BALANCING CYBER LIBERTIES AND NATIONAL INTERESTS: EXAMINING INDIA'S INTERNET FREEDOM LANDSCAPE

Yash Singh Naruka, National University of Study and Research in Law, Ranchi

ABSTRACT

The Information technology since the last decades has penetrated the mind and souls of human beings with its unfettered functionalities and has acquired such a significant place in the lives of people, that depriving someone of their right to internet access would be violative of a basic human right as stated by the United Nation Human Rights Commission in 2016. The apex court of the country through its rulings has also held that any law depriving the citizens of their personal liberty has to go through tests under articles, 14, 19, and 21 i.e, the golden triangle of the Constitution of India and also that article 19 (1) (a) protects the right to disseminate and receive information through the internet. But the frequent escalation of internet shutdowns or such blanket bans to curb hate speech and misinformation by the government in recent years has put themselves in controversy every now and then who justify these actions in the name of "national security" and "ensuring public safety". These are not always convincing unless transparent reasons are made apparent to the voices of dissent concerned about their democratic rights such as freedom of expression and assembly. Such shutdowns are ordered under section 144 of the CrPC, section 69 A of the Information Technology Act 2000 or section 5(2) of the Telegraph Act which has been debated extensively regarding their constitutionality in many cases leading to formulation and introduction of the "Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017" (Internet Shutdown Rules, 2017) prescribing competency of the authorities to order such shutdowns resulting in imposition of 55 curfews in the state of Jammu and Kashmir alone in 2019 depriving the territory of internet for 18 months. This paper discusses existence of the right to internet, the statutory validity of internet shutdowns and tries to explore the justifications behind the action of the authorities in context of various landmark cases and recent facts and figures. Further, the disputed arguments behind the supporters of

this impediment to internet access with that of advocates of article 19 are also discussed.

Keywords: National Security, Public Safety, Internet, Emergency.

INTRODUCTION

"Everyone is entitled to their opinion about the things they read (or watch, or listen to, or taste, or whatever). They're also entitled to express them online"

- *John Scalzi*

The internet and digital media have become an essential part of our lives, providing us with connectivity, communication, information sharing, learning, and knowledge. With the COVID-19 pandemic, we have realized the importance of the internet in keeping us connected and productive. India has over 104 crore active wireless subscribers as of August 2022, which is a testament to the importance of the internet in the country. Vinton Cerf and Bob Kahn, who invented the internet, have truly blessed us with this technology, and it has become an indispensable part of our lives.[1]

Furthermore, the government is also continuously striving for making the internet connectivity reach every corner to keep their connectivity with the government's service centers, education resources and real time information as much as possible with various programs like the BharatNet under the Ministry of Communications and Technology which has already provided wi-fi access to 1,32,700 Gram panchayats throughout the country as of now.[2] Also, the flagship program of the government to increase internet accessibility among its citizens and economy, improve stable digital infrastructure and deliver internet services, the Digital India Program launched in 2015 has been flourishing and has brought a digital revolution in the country. Therefore, the internet is being treated as a public utility as we can derive for it is a basic necessity these days in the form of digital spaces, clouds, and other digital platforms hence it puts the onus on the state to protect, guarantee, and promote internet services throughout the country.

But when the state itself tries to intervene with such a right which itself has provided to the people, we see conflicts arise regarding a number of issues and have witnessed the setbacks

[1] Hogback, J. (2016). *Who invented the internet? Encyclopædia Britannica*. Available at: https://www.britannica.com/story/who-invented-the-internet (Accessed 14 February, 2022).
[2] http://bbnl.nic.in/usage2.pdf (Accessed 14 February, 2022).

various states have experienced with the restriction in the name of blanket bans on the internet or the internet shutdowns in their territory by the central government. Internet shutdowns could be defined as either partial or total restriction to internet access in an area through intervening with internet servers, mediums, and mobile networks which does no discrimination between the kind of content needed or shared through it thereby witnessing issues from human rights and freedom of speech and expression advocates. It has been observed to be disrupting the internet in a whole region for a period of time which could either be intimated earlier or be kept suspended for an infinite period as the circumstances allow as according to the authorities. Since 2012, the country has seen 647 government-imposed internet shutdowns being the highest in the world as of June 2022, a Statista report says.[3]

