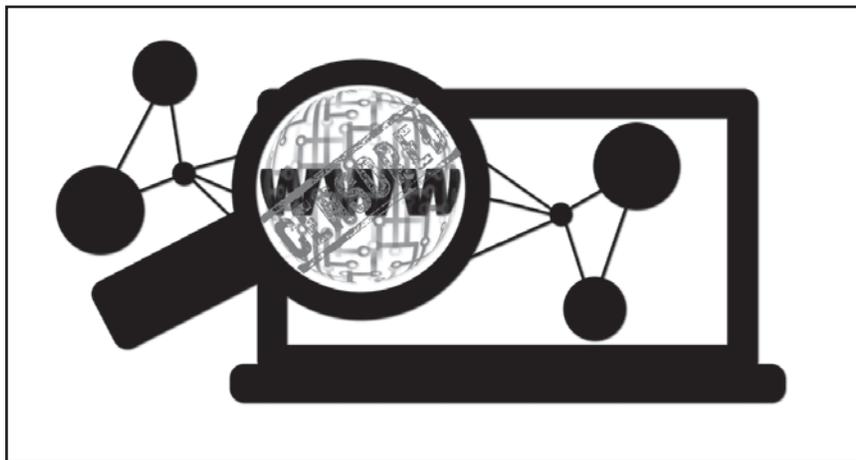


THE HIGH PRICE FOR ONLINE FREEDOM

The Role of Rights, Realities and the Law

Anshi Beohar*



The Constitution of India has guaranteed freedom of speech and expression and personal liberty of the citizens as well as ensured freedom to the press under Articles 19 and 21 as fundamental rights. However, these rights are subject to reasonable restrictions placed on grounds of national security, morality or public indecency, contempt of court, threat to the sovereignty and integrity of India or on similar grounds. Engaging in acts like sedition, hate speech and defamation can have serious consequences under the Indian Penal Code. Often, the line between offensive behaviour and innocuous communication is exceedingly blurred. These wide and ambiguous interpretations of expression are brought into sharper focus in online spaces, where limits on free speech are constantly tested and scrutinised.

This article will focus at the right

to freely use the internet from various perspectives, specifically highlighting the legal frameworks around it. In addition to this, it will discuss how various mechanisms to restrict access to online content or websites such as internet shutdowns come into direct confrontation with the right to the fair use of internet.

Common Cause Petition

Section 66A of the Information Technology (IT) Act, 2000 had been in the eye of a storm for being a provision in cyber law that was seen by advocates of free speech as targeting people with critical political views. It provided punishment of imprisonment for up to three years and fine for sending offensive messages online.

This law was often used to treat so-called offenders with a heavy hand and they frequently received penalties disproportionate to their actions.

In light of such incidents, Common Cause filed a writ petition in the Supreme Court, challenging the constitutional validity of sections 66A, 69A and 80 of the Information Technology Act, 2000 (as amended in 2008), among other provisions, on grounds of being violative of Articles 14 and 19 of the Constitution of India. The petition was tagged along with Writ Petition (CrL.) No.167 of 2012, *Shreya Singhal v. Union of India*.

The two-judge bench of the Supreme Court comprising Justice Chelameswar and Justice Nariman passed a landmark judgment in March 2015, where Section 66A of the Information Technology Act, 2000 was struck down as being violative of Article 19(1)(a). The court held that Section 66A of the Act restricted freedom of speech and expression while failing to classify between discussion or advocacy and incitement.

However, according to a report by *HUFFPOST*, 3,137 arrests were made under Section 66A in 2015, even though the Section was struck down in March 2015.

Online Censorship and Bans

Like most nations, India too has become an engaged participant across social media platforms.

*Anshi is a Legal Consultant at Common Cause

Unfettered access to the internet has ensured that it has become a podium of meaningful debate and conversation.

Across the world, social media has driven political change, helped democratically minded individuals to come together and be a catalyst for social movements. Simultaneously, comment threads on the same online platforms are coloured with prejudices like racism, sexism and much more.

Therefore, ideas of monitoring, surveillance and censorship of online content are gaining momentum more than ever before.

In India, both the excess as well as lack of censorship on internet have been realities. One's freedom of speech has often been in conflict with another's right to privacy. As the right to privacy has been recognised as a fundamental right under Article 21 of the Constitution by the Supreme Court in August 2017, the concerns and issues around it in the online domain are bound to undergo rapid transformation.¹

Even when the right to privacy was not so clearly defined, there were other grounds for implementing "reasonable restrictions." The debate around censorship is a complex one in India, as it needs to be framed against morality and ethics. Also, much of the online censorship is carried out in a heterogenous manner, but the most common practice is to remove the censored content or completely ban the concerned website/s.

