# INTRODUCTION

## Data Without Content, or the Medium With no Message

In February 2015, India’s Supreme Court delivered a landmark judgment on the right to speech.[[1]](#footnote-1) The issue was itself, certainly by today’s standards, relatively insignificant – a Facebook post by a young woman in the small town of Palghar, in Maharashtra, that another young woman had ‘liked’ – that blew up when police arrested the two women under something named Section 66A of India’s Information Technology Act, 2000, which redefined India’s hallowed right to free speech into the digital era.[[2]](#footnote-2)

The Court easily agreed with the primary argument of the petitioners on the specific question of free speech. This was the easier part, for, as legal scholar Pranesh Prakash wrote, it would have taken ‘a highly clever lawyer and a highly credulous judge to make ‘liking’ of a Facebook status update an act capable of being charged with electronically “sending … any information that is grossly offensive or has menacing character”’.[[3]](#footnote-3) Most lawyers also were agreed that, as Prakash elsewhere unambiguously asserted, ‘‘liking’ is protected speech under Article 19(1)(a)’.[[4]](#footnote-4)

Justice Rohinton Nariman, who wrote the judgment, however went further. He took the debate beyond the relatively settled domain of the content of protected free speech and into a far more ambiguous and contested space, namely the legal nature and the properties of data itself. In seeking to regulate speech, the specific amendment to the Information Technology Act that was now being challenged had sought to define speech as *all* forms of digital storage and movement. ‘Section 66A’, Nariman said, ‘casts the net very wide’, for it effectively seeks to control ‘all information that is disseminated over the internet’. Its diktat was being sought to be extended, he pointed out, over any ‘computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record’.[[5]](#footnote-5)

Could all of this data be even understood as speech? Speech in India has a specific legal history. The right to speech is a key right, defined by the Constitution of India as one of the cornerstones of the freedom that India’s citizens had been promised with Independence. Such speech has had particular meaning. It has defined speakers as conscious subjects who know what they are saying, what meaning their speech can have, who take responsibility for what they are saying. If what they are saying is seen as dangerous, such danger ‘should not be remote, conjectural or far-fetched’ but should have ‘proximate and direct nexus’ with what is said.[[6]](#footnote-6) Did all data disseminated over the internet produce such a speaker? If not, how was it speech?

But even that wasn’t the real problem. The real problem was that, in defining objectionable speech, the Act ‘refers only to the medium through which such information is disseminated’. It was, reversing the famous McLuhan dictum, as though the *message was now the medium*. ‘Information of all kinds is roped in’, Nariman went on. ‘Such information may have scientific, literary or artistic value, it may refer to current events, it may be obscene or seditious’, none of this apparently made any difference to the regulator. As a result, ‘no distinction is made between mere discussion or advocacy of a particular point of view which may be annoying or inconvenient or grossly offensive to some’ and the far more inflammatory ‘incitement by which such words lead to an imminent causal connection with public disorder, security of State etc’.[[7]](#footnote-7)

\*\*\*

It may well be possible to read into Nariman’s view of data’s content neutrality, and the potentially inflammatory nature of *all* data in the paranoid view of the state censor, an inevitable if unintended afterlife to Tim Berners-Lee’s original famous May 1990 conception of the ubiquity of information on the internet – when a ‘web’ of ‘hypertext documents’ would become intelligible across browsers everywhere. Now it was precisely the *illusion of its intelligibility* – the capacity of the digital delivery mechanisms to simulate speech in the way they assumed that universal accessibility automatically equated with damage – that allowed police and judicial authorities to read whatever they chose into it. It also made the sheer possession of any device traceable however remotely to seemingly suspect data into a non-bailable criminal act.

A scant three years later, in another Supreme Court case in 2018, Justice Nariman’s premonition was graphically on view when the eminent historian Romila Thapar led a small group of senior academics to challenge the legality of the arrest of five human rights activists and lawyers.[[8]](#footnote-8) In their rejoinder, the police made a series of fantastical, ever-expanding claims of a nationwide conspiracy on the part of the accused to overthrow the Indian state. They based this entirely on ‘material retrieved from the computers, laptops, pen drives and memory cards of […] accused persons’. Such material, they asserted, revealed the arrested ‘as active members of the Communist Party of India (Maoist), a banned organisation, and reflected a design of being involved in the commission of offences having the potential to destabilise the country’. They had been, the police added, arrested ‘not because of their political activities’ but for ‘selecting and encouraging cadres in […] banned organizations to go underground […] mobilizing and distributing money, facilitating selection and purchase of arms, deciding the rates of such arms and suggesting the routes and ways of smuggling such arms into India for […] training and laying booby traps and directional mines’.