This has resulted in the country's position in the international stage on freedom of internet degrade further and has designated India being partial free democracy going along with the trend of declining global freedom of internet in the world as the Freedom House reported[4]. These shutdowns are also seen as an authoritarian act to prevent the mobilization of information that has the ability to challenge the ruling government[5]. Also, the legal and democratic values including the economic, commercial interests are overlooked and hence are being traded off with this technological disruption. With an alarming rise in numbers throughout the territory, these shutdowns being an issue of concern has attracted lots of attention with legal and policy issues. Because of the importance of the digital environment in today's society, the impacts of Internet outages cannot be ignored. The Internet is important as a source of information and knowledge since it is not just vital from a technological or commercial standpoint but also for the practise of democratic ideals like assembly and freedom of expression. The Internet has developed into an important forum for the approximately 50% of the world's population that is online, despite the traditional media outlets—TV and radio—continuing to play a fundamental role in the creation and dissemination of content. Particularly in many of the nations impacted by widespread Internet shutdowns, marginalization and exclusion from the Internet remain serious problems.

---

[3] Basuroy, T. (2022, June 9). *India: Number of internet shutdowns 2022. Statista*. Available at: https://www.statista.com/statistics/1095035/india-number-of-internet-shutdowns/ (Accessed 14 February, 2022).
[4] Shahbaz, A., & Vesteinsson, K. (2022). *Freedom On Net 2022. Freedom house* Available at: https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf (Accessed 14 February, 2022).
[5] Ruijgrok, K. (2022) *The authoritarian practice of issuing internet shutdowns in India: the Bharatiya Janata Party's direct and indirect responsibility, Democratization,* 29:4, 611-633, DOI: 10.1080/13510347.2021.1993826 Available at: https://www.tandfonline.com/doi/epdf/10.1080/13510347.2021.1993826?needAccess=true&role=button (Accessed 14 February, 2022).

Now, what argument government provides to justify this measure comes out to be for national security which has continuously been applied to protect the state and its citizens from any national crisis like terrorism, Communal disharmony, nuclear issues, espionage, etc, which are governed as subjects of security given by Article 352 and under Emergency provisions in Part XVIII of the Constitution of India. No matter what arguments are in place, when nations choose to ban access to the Internet, they are interfering with crucial communications networks. Many advocacies' organizations link this to the restriction of free speech. The "right to connect" or "freedom to connect" movement essentially contends that access to the Internet is necessary for people to exercise their First Amendment freedom of expression rights. The UN stated its concern with measures that "intentionally prevent or disrupt access to or dissemination of information online," a clear reference to Internet shutdowns, and asserted that "the same rights people have offline must also be protected online." This paper basically revolves around this controversial argument of the state to curb internet services under its statutory power exercised by their executives which is also discussed. This paper's main interest is not whether an Internet shutdown impacts the freedom of speech in this situation, but rather whether the restrictions put in place by governmental actors may be justified in the name of national security or not and, if so, under what legal circumstances. Further, its ambit and its conflict with the right to internet under Article 19(1)(a) of the constitution of India has been discussed and legal analysis within the constitutional framework has been done to understand the facts and various cases relating to the issue with an analysis of historical records.

INSTRUMENTS OF INTERNET SHUTDOWNS

While we talk of getting the refuge of section 19 of the Constitution of India, we must keep in mind that this fundamental right can only be exercised if the state according to article 12 when takes away or abridges any such right. But the state has been given an exception under the same article which gives the right to the state to impose reasonable restriction on the exercise of such rights as under article 19(2) for the interests of the sovereignty, and integrity of India as Article 19 does not confer on its population an absolute right. The state by exercising these right uses internet shutdowns as a tool to restore public integrity and peace by their executives through Section 144 of the Criminal Procedural Code, 1973, Section 69 A of the Information Technology (Amendment) Act, 2008 and Section 5(2) of the Telegraph Act, 1885 along with Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017.