Therefore, regulation of online content is at the centre of conversations around democracy now.

One recent instance of content blocking has been the banning of websites hosting pornography. On one hand, this was perceived as an act of moral policing and violation of the net neutrality rules while on the other there have been opinions validating this step, citing research studies on porn and violence against women and children. As of November 2018, more than 800 websites have been banned while social media websites like Twitter have transformed into a slugfest of views favouring and opposing the ban.

As of now there are no legal provisions in India that specifically curb viewing pornography. However, its publication or transmission is legally forbidden. Interestingly, the latest order of an Indian court has led to a blanket ban or generic ban, where many online portals carrying pornographic content were taken down.²

The question of internet censorship needs to be seen against the backdrop of India being the world's largest democracy. Internet freedom acquires grave undertones when we place it in the context of the country's large population which is seeing a fast penetration of the internet.

"In a nutshell, while there is no sustained government policy or strategy for large scale internet

censorship, central and state governments in India have adopted a number of measures and powers in order to remove internet content or block access to it," says Dr. Pradeep Kumar Misra, in his post *Public Opinion On Censorship Of Internet In India: A View From Up*.³

Before net neutrality came into force, even service providers could restrict access to specific online material within their network. Websites too were banned by the state owing to intellectual property violations, especially on distribution of pirated content. Today, a lot of websites conduct automated sweeps for pirated, inappropriate or offensive content so that their websites are not banned by the state.

On April 25, 2018, *The Indian Express* revealed that Indian internet service providers (ISPs) have installed the highest number of Internet filtering systems and blocked the maximum number of web pages. It added that other than those dealing in porn or piracy, websites and web pages found blocked at different points during the testing period in India include those belonging to domestic and foreign NGOs, United Nations organisations, human rights groups, health forums, feminist groups and political activists.⁴

Cyber Security: A Real Threat

With the advance in technology, cyber security has become a

serious concern. Given the increase in number of incidents in this domain, a government-mandated information technology security organisation called Indian Computer Emergency Response Team, or CERT-In was established. It was set up by the Department of Information Technology in 2004 to report on vulnerabilities and to promote effective IT security practices throughout the country. CERT-In is also responsible for ensuring emergency measures when episodes of cyber security breach occur and can issue guidelines, advisories and whitepapers relating to information security practices, procedures, prevention, response and reporting of such incidents.

Internet Shutdowns

Policing the internet is a reality today. And a weapon to bring digital communications to a grinding halt is the internet shutdown. The authorities temporarily shut down telecom networks with the objective of disrupting chains of misinformation or controlling law and order situations.

Access Now, an international non-profit, human rights, public policy, and advocacy group dedicated to defending and extending the digital rights of users has initiated #KeepItOn, a global campaign against Internet shutdowns .

According to Access Now, in order to control the actions of people, governments use blackouts to disrupt particular

mobile apps or sometimes, internet, within their territories. It says: "An internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information."

India has seen a sharp upsurge in the number of internet shutdowns in the last three years. Of the total 268 shutdowns since 2012, more than 120 shutdowns took place in Jammu & Kashmir, followed by 56 in Rajasthan while more than 240 have been reported in the last three years.⁵

Additionally, internet shutdowns have impacted the Indian economy. Internet bans in 2018 alone have led to a loss of more than Rs 22,150 crore in the country.⁶

Until recently, there was no specific regulation to deal with internet shutdowns. On August 7, 2017, the Ministry of Communications issued and notified Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 (to be referred to hereafter as Telecom Suspension Rules). This was meant to regulate the temporary suspension of telecom services due to public emergency or public safety, and the rules were issued under Section 7 of the Indian Telegraph Act, 1885. Prior to the Telecom Suspension Rules, the Telegraph Act, 1885 and Code of Criminal Procedure,

1973 were invoked to impose internet shutdowns.

Indian Telegraph Act, 1885

The first incident of internet shutdown occurred in 2012, in Kashmir.⁷ Mobile internet services were suspended for a few hours then in the Kashmir Valley, under Section 5 of the Indian Telegraph Act, 1885, in the interest of public safety and for maintaining public order. Section 5(2) states that "on the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence..."

This provision empowers the government to take possession of licensed telegraphs or order interception of messages. Section 3(1AA) of the Telegraph Act, defines telegraph as: "any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, radio waves or Hertzian waves, galvanic, electric or magnetic means."