None of this had been proved in any court. Instead, as Justice Chandrachud pointed out, the police claimed at a press conference to possess ‘more than sufficient evidence against the five individuals’ without indicating what this evidence was. Three days later, the judge continued, ‘letters (many of which should form part of the case diary) were selectively flashed and read out’ and ‘leaked to the media’, even though the concerned officer admitted – once again only on television – that ‘the letters which had been read out by him were still undergoing forensic analysis together with the electronic devices’.[[9]](#footnote-9) Since then, as regards the specific detainees of the Bhima-Koregaon undertrials, a US-based forensics company named Arsenal Consulting has shown, in its own analysis of some of the disks owned by them, that significant malware existed indicating the possibility of ‘planted’ evidence. Although Arsenal’s report has been widely circulated, it too has not appeared in Court evidence since the National Investigative Agency has challenged the *locus standi* of this organization, and so it too hangs – like the data the police claim to have – in a liminal ghostly existence hovering over the actual legal process.

## Possession

This book is centered around a proposition. ‘Somewhere’, says Nishant Shah in his essay, ‘in the last few years, without us even realizing it, and in an almost non-dramatic fashion, we have foundationally changed our idea of who we are as information subjects’. The human being has become ‘rehumanized’, ‘parsed, processed, and presented only through interfaces that render it recognizable’.

The essays in this book address a relatively recent development: the ever-expanding tsunami of data that surrounds, engulfs, and contaminates us all, passes through our devices and implicates us in multiple actions. We look at how the experience of both receiving and producing data has transformed several basic concepts of democratic politics such as citizenship, authorship, the right to life, to livelihood and to speech, and indeed our experience of the public domain itself. Such data defines us as much to the state as to online entities trying to access us, sell us things, troll us, qualify or disqualify us, even as we on our side relentlessly seek to understand and avail of an ever-expanding range of new and often unfamiliar rights, goods, services, and privileges available ‘online’.

This transformation has taken place within a relatively short span of time. Although Nafis Hasan’s essay explores an essential 70s-80s prequel, the book mostly covers a narrower period – between, as Nishant Shah has it, the Information Technology Act of 2000 and Facebook’s Free Basics project of 2016 or, as Ashish Rajadhyaksha suggests, between 2009 (when in a single month India announced its massive biometric Aadhaar project and passed the draconian Section 66A) and 2020, which saw the Supreme Court judgment on the longest and severest internet shutdown the world has yet seen in Kashmir.[[10]](#footnote-10)

In this time, we saw data – together with the manner of its gathering, its location, its securing, and the ability to interpret it – foundationally transform the basic armature of the modern state. In some measure the technological transformation was built, Hasan argues, on the arrival of RDBMS (or Relational Database Management System) to India. Introduced as a corporate technology, and responsible for much of the famous information technology boom of the 90s, it was the mounting of governmental functioning onto RDBMS that reinvented governance itself into something of a corporate-style service provider with the National e-Governance Plan (NeGP) of 2006, and also thereby into what Indian political scientist Partha Chatterjee has described as the ‘tactically extended state’.[[11]](#footnote-11) It transformed the modern state away from what Hasan calls the constraints of ‘an overbearing fidelity to the organizational design of bureaucracy, to its hierarchies and rules, as well as to the computational design of information systems’ and into a new era in which digital governance ‘clogs the information highway, storms into the lanes, cracks, and crevices of daily life’.

A more complex register concerned the parallel morphing of several universal and ‘unbound’ conceptions of identity into unrecognizable avatars following the rise of targeted delivery of benefit alongside equally targeted surveillance technologies. We began encountering a new kind of subjectivity that surely rewrote the old Hegelian negotiation between subjec*tion*, or the condition of being a sovereign subject defined by the King and the State, and subjec*tivity*, or the individual egotistic interiorization of both the freedoms and responsibilities of the citizen-subject. Shah calls it a crossroads between being subjects *of* information (where we spend much of our life producing, consciously or otherwise, information about who we are, what we do, and how we relate to the world around us), subjects *to* information (as algorithmic data mining constantly produces information structures that determine various markers of who we think we are), and *subjective to* information (as we keep filtering everything that does not directly pertain to us, produce a bias in favor of information that is customized for our specific needs, and eventually find ourselves in filter bubbles, ‘echo chambers of network neighborhoods that protect us from people who are unlike us’).