Section 144, CrPC:

The Executive Magistrate of any state or territory may make an order under the provision of the CrPC preventing any assembly of four or more individuals in a certain location. Each participant in such an "unlawful assembly" might be charged with rioting, according to the law. In circumstances of immediate annoyance or suspected threat of an occurrence that might create problems or damage to human life or property, Section 144 is applied, giving the district magistrates of the area the authority to also ban internet connection which was judicially affirmed and held to be legal by the Gujarat High court in 2015.[6] Also, these district magistrates have their own discretion as to apply the act in situations as they see fit in their own "opinion". By exercising this section, the executive first has to ascertain the threat and annoyance, deterrence or injury to any person's life and security, then only it can curtail the speech and expression in any form for restoring public order when such an expression has grave consequences[7] and that repeated use of the section would amount to an abuse of the power given[8] which would threaten the democratic rights. Further it has also been emphasised that the orders under the section must be based on the type of emergency, the amount of territoriality, the type of restriction, the proportionality principle and the length of the restriction, whereas, we see no trends of certainty as regards to the restoration of internet with the biggest example being the shutdown imposed in the state of J&K in 2019 which continued the blackout for 213 days till March 2020 with partial shutdown still imposed by lowering the speed of the internet connectivity only after pressure from human rights activists, advocates and students for basic requirement of imparting education and business operation finally uplifting the total ban after 18 months of disconnect in the region with total 402 internet shutdowns being highest in the country. Also, cases have been there when restrictions have been imposed in states like Rajasthan and Uttar Pradesh for purposes of conduction of competitive exams which finds no danger, no apprehension of injury, and no national security threat turning a blind eye to the fundamental rights of the citizen to access the internet in the name of national security.

IT ACT, 2000

Section 69A of the IT Act, 2000 states:

[6] Gaurav Vyas v. state of Gujarat, 2015 SCC OnLine Guj 6491.
[7] Madhu Limaye v. Sub-Divisional Magistrate, Monghyr (1970) 3 SCC 746.
[8] Acharya Jagdishwaranand Avadhuta v. Commissioner of Police (1983) 4 SCC 52.

69A: "Power to issue directions for blocking for public access of any information through any computer resource. -

(1) Where the Central Government or any of its officer specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, 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 above, it may subject to the provisions of sub-section (2) for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine."

This act, therefore empowers the Central Government to "direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource".[9] This clause gives the government the authority to order the blocking of online resources by intermediaries and organisations that store or transmit data on behalf of others, a category that encompasses social media platforms and internet service providers equally. Blocking orders may be issued under Section 69A for a variety of reasons, including "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." Further, in Anuradha Bhasin v. Union of India[10], the ambit of the section was revisited by the Hon'ble court which specified its area to be only dealing with shutting down of several websites and not the internet as a whole.

[9] Information Technology Act, 2008, Section 69 A (1).
[10] Anuradha Bhasin v. Union of India, AIR 2020 SC 1308.

Suspension Rules 2017

Following the exponential rise of Internet Shutdown trend since 2012, the Central government for the first time addressed the issue of arbitrary internet shutdowns and empowered the competent authorities, and brough the governance of Internet shutdowns with certain restrictions under the Telegraph Act, which were announced by the Department of Telecoms in the Ministry of Communications, the official branch of the Central Government dealing with the telecommunications business. The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 (Suspension Rules) issued under section 7 of the telegraph Act, 1885. These rules have replaced the old regime of the colonial-law of Section 144 CrPC.[11] These rules explained what a competent authority would be and also emphasized that any order restraining internet access must be done only after providing the reasons for such directions. These rules included the Ministry of Home Affairs and the Secretary to the State Government in-charge of the Home Department in case of the government of India and in the case of a state government respectively. Furthermore, there rules also mandated the inclusion of reasons in the order which is to be passed only after a review of a committee comprising of Cabinet Secretary, and Secretaries of Legal Affairs and Department of Telecommunication in case of central government and Chief Secretary, Secretary Law or Legal Remembrancer In-Charge, Legal Affairs and Secretary to the State Government when constituted by any state government as according to section 5(2) of the Rules. This procedural query was also recently addressed in the parliament after whether the government maintains records for shutdowns or has plans to do so, and if not, what protocol is followed was raised.[12] But the application of the section 5(2) has also suffered from lots of challenges regarding its validity and constitutionality into the legal paradigm with regard to the principles that govern the section. But first, let's find out what the section actually states,

"*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,*

[11] Nayak, N. (2018, October 18). *The Legal Disconnect: An Analysis of India's internet shutdown laws. SSRN.* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3254857 (Accessed 14 February, 2022).
[12] Singh, R. (2022, July 3). Explained: The frequency, reasons, and controversy over internet suspensions by the Government. The Indian Express. Available at: https://indianexpress.com/article/explained/explained-the-frequency-reasons-and-controversy-over-internet-suspensions-by-the-government-8005450/ (Accessed 14 February, 2023).

friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section."