This law is more than 150 years old and yet, the definition is broad enough to cover internet and any other future technological developments. This statute gives uncontrolled power to both the central and the state governments as well as any authorised officer to prevent the transmission of any information. The same law also empowers the state to tap phones.

Code of Criminal Procedure, 1973

The most frequently invoked legal measure to cut off internet access in India is Section 144. The majority of internet shutdowns recorded from 2012 to April 2018 have been ordered under Section 144 of the Code of Criminal Procedure, 1973.⁸ This section provides state governments the power to issue orders for immediate remedy in urgent cases of nuisance or apprehended danger. It has been used to deal with law and order situations and unrest in the community by imposing curfews, dismissing unlawful assemblies and issuing any other necessary orders. Apart from a maximum time period of six months, this provision has no other limitations. In fact, a Judicial Magistrate can order service providers to blackout internet, in order to handle an emergency situation or crisis.

Critics have hailed internet clampdowns across the world as emblematic of authoritarian regimes. Human rights groups and press freedom advocates have consistently decried

internet bans and other acts of cyber repression for intruding on human rights. Section 144 itself has come under censure from a lot of quarters. “Governments initially justified shutdowns on the back of Section 144 of the Code of Criminal Procedure (CrPC)—an amorphous legal provision that empowers a district magistrate with wide discretion to pass orders as she deems necessary for public safety,” says Nakul Nayak.⁹ According to Apar Gupta, Co-Founder of Internet Freedom Expression, the social costs and the deprivation of fundamental rights are high when the internet is shut down. He says that a shutdown takes away the freedom of speech and expression from people, but much more deeply.¹⁰

Internet shutdowns also impact the right to education or right to practice business or trade. This led to a PIL in the High Court of Gujarat, *Gaurav Sureshbhai Vyas v. State of Gujarat*,¹¹ where the High Court upheld the power of the State Government to impose the internet shutdown under Section 144. On appeal, the Supreme Court bench headed by the then Chief Justice T S Thakur upheld the High Court’s decision in this regard.

Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017

As discussed earlier, the specific regulatory framework around

internet shutdowns in India is pretty recent. Through these rules competent government authorities were conferred the powers to order internet bans in districts and states of India.

According to the Telecom Suspension Rules, directions to suspend telecom services shall not be issued, except by an order made by the competent authority, accompanied by the reasons for the suspension. In this case, competent authority is the secretary in the Ministry of Home Affairs for the central government and the secretary to the state government, in charge of the Home Department. However, in “unavoidable circumstances,” an order might be issued by an officer of the rank of joint secretary or above who has been duly authorised by the Union Home Secretary or State Home Secretary, subject to the confirmation of the competent authority within 24 hours of the aforesaid suspension order.

There are several reasons why the Telecom Suspension Rules have been smothered in criticism. To begin with, these new rules were passed without any pre-legislative public consultation,¹² and the stark ambiguity of the statute reflects that. More importantly, the rules do not define “unavoidable circumstances.” Even where the statute provides definitions, they are broad and vague.

In addition, the rules also do not mandate a public notice to disseminate the information of a

shutdown. There is provision for review committees, both at the centre and state levels, which will receive these suspension orders in the next working day of the date these orders are issued. They will then conduct a meeting within the next five working days of the issue of directions for suspension, to record its findings on the legitimacy of the order. However, there is no mention of another appellate authority in the rules.

Additionally, the review committee only includes members of the executive, a structure that does not guarantee transparency. Next to no consideration is given to the undeniable reality of modern life, which is governed by a high reliance of citizens on the internet for accomplishing daily processes like e-commerce, e-governance, cloud computing and financial services. For fair representation the review committee should have included all stakeholders.

The new rules have been panned by several sections for their defects. Although they bring in a lot of checks and balances, including giving powers to higher authorities to issue internet shutdown orders, they also entail curbing fundamental rights of citizens. One may argue that it is reasonable when severe measures like internet shutdowns are used to put an end to an ambience of fear and mistrust heightened by rumours on social media. However, the same instrument can easily

be employed, time and again, merely to interrupt a channel of communication and to present a situation perceived to be more critical than it actually is.

This also feeds into an ongoing global debate on whether it is justifiable for governments to monitor and analyse online content before blocking it altogether. There are also worldwide conversations on the reasonableness of being penalised for what the state considers transgressive internet behaviours.