At all these stages we encounter informational excess as a condition of existence, as we turn into subjects ‘whose *ontology* lies in information overload’. Such an ‘ontology’, says Shah, is pivoted around what may be the most basic, founding transformation taking place in our ‘rehumanization’: a move away from *representation*, upon which the entire polity of the 20th century was based, and into *simulation*. It is not, as we saw (in the Nariman judgment when free speech was being sought to be re-simulated into media of data storage and dissemination) a *break* from the past as much as it is the *re-signification* of the classical public sphere, morphing its key concepts such as democracy or rights into a new era that significantly redefines basic meaning-making languages that have historically founded our representation-driven 20th century. The shift from representation to simulation, paralleled by further transformations from author*ity* to author*ization*, also forces another transformation from older conditions of possibility to new structures defined by probability.

This ontology is manifested in permanent systemic crisis, but it is a crisis that, for perhaps the first time in history, has become *naturalized*. It has even turned into an everyday state of being. As human beings reconcile to their new condition (one that Hasan, on his side, names ‘responsibilization’), they become ever-more dependent on ‘information-overload managing technologies’, even as these technologies in turn ‘train’ human users to meet technology halfway. At the heart of information overload, says Shah, is the argument that we are now in a cybernetic feedback loop with ourselves, where we produce and consume our own data, and engage with it through multiple terrains so that we no longer can see outside of the data streams into which we are permanently immersed.

Such humans are a new construct – ‘yousers’, Shah calls them – with new claims, new promises (including, as he points out, the promise of immortality that requires the older human to step out of the model of being either human or relevant and to enter this new world where Google would be their savior) and, most of all, transformed citizenship norms. We are possessed by a ‘condition of informality’ that defines ‘our authorship, which in turn defines who speaks, on behalf of whom, in what voice, and with what authority’. It defines ‘agency, choice, freedom, and truth’.

It also appears connected with what Hasan calls a *techne* of neoliberalism that, while demanding a lesser or leaner government, often actually *expands* regulation and domination through multiple seemingly autonomous entities not part of the formal state apparatus but guided instead by a corporate enterprise logic. Hasan sees it as a confluence of two interconnected trajectories. One is precisely technological – the ‘electronification of governance’ redefined an old command-driven, centralized planned economy into a new center-periphery imagination. The second is more ideological, a neoliberal transformation of the democratic state that allowed – often in the name of the very people whose rights were being taken away – the conversion of state benefit into elite privilege.

## Being Possessed By

The authors of this volume first came together in 2010. This was a year after Aadhaar or the ‘Unique Identity for Every Indian Resident’ project had been announced with much fanfare by the Government of India, under which members of a large team were to research the grassroots social impact of mass digitization. ‘The Identity Project’ (as we named it) ran for three years, during which time we carried out detailed field research in seven Indian states, generated a mound of documentation, conducted four major workshops, and published three books.[[12]](#footnote-12) The multiple outcomes and findings of that particular project, on paper, PDF, and video, have been p8ublished and are easily accessible.[[13]](#footnote-13)

At that time, in 2010, we had sought – against, it must be said, considerable pressure from numerous friends, coworkers, and colleagues who offered grim forebodings about this new development and saw totalitarian designs behind it – to withhold judgment, and to try and understand what the digital ecosystem of governance might actually look like. It has been, as Ashish Rajadhyaksha’s essay shows, an unfolding story, especially in the startlingly *déjà vu* manner in which the new Arogya Setu app evoked, in 2020, much of the voluntary/mandatory shadow dance that we had seen in the old Aadhaar playbook. As the last decade panned out, especially in the series of Supreme Court judgments between 2016 and 2018, it appeared that a new story could be told of the earlier period when, coinciding with the arrival of social media, a new apparatus of state regulation was also being assembled.

Such a retrospective retelling, Rajadhyaksha suggests, would now place the National Population Register (NPR) as a far more central player in the story of the first two decades of the present century than we recognized when it was passed into law in 2010, to create a register of India’s ‘usual residents’, redefining both the Citizenship Act, 1955 and the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003. In 2010, it had appeared that Aadhaar, which had repeatedly claimed *not* to be mandatory and *not* about citizens but rather about residents, and had presented itself in far more social media-friendly terms than the NPR, had been in some conflict with the coercive approach of the NPR, which had made registration mandatory for all those who had either lived or intended to live in in India for six months or more. A retrospective timeline – especially outlined in detail by the 2018 Supreme Court judgment on Aadhaar – however suggests that the two were very much envisaged together and were indeed always meant to be two halves of a single picture.

Although this picture came together in public imagination only in 2019 with the passing of the Citizenship Amendment Act, 2019 and in the protests that followed, what it did mean was that, even as information-starved Indians everywhere were both consuming and producing digital content, we were also being possessed by a larger ecosystem that governed us. Such a state, and its attendant crisis, has been often most directly evidenced in anxiety around access: both the *granting* of access and concerns about the *control and regulation* of practices that emerge.

In 2018, the Supreme Court judgment defined the condition of being possessed by data in yet another way: by calling it ‘civil death’.[[14]](#footnote-14) It described what was happening as a ‘compulsory bartering away’ of ‘rights freely exercised, liberties freely enjoyed, entitlements granted by the Constitution and laws’. All these rights, liberties, and laws were being ‘made conditional’, and citizens were being compelled, in return, to give up their biometrics ‘voluntarily’, allow their biometrics and demographic information to be stored by the state and private operators, and then used for a process termed ‘authentication’.

Such an operation has, said the Court, the ‘*propensity to cause the civil death of an individual by simply switching of Aadhaar of that person*’. If the Indian Constitution ‘balances rights of individuals against State interest’, Aadhaar ‘completely upsets this balance and skews the relationship between the citizen and the State enabling the State to totally dominate the individual’.

Civil death, in this sense, may well be the extreme condition of such possession – where data is viewed as something of a life-support apparatus. More commonly, however, it redefines citizenship into a condition of suspended animation of what Hasan calls ‘slow violence’. In his detailed example of the digitization of landownership records, he describes it as the routine ‘violence of data repair’ when actual people find themselves trapped in a legally precarious condition of ‘temporal vacuity, a state of limbo, a temporary break from ongoing relationships’ which, while not an extraordinary event of ‘spectacular violence’, is nevertheless an equally deadly ‘circuitous low-grade suffering’.

## Accidental Possession and Verifiability

In July 2020, Delhi University’s much-respected professor of English, Hany Babu, was arrested by the National Investigation Agency, yet another target in the state crackdown on intellectuals, academics, and activists on the Left. As part of their inquiry, the Agency seized Babu’s computer, and their ‘forensic inquiry’ claimed, in what had become a by-now familiar police playbook, that some sort of a ‘disk partition’ had existed in that machine between February and April 2019, and that this partition had contained 62 files with ‘‘incriminating details’ about his involvement in the Maoist movement’.[[15]](#footnote-15) Hany Babu said he had made no such partition, possessed no such files.

Eight months later, five senior academics – including several of Hany Babu’s colleagues – went yet again to the Supreme Court with what appeared to be a far more basic anxiety than even the protection of their liberty: namely the potential loss of their research through unauthorized seizure of their computers and hard disks. Such seizure, they said, endangered decades of research work for their computers contained ‘their life’s work’, ‘extensive field work spanning decades or the results of scientific experiments or calculations’, ‘patentable material […] or work that runs the risk of being plagiarised’. All such research work was ‘irreplaceable’. In the hands of the police, it could ‘run the risk of damage, loss, destruction’ or – the academic’s ultimate nightmare – ‘even distortion’.[[16]](#footnote-16)

The question of what data is may in these fraught times open up, together with an ontology, a parallel epistemic trajectory. Documents, as Lisa Gitelman says in the beginning of her book *Paper Knowledge*, are at base ‘epistemic objects’, ‘recognizable sites and subjects of interpretation across the disciplines and beyond’ and are thus ‘evidential structures’ – essentially there to document, to *know* and to *show* (along with their corollary, ‘no show’, or no proof).[[17]](#footnote-17) While their digital variants may inherit some of these properties, these successor objects reveal a deeply disquieting elusiveness, where you (or rather, your device) could have chance encounters with other data or other human beings tampering with it, that can only be navigated in real time.

Raw data, says a well-known book, is an ‘oxymoron’ for data is everywhere, always already ‘cooked’.[[18]](#footnote-18) ‘Access-centered discourse overrides the complex terrain of the human-technology relationship – usage, adoption, penetration, internalization, proliferation, nudging – and becomes the single point of obsession in telling the promise of the internet’, writes Shah. There is a double bind of anxiety, defining both the concerns around privacy (and the draft Personal Data Protection Bill of 2019) or the multiple Terms of Service and of Intermediary Liability that define both informational control and access regulation. It is a role that the state in its orthodox avatar is often unable to perform, forcing new layers of ‘*state-like organizations* that would take up state-like functions in order to help deal with the threat of access’.

Shah’s introduction of pornography into this picture, and his addition to the famous Rule 34 of the internet that claims that ‘If something exists, there is [internet] porn of it’, with a further Rule 35 that ‘If there is porn on the net, people will access it’, also brings a new political edge to transgressive access which he understands as a question of agency within the logics of regulation. In January 2018, when a news report appeared that a journalist had been able, via a WhatsApp group and an INR 500 bribe, to access the main databases of Aadhaar, the journalist, instead of being recognized as a whistleblower, was promptly charged with a criminal offence.[[19]](#footnote-19) Among those who came to her rescue at the time was Edward Snowden. He contended that Aadhaar was ‘creating a systemisation of the public’ that was unrelated to its original agenda.

The incident, alongside the tantalizing ease of the hack, also brought to the fore the phenomenon of what we might call accidental possession. This is *data contaminated*, not in its content, not even by how you came across it, but most commonly in the way *it* accessed *you*. The idea that there exists only one single definable truth and any truth becomes a truth only when it is *verifiable*, as this entire teleology of truth-production got technologized (usually by interminable systems of authentication), it also produced strange fruit that produced the very opposite of their stated intentions when you found yourself caught within the irresistibility of its flow.

There has been, for example, the growing phenomenon of *impunity*, or what political theorist Anant Teltumbde calls the ‘macabre spectacle’ of extreme violence conducted in the full glare of the media.[[20]](#footnote-20) When perpetrators of violence perform their actions in front of cameras, leaving no one in doubt as to what happened, but nevertheless force a legal challenge to the verification apparatus precisely from the excess of data they have produced, they point to one of the basic consequences of what Rajadhyaksha calls ‘creep’. If the entire history of state digitization, from the Information Technology Act of 2000 through to Aadhaar 2009 to the Citizenship Amendment Act of 2019, unveils a relentless process of making ‘creep’ ubiquitous through the incessant production of information overload, it necessarily also opens a disquieting underside. Both the hacker’s pornographic transgressions and its opposite, fears of police tampering, evoke the same crisis as do the perpetrators of violence on camera – the possibility that data in its very nature is always already contaminated, and that both the ‘truth’ it stands for as well as the apparatus of its verifiability remain compromised. What we see is, in a way, a new problem for democratic governance, and it points to one of the more bizarre consequences of the transition of the subject from a beneficiary of data practices into a source for data harvesting.

## The Body, the State

Much of this book deals with the apparatus of the digital state. As the crisis of the informational subject reveals itself and reveals thereby the unprecedented challenges to the Directive Principles of the Constitution of India that define the responsibilities of the state, it necessarily opens up a larger question on the ideologies of the state apparatus itself – as distinct from the ruling ideologies of whichever government happens to be in power. There was once the idealism of a hierarchical, centralized, ordered state that regulated, along with its data itself, a parallel meaning-making apparatus on what the data meant, how it should be interpreted, who should be given access to it, and how it could translate into policy. From the 80s, this idealism was replaced with a second idealism of the neoliberal state, this time premised on the seamless capacity of data to travel unhindered, to become both universally accessible and universally intelligible. Such a belief, which underpinned the protocols of networking and delivery of targeted benefit, was in some measure adapted from the early idealism of the internet, one that (we have suggested above) Justice Nariman’s judgment of 2015 may well have brought to a close. We need, as we turn to a yet more recent chapter in both idealisms, to not only question their salience, but also to track – as Nafis Hasan does at the end of his essay – a yet further development, where once again the state is seeking to close down its borders to once more localize access: this time within the boundaries of the nation.

Already, in 2019, and long before the pandemic saw national borders being made tighter and more impregnable than perhaps ever in history, both the morphing of the colonial Section 144 of the Indian Penal Code (the right to public assembly) into the longest and most severe internet shutdown the world has seen in Kashmir (over 500 days) – a blanket shut off from data that threatened a ‘civil death’ type crisis of unprecedented proportions – as well as the extreme Emergency-like deployment, with the first COVID-19 outbreak, of the National Disaster Management Act, 2005 in March 2020 revealed further state reinventions through reinscribing real-life conditions into virtuality and back into real life, and also the central presence of the embodied informational subject in these makeovers. Overriding the question of how data challenges the sovereignty of the nation-state, what we may be witnessing is something opposite, namely the reinscription of data to make something of a massive digital cartography project in the re-encoding of the state. Its various *avatar*s,[[21]](#footnote-21) from hierarchical to networked to boundary-driven – and the corresponding *avatar*s of its citizen, from resident (Aadhaar’s favored term) to ‘usual resident’ (as used in the NPR) to beneficiary to ‘natural person’ and ‘data principal’ (as used in the Personal Data Protection Bill) – may well be best comprehended as simulations of the models of democracy rather than merely their digital renditions.

One result of this simulation process is the growing *weaponization* of concepts like ‘sovereign national interest’ and ‘security and integrity of India’ to define a new legal apparatus alongside the multiple new identity and biotechnological checks that regulate national borders. India’s legal system has, says legal theorist Gautam Bhatia, in recent years taken a major turn.[[22]](#footnote-22) Indian law has historically been constituted by two parallel regimes, the criminal justice system (or CJS) characterized by elements of due process, personal rights, and rigorous judicial review of state power, and a parallel ‘preventive detention system’ (PDS) in which none of these features obtain.

The two halves have been historically incompatible, but in recent years this incompatibility has been solved by the simple if deadly expedient of the return of the old colonial sedition law and its sequel laws, Terrorist and Disruptive Activities (Prevention) Act, 1987 (TADA), Prevention of Terrorism Act, 2002, and now the Unlawful Activities Prevention Act, 1967. All of these have been premised on custodial detention, on absolute executive (as against judicial) supremacy. Almost all are derived from unpredictable encounters with contaminated data.

Such weaponization of the apparatus of verifiability could be intentional and targeted, as with digital benefit and surveillance, or could emerge as a consequence of the sheer randomness of accidental possession – where you did not discover data as much as it discovered you, or when your inadvertent stumbling into a data ecosystem automatically criminalized you. Identity here becomes a life-and-death matter of dealing with essentially accidental encounters. If its extreme condition is the threat to life itself – when a person’s digital identity gets obliterated, hacked, or simply shut off – mostly it is a slow-burning process of coming to terms with both the aspirational as well as targeted consequences of overload, to learn overnight when to be visible and when it is best not to be.

The focus on the embodied data-subject is thus no longer merely the bearer of data but an instantiation of the data practices into which the body finds itself immersed, voluntarily or otherwise. The weaponization of data as evidence to punish, control, and contain the body is therefore a corollary of digital misinformation and civil death. Both conditions are eventually tied to the idea of ownership defined not in terms of possession but of *distribution*. If data evidences are no longer about discrete bodies and institutions where ownership can be demonstrated, disrupted, or contained, then we could be looking at new challenges posed by the conditions of data circulation to meaning itself.

In the end, if Justice Nariman’s pronouncements on data may have ended one kind of internet dream, his parallel point about making ‘no distinction’ between ‘mere discussion or advocacy’ and ‘incitement by which such words lead to an imminent causal connection with public disorder’ may well open up another possibility.[[23]](#footnote-23) The signification of data through circulation exists within, but also breaches, the boundaries of the state. In either case, it defines several of our immediate political challenges, the subjective condition of being immersed in informationality, or the consequences of being disconnected from it.

1. Supreme Court of India, *Shreya Singhal* v *Union of India*, WP (Criminal) No. 167 of 2012 (24 March 2015), https://indiankanoon.org/doc/110813550/. [↑](#footnote-ref-1)
2. The original 66A said that ‘any person who sends, by means of a computer resource or a communication device, (a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device, (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine. [↑](#footnote-ref-2)
3. # Pranesh Prakash, ‘Social Media Regulation vs. Suppression of Freedom of Speech’, *Kafila Online*, 19 November 2012,

   https://kafila.online/2012/11/19/social-media-regulation-vs-suppression-of-freedom-of-speech-pranesh-prakash/. [↑](#footnote-ref-3)
4. Pranesh Prakash, ‘Adding Insult to Injury’, *Outlook India*, 19 November 2012, https://www.outlookindia.com/website/story/adding-insult-to-injury/283033. [↑](#footnote-ref-4)
5. *Shreya Singhal* v *UOI*. [↑](#footnote-ref-5)
6. Supreme Court of India, *S. Rangarajan Etc* v *P. Jagjivan Ram*, 1989 SCR (2) 204, 1989 SCC (2) 574, 30 March 1989, https://indiankanoon.org/doc/341773/. [↑](#footnote-ref-6)
7. *Shreya Singhal* v *UOI*. [↑](#footnote-ref-7)
8. Supreme Court of India, *Romila Thapar* v *Union of India*, Writ Petition (Criminal) No. 268 of 2018, 28 September, 2018, https://indiankanoon.org/doc/52834611/. This concerned the arrest and incarceration without bail of several well-known activists, lawyers, and academics in 2018, known as the ‘Bhima-Koregaon’ case. On the occasion of the bicentenary celebrations of a colonial war celebrated by the Dalit community in Maharashtra, a political rally was held. It led to retaliatory violence, that in turn led to a major crackdown across the country. Most of the arrested are still in jail. [↑](#footnote-ref-8)
9. *Romila Thapar* v *UOI*. [↑](#footnote-ref-9)
10. Internet shutdown for 552 days, starting August 4, 2019, when Article 370 of the Constitution was abrogated by Parliament. [↑](#footnote-ref-10)
11. Partha Chatterjee, *I am the People: Reflections on Popular Sovereignty Today*, Ranikhet: Permanent Black, 2019, p 73. [↑](#footnote-ref-11)
12. See Ashish Rajadhyaksha, *The Last Cultural Mile: An Inquiry into Technology and Governance in India*, Bangalore: The Centre for Internet & Society/Researchers@Work, 2011; Rajadhyaksha (ed.), *In the Wake of Aadhaar: The Digital Ecosystem of Governance in India*, Bangalore: Centre for the Study of Culture and Society, 2013; Atig Ghosh (ed.), *Branding the Migrant: Arguments of Rights, Welfare and Security***,** Kolkata**:** Frontpage Publications Ltd., 2013. [↑](#footnote-ref-12)
13. The entire video archive is available on the open access platform pad.ma. See https://pad.ma/grid/title/list==zi:The\_Identity\_Project. [↑](#footnote-ref-13)
14. ‘Gist of the Challenge to the Aadhaar Scheme as Well as the Act’, Sec 59, Supreme Court of India, *Justice K.S. Puttaswamy (retd)* v *Union of India*, Writ Petition (C) 494/2012 (2018), https://main.sci.gov.in/supremecourt/2012/35071/35071\_2012\_Judgement\_26-Sep-2018.pdf. [↑](#footnote-ref-14)
15. Sukanya Shantha, ‘Elgar Parishad: NIA Arrests Hany Babu, 'Pressured Him to Implicate Colleagues, Others,’ Says Wife’, *The Wire*, 28 July 2020, https://thewire.in/government/nia-bhima-koregaon-hany-babu-arrest-gn-saibaba. [↑](#footnote-ref-15)
16. Krishnadas Rajagopal, ‘Plea in Supreme Court to Save Academic Freedom’, *The Hindu*, 30 March 2021, https://www.thehindu.com/news/national/plea-in-supreme-court-to-save-academic-freedom/article34200750.ece. [↑](#footnote-ref-16)
17. Lisa Gitelman, *Paper Knowledge: Towards a Media History of Documents*, Durham: Duke University Press, 2014, pp 1–2. [↑](#footnote-ref-17)
18. Lisa Gitelman (ed.) *‘Raw Data’ is an Oxymoron*, Cambridge: MIT Press, 2013. [↑](#footnote-ref-18)
19. ‘Journalists Exposing Aadhaar Deserve Award, Not Investigation: Edward Snowden’, The News Minute, 9 January 2018,

    https://www.thenewsminute.com/article/journalists-exposing-aadhaar-deserve-award-not-investigation-edward-snowden-74409. [↑](#footnote-ref-19)
20. Anant Teltumbde, *The Persistence of Caste: The Khairlanji Murders and India's Hidden Apartheid*, London: Zed Books, 2010, pp. 54, 137. [↑](#footnote-ref-20)
21. Avatar, in this context, is a variant phase or version of a continuing basic entity. [↑](#footnote-ref-21)
22. Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts*, New Delhi: Harper Collins, 2019, p 257. [↑](#footnote-ref-22)
23. *Shreya Singhal* v *UOI*. [↑](#footnote-ref-23)