Since this section solely empowered the executives of the state to intervene with telephonic communications, whenever a situation of public emergency arises which has been interpreted in Hukam Chand Shyam Lal v. Union of India and Others[13] where a hotel in Delhi had several phones that were being used to support illegitimate forward trading. On the grounds that "public emergency arises and that the continuing of "satta" at the aforementioned premises through the telephones indicated above is injurious to public interest," the Administrator of Delhi authorised the police to temporarily seize the telephones. These orders were challenged in front of the court which heard the matter and held that the situation did constitute a public emergency and the order was validly exercised under the section. Therefore, the potential of this section must not be overlooked looking at the PUCL[14] judgment, where the petitioner questioned the constitutionality of section 5(2) and additionally pleaded for the section to be "read down to include procedural safeguards to rule out arbitrariness and to prevent indiscriminate telephone tapping."

However, the Court observed that the petitioner did not "seriously challenge" the constitutionality of section 5(2), instead requesting that the Court "lay down necessary safeguards to rule out the arbitrary exercise of power under the Act." As a result, in its final ruling, the Court did not consider it necessary to make a judgment regarding the constitutionality of section 5(2) but held that telephone tapping infringed the fundamental right to privacy, and created safeguards against arbitrariness in the exercise of the state's surveillance powers thereby admitting that the telephone-tapping infringes citizens' right to life under Article 21 and the right to free expression under Article 19(1)(a) but still the government can

[13] Hukam Chand Shyam Lal v. Union of India and Others, 1976 AIR 789.
[14] People's Union for Civil Liberties v. Union of India, AIR 1997 SC 568.

exercise this power given in circumstance found to be reasonable and hence provided the executives with enormous power but the court in order to check the arbitrariness and procedural irregularities laid down safeguards to prevent the abuse of power. These safeguards are what laid the foundations of regulation in internet shutdowns in the country leading to the recent amendment in 2020 which inserted Rule 2A which stated that, *"the suspension order issued by the competent authority under sub-rule (1) shall not be in operation for more than fifteen days." Though it still does not make sense how states like Jammu and Kashmir and West Bengals experience prolonged restrictions even with the presence of this rule*[15].

JUSTIFICATIONS FOR THE SHUTDOWNS: NATIONAL SECURITY

Internet shutdowns are among of the most intrusive and direct kinds of internet censorship. These shutdowns, which are architectural in nature and influence a foundational state in the information society, differ from conventional kinds of censorship like blocking Internet pages or particular content: using the Internet. And to justify these measures, spreading false information, mass mobilisation communal conflict, technical malfunction or safeguarding national security are some of the reasons the state mostly cites.

Democratic nations typically justify Internet shutdowns as a necessary and temporary measure of protection to deal with emergencies, denying their intention to use Internet shutdowns as a general practise to pursue legitimate interests, such as national security, when governments do explain their actual or potential actions, which they frequently do not. Every state and nation is required to safeguard its citizens via the exercise of political, diplomatic, and economic power. This is known as national security. Another essential responsibility of every government is to safeguard the national security of the nation. To safeguard its own security, each nation has its own laws and ordinances. On the Pakistani side of the Line of Control (LOC), Indian Army Special Forces launched surgical attacks in September 2016. In February 2019, the Indian Air Force (IAF) launched an airstrike against a Pakistani training camp in Khyber-Pakhtunkhwa. However, after the suicide bombing on February 14, 2019, J&K was the first in an armed conflict in Kashmir, killing about 40 Indian paramilitaries, mobile internet services were quickly suspended in southern parts of UT, while the high-speed internet in Srinagar was reduced to 2G-level as a precaution to maintain law and order. Using social media

[15] Mukhopadhyay, D. (2020, November 12). *Amendment to the telecom suspension rules offers little protection against arbitrary and prolonged internet shutdowns #keepusonline*. Available at: https://internetfreedom.in/telecom-suspension-rules-amendment-15-day-time-limit/ (Accessed 14 February, 2022).

carried the potential of making things awkward. Social media users released a footage of a suicide bomber driving into a CRPF convoy with explosives on a highway in the Pulwama area. Officials in charge of intelligence were concerned that the circulation of videos would inspire anti-national elements and lead to issues. Various terrorist groups used the internet to connect with their followers and find new recruits.[16]

Evolution of the concept of national Security.