Conclusion

Internet use, or going online is a daily ritual for most of us. Internet, in fact, is an enabling technology that is helping people to engage with multiple voices and cement a political and social identity. It is also the great transformer with the ability to pull populations out of poverty and foster opportunities. Its empowering influence, however, comes with a rider. One is exposed to data surveillance more than ever before. Simultaneously, there's censorship and continuous encroachments on digital privacy.

In 2018, Freedom House, an independent watchdog organisation, dedicated to the expansion of freedom and democracy around the world, analysed 65 countries across the globe and came up with a Freedom on the Net Report. Titled *The Rise of Digital Authoritarianism*, it says: "With or without malign intent, the

internet and social media in particular can push citizens into polarized echo chambers and pull at the social fabric of a country, fueling hostility between different communities. Over the past 12 months in Bangladesh, India, Sri Lanka, and Myanmar, false rumors and hateful propaganda that were spread online incited jarring outbreaks of violence against ethnic and religious minorities."¹³

The report also drove home some hard truths. It laid bare Facebook's claim that the majority of content requested to be removed by Indians were found to be in violation of laws on hate speech and defamation of religion and the state . It also revealed that there has been a rise in disturbances on the grounds of ethics and religion, on issues like cow smuggling, child kidnapping, etc. due to fake news distribution on various platforms and an escalation in the circulation of hate speech . Tools like Social Media, Blogging, etc. have become the vessels of hate speech and fake news.

Clearly, given India's economy slowly moving towards internet connectivity, costs of switching off can be high. Online censorships will not only result in continued and sustained losses to the nation's coffers, but will also be a strain on the rights of individuals. Denial of the free use of internet undermines possibilities of political participation and limits opportunities for civil societies. And that can only have negative

consequences for the health of our democracy.

Endnotes

1. Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors., WP (C) 494 of 2012
2. Digital Empowerment Foundation (2015, September) Limited Access Restricting Expression. Retrieved November 13, 2018, from http://internetrighits.in/wp-content/uploads/2015/10/Country-Research-Report_September-2015.pdf
3. Dr. Misra, P K. (December 3, 2014) Public Opinion On Censorship Of Internet In India: A View From Up. CGCS MEDIAWIRE. Retrieved December 30, 2018, from <https://global.asc.upenn.edu/public-opinion-on-censorship-of-internet-in-india-a-view-from-up/>
4. Mazoomdaar, J and Sarin, R. (April 25, 2018) India tops list of websites blocked, its telcos filter the most. *The Indian Express*. Retrieved December 30, 2018, from <https://indianexpress.com/article/india/india-tops-list-of-websites-blocked-its-telcos-filter-the-most-netsweeper-5150620/>
5. SFLC.IN. Internet shutdowns. Retrieved November 30, 2018, from <https://www.internetshutdowns.in/>
6. Jalan, T. (December 10, 2018) Congress MP Tharoor urges a review of internet shutdown rules in India. *MediaNama*. Retrieved December 10, 2018, from <https://www.medianama.com/2018/12/223-shashi-tharoor-review-internet-shutdown-rules/>
7. SFLC.IN (2018,May) Living in Digital Darkness - A Handbook on Internet Shutdown. Retrieved November 15, 2018, from <https://sflc.in/sites/default/files/reports/Living%20in%20Digital%20Darkness%20-%20A%20Handbook%20on%20Internet%20Shutdowns%20in%20India%2C%20May%202018%20-%20by%20SFLCin.pdf>
8. *Ibid.*
9. Nayak, N. (October 6, 2017) The Recently Notified Rules on the Suspension of Telecom Services Legitimise Internet Shutdowns and Facilitate Voice Call Bans. *The Caravan*. Retrieved December 31, 2018, from <https://caravanmagazine.in/vantage/suspension-telecom-services-rules-legitimise-internet-shutdowns-facilitate-voice-call-bans>
10. (October 3, 2018) IETHinc: Is Internet shutdown the new order for law & order? *The Indian Express*. Retrieved December 31, 2018, from <https://indianexpress.com/article/technology/tech-news-technology/is-internet-shutdown-the-new-order-for-law-order-5383491/>
11. *Gaurav Sureshbhai Vyas v. State of Gujarat*, W.P. No.191 of 2015
12. Internet Freedom Foundation. Keep Us Online. Retrieved November 30, 2018, from <https://internetfreedom.in/shutdowns-petition/>
13. Freedom House (2018, October) The Rise of Digital Authoritarianism: Freedom on the Net – 2018. Retrieved November 22, 2018, from https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf