies and in the academic literature may give recommendations for the regulation of misinformation— including multi-stakeholder engagement, oversight mechanisms, and technological solutions—determining the exact contours of such regulation would require a much deeper discussion. This would necessitate identifying the different actors within the misinformation cycle and their motivations. Any such discussion would also have to be contextualised within the broader jurisprudence regarding freedom of speech, a fundamental right in India. Any regulation that deals with misinformation would also need to satisfy the requirements of Article 19(2)\textsuperscript{171} of the Constitution of India, which contains the recognised exceptions to freedom of speech.

\textsuperscript{170} Rule 4(4) and 3(2)(b) of the Intermediary Guidelines, 2021.

\textsuperscript{171} Article 19(2) reads as follows:

(2) Nothing in Sub-clause (a) of Clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.