After World War II, the United States of America is where the notion of national security was primarily created. The older perspective described national security as the need to preserve the existence of the nation-state by the use of economic, military, and political power as well as the use of diplomacy. A nation must have economic security, energy security, environmental security, etc. in order to have national security. However, the meaning and practical interpretation of the term "Security" have changed conceptually with the advent of globalisation, defining the regions that fall under the jurisdiction of National and Internal Security. The term "security" was expanded to cover food security, energy security, including nuclear security, clean environment, equality before the law, and good governance under the new techno-economic model. The idea of "globalisation" of economies further changed the security aspects by incorporating socially acceptable mitigation of cultural conflicts and concerns of ethnic identity. According to the constitutional framework, nothing of the three lists—the Concurrent List, the State List, or the Union List—specifically mentions the topic of "National Security." The Union Government has been given responsibility for security under Article 352 and the emergency provisions in Part XVIII of the Constitution. However, in constitutional practise, "Security" is a topic in which the States and the Union have a shared interest and are expected to work in concert, despite the fact that it is an overwhelming executive authority of the Union. The duties and obligations of the Union and the States under the cooperative partnership are principally addressed by Articles 256, 355, 356 and 365 as well as other applicable laws. List-I of the Seventh Schedule contains entries relating to the defence of India as well as the command and management of the Union's military forces. Entries 1 and 2 in the List II are for Public Order and Police, respectively. List III covers criminal law, criminal process, and administration of justice as Entries 1, 2, and 11A. The National Security Council is an organisation that was founded in 1998 by the previous prime minister of India

[16] Mir, S. (2020). *J&K internet shutdown based on 'dubious' legal framework: Report*. The Wire. Available at: https://thewire.in/government/jammu-and-kashmir-internet-shutdown-jkccs (Accessed 14 February, 2022).

with the goal of preserving national security and peace. India's top investigative body for political, economic, energy, and strategic security issues is the National Security Council (NSC). Without a doubt, the government, the armed forces, the security services, the bureaucracy, the academic community, and the entire private sector—including the agricultural, industrial, and service sectors—are working together to advance the grand goal of creating the most populous, democratic, pluralistic, and secular state in the world.

The problem of governance facing this nation is to rally all of their resources and steer them toward the lofty objective. The primary danger to Indian national security comes from terrorist actions sponsored by the nation's neighbours. As evidenced by the ongoing cases in Jammu and Kashmir, evil terrorists or wrongdoers who threaten the country's peace can easily shield themselves under the protection of fundamental rights and provisions provided by the constitution. These provisions give states a legal means of restricting access to the digital environment and suspending digital services provided by other States when placing national sovereignty within the context of Internet shutdowns. For instance, social media's recent role in escalating mass atrocities by disseminating violent and hateful content could serve as justification for governments to censor the internet. In this situation, internet shutdowns may be carried out to prevent harm from cyberattacks or may be sparked by the lawful exercise of the right to self-defense against the intrusion of other states.

FREEDOM OF EXPRESSION V. NATIONAL SECURITY

Article 19(1)(a) of the Constitution of India provides an Indian citizen with the right to freedom of speech and expression. And since, the Internet is a medium of expression, it is useful to analyze the link between freedom of speech and sovereignty to comprehend how and to what degree the international legal system can prevent an Internet shutdown. However, in the context of Internet outages, the responsibility of state actors to safeguard and promote the enjoyment of human rights needs to be understood. Even if it would seem that barring access to the digital world is prohibited under the vertical structure of international human rights protection, the reality is more complicated. First, in order to safeguard other interests that might otherwise be eclipsed by the supremacy of freedom of expression, the international human rights framework tolerates speech limits. Second, despite the fact that the Internet is international, governments continue to have the right to exercise sovereignty over their national borders. Since the use of this power involves interfering with human rights, any measures taken must adhere to the principles of legality, necessity, and proportionality. In order to defend general interests like

security, state actors can therefore control the national "Internet switch" through telecommunications infrastructure and online middlemen in their jurisdiction. As a result, when discussing Internet shutdowns, the focus should not only be on how these practises may affect human rights but also on what level of proportionality could ensure a just balance between these various interests, particularly between the right to freedom of expression and other legitimate (or sovereign) interests. In Thappar v. State of Madras,[17] the Supreme Court of India clearly noted that "security of state" does not refer to ordinary breaches of public order, because they do not involve any danger to the State itself. The Constitution (First Amendment) Act of 1951 followed this rule, as preservation of public order became one of the grounds for imposing restrictions on the freedom of speech and expression. Additionally, freedom of speech and expression is guaranteed by Article 19 of the UDHR and Article 19(2) of the ICCPR, even in the case of the internet and social media. Thus, it can be seen that many international agreements recognise the right to freedom of speech and expression as a fundamental one. The UDHR, section 19 states that, “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.” Section 32 adds “The promotion, protection and enjoyment of human rights on the Internet” and another 15 recommendations that cover the rights of those who work in and rely on internet access. It also applies to women, girls, and those heavily impacted by the digital divide. Further, section 19(2) of International Covenant on Civil and Political Rights which India is a signatory to, states that “Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice”.

The indispensable fact regarding press freedom is very well known and could be substantiated by the ranking of the country in Reporters Without Borders’ World Press Index being 150th out of 180 countries in the world.[18] Press freedom is under threat in the country and Internet Shutdowns are only exacerbating them. Indian authorities have detained journalists on fabricated terrorism and sedition accusations and frequently target detractors and independent news organisations, including raiding their offices, amid escalating limitations on media freedom. For posting anything that is critical of the

[17] Thappar v. State of Madras, AIR. 1950 SCR 594.
[18] Editorial team. (2022). India: Media freedom under threat. RSF. Available at: https://rsf.org/en/india-media-freedom-under-threat (Accessed 14 February, 2022).

government, journalists and online critics run the possibility of being prosecuted under the Information Technology Act and IT Rules of 2021. Throughout the world, there has been concerns on how this preventive measure curtails the rights of the press and the media and hence their rights guaranteed under section 19 of the constitution. Further, the government recently has introduced the Telecom Bill, 2022 which is being criticised for undermining Internet's potential. The bill broadens the definition of "telecommunication services," which, depending on how it is applied, could encompass broadcasting services like Tata Sky, email services like Gmail and Yahoo, video communication services like Skype, internet and broadband services like Excitel, internet-based communication services like WhatsApp, Gmail, Zoom, and Microsoft Teams, machine-to-machine services like smart cars, smart TVs, and smartwatches, and over-the-top services like Instagram, Twitter and Snapchat. The open, global, interoperable Internet is significantly impacted by the inclusion of possibly every communication system now in operation, regardless of whether it relies on cable, spectrum, or the Internet. Further, the bill provides exclusive power for the government to issue licenses to the service providers for continuing to provide services as according to clause 3 of the Bill. Moreover, in some circumstances, such as when the government believes it is necessary in the interest of the nation's sovereignty, Clause 24(2) gives the government at the Union and State levels the authority to stop the transmission of messages or to intercept or reveal them. End-to-end encryption systems will have to compromise security in order to meet these demands by giving government access to end-to-end encrypted material through a backdoor or other special access. And as explicitly relating to Internet shutdowns in section 24, the bill gives explicit powers to the state with no safeguards.

Reasonability of Restriction: Important to maintain Public Order

Despite the potential importance of these legal processes, shutting down the Internet is still subject to some legal restrictions. It is difficult to predict how the scope of a given law will be read, and similar issues arise when dealing with legitimate interests that may be liberally construed to further political objectives. These issues are especially important when authoritarian nations are engaged since it might be more challenging to evaluate the openness and accountability of their public systems.

As a result, the political motivations behind Internet shutdowns may be hidden by an unconnected legal justification. Or, as we observe more frequently, states merely take political

action rather than use legal justifications to apply Internet shutdowns.

The restriction must be "in the interests of" public order, according to Article 19(2). A statute "may not be meant to actively protect public order and yet it may have been adopted in the interests of public order," according to the Supreme Court's prior expansive interpretation of the phrase "in the interests of public order." The linkage requirement of Article 19(2), however, was construed more strictly by later judgements. The concepts established by Lohia-I[19] would later serve as a reliable standard for interpreting Article 19(2). The Court determined that for the purposes of Article 19, "any distant or fanciful link" between the limitation and public order is insufficient (2). The limitation "should be one which has a proximate connection or nexus with public order," according to the law. This agreement continued in Rangarajan, where the Court ruled that, “In other words, the expression should be inseparably locked up with the action contemplated like the equivalent of a “spark in a powder leg”. In the case of internet shutdowns, these ideas would still hold true. Therefore, internet can be restricted at the time of threat to sovereignty, public order, morality and decency… etc under Article 19 (2).[20]

Therefore, a shutdown may only be enacted when the government foresees an immediate threat of violence and a violation of the peace, as opposed to circumstances where the foreseen risk is either distant in time or just improbable and hypothetical. For instance, in a 2019 order, the Guwahati High Court rejected the government's argument that the State of Assam was under threat of public disorder due to anticipated protests over the Citizenship Amendment Act and that this threat was sufficient justification for the suspension of mobile internet services. When the State failed to comply with the Court's demand that it provides tangible evidence to support its assertion that it had reason to apprehend violence, the Court ordered the reinstatement of mobile internet services. Under Article 19, reasonableness is a stringent and specific threshold of evaluation. A reasonableness assessment must take into account. "The nature of the right allegedly violated, the underlying aim of the limitation imposed, the magnitude and urgency of the ill-intended to be addressed by such restriction, the disproportion of the imposition, and the existing conditions at the time”[21]. Therefore, the term "reasonableness" relates to the need and appropriateness of the action in light of the nature of the right and the goal that the State is attempting to pursue. Therefore, restrictions must be narrowly tailored[22] to the aim which has

[19] Central Prison v. Ram Manohar Lohia AIR 1960 SC 633.
[20] S. Rangarajan Etc vs P. Jagjivan Ram, 1989 SCR (2) 204.
[21] State of Madras v. V.G. Row AIR 1952 SC 196.
[22] Shreya Singhal v. Union of India (2015) 5 SCC 1.

been sought to be achieved by the state. Therefore, in order to adhere to constitutional standards, shutdowns must not go longer than what is required to keep the public in order. A shutdown that encompasses all forms of speech and behaviour, regardless of whether they involve a violation of public order, is overbroad and unlawful. By using these guidelines, the Court determined that before invoking the Suspension Rules, the government must precisely determine the "stage" of the public emergency. The proportionality of the contested measure may only be determined in light of the severity of the situation. Only "necessary" and "unavoidable" shutdown orders may be issued, that is, when no "less intrusive remedy" is available. In particular, the State must consider the possibility of restricting access to social media websites only, as opposed to the entire internet.

CONCLUSION

It can be difficult to decide whether and when Internet shutdowns could be appropriate. We acknowledge that Internet shutdowns are a very intrusive type of censorship, yet there are circumstances in which these actions can be acceptable. States' justifications must be evaluated through the lens of legality, legitimacy, and proportionality in order to limit the justifications for Internet shutdowns on the grounds that they violate human rights. But without a system for enforcing it, this test is only a formal exercise. It can be challenging to have a nuanced discussion about when and under what circumstances shutdown should occur due to the polarised debate where governments are attempting to control flows of misinformation and hate speech, with legitimate concerns and frustration over the negligence and inability of social media companies to regulate such content on their platforms, and the overwhelming condemnation of Internet shutdowns by advocacy groups and the human rights community. By limiting the space needed to examine whether shutdowns could be proportionate or what domestic procedures might be in place to assess when and what sort of shutdown to impose, for how long, and how such a shutdown would be monitored, the blanket condemnation can be unproductive. Hence, even if the decision to shut down the internet and curtail one’s right to internet is taken away by the state, the decision must have been gone through the tests of Article 19, i.e, it must be, lawful, i.e, this power must have been originated from legislation giving full power to the authorities doing so second, it must be legitimate and reasonable in a way that the reason behind imposing such a ban must be for the national security, of any public emergency and only for restoring the public order of the population concerned. The proliferation of low-cost wars, through terror groups as well as religious and ethnic conflicts, in and around the borders, and the interaction of economic and technological concerns in the process of

globalization further widened the scope of what is referred to as "the global security concerns," which had a qualitative impact on the traditional national security ethos. There is a need for adjustments in security policy, strengthening the intelligence apparatus by stopping the current ad hocism and lack of good planning in regard to both personnel and a limit on parochialism in light of globalization and other conflicts.