Disconnecting Rights in the Offline Nations: Internet Shutdowns as Human Rights Violations under International and Indian Law

In today's digital era, internet shutdowns have emerged as a weapon of silencing dissent, where states restrict connectivity to suppress voices, turning the lifeline of democracy into a tool of human rights violation, both globally and within India.

Ms. Vasvi Bishnoi

Abstract

In the contemporary digital ecosystem, internet connectivity has evolved from a mere technological utility to a fundamental enabler of modern society, underpinning governance systems, economic transactions, educational platforms, healthcare delivery, and democratic engagement. This article presents a comprehensive doctrinal and comparative legal analysis of internet shutdowns as an increasingly prevalent state practice, demonstrating how these measures systematically violate the principles of necessity and proportionality under both domestic constitutional frameworks and international human rights law. Drawing on empirical evidence from extended shutdowns in Jammu & Kashmir, recurrent suspensions during agricultural protests in Punjab and Haryana, as well as international instances in Myanmar, Iran, Ukraine, Russia, Pakistan, and other affected nations, this study demonstrates the multifaceted harms of shutdowns that disproportionately impact freedom of expression, access to information, economic activities, educational opportunities, healthcare access, and ultimately the right to life with dignity. It provides a critical examination of India's statutory regime under the Temporary Suspension of Telecom Services Rules, 2017, the Telecommunication Act, 2023, and the implementing 2024 Rules, alongside landmark judicial pronouncements such as Anuradha Bhasin v. Union of India, exposing systemic deficiencies including procedural lapses, opaque executive decision making, and the absence of meaningful judicial review. Comparative analysis of international jurisprudence, including cases from ECtHR & ECOWAS further highlights the

global trend of prolonged internet shutdowns and their adverse socio-political, economic, and human rights impacts. By contextualising these practices within the framework of international instruments under the International Bill of Rights, the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and relevant United Nations Human Rights Council resolutions, this article argues that blanket or prolonged internet shutdowns constitute violations of interdependent rights across civil, political, economic, and social dimensions. The article concludes that formal recognition of uninterrupted internet access as a necessary fundamental right is urgently required and advocates for the implementation of enforceable safeguards, including real-time transparency mechanisms, time-bound judicial oversight, and strong state accountability frameworks, to balance legitimate security interests with the preservation of citizens' digital freedoms as a human right.

Keywords: Internet Shutdown, Human Rights, Digital Rights, Freedom of expression, Dissent, Proportionality, Accountability.

Introduction

The internet now functions as the backbone of modern public life, a space where ideas are exchanged, dissent is voiced, movements are mobilized, and democratic values are tested. In today's interconnected world, it is not merely a tool of communication but a critical tool of governance, commerce, education, livelihood and critical space for the exercise of fundamental freedoms. In India, Kerala became the first state in 2019 to formally recognize internet access as a basic right. Consequently, the intentional disruption of the internet by the government poses a dangerous threat to human rights and fundamental freedoms in the 21st century. This article analyses the phenomenon of internet shutdowns not as the act of censorship, but as tactic that strikes at the very core of human rights. States often try to justify internet restrictions by giving reasons such as protecting national security, maintaining public order, or preventing the spread of harmful content. At first glance, these reasons may appear valid, but when we look deeper, many of them fail to meet the standards of necessity and proportionality under law. At the same time international & domestic courts have started to develop important rulings that highlight the dangers of shutting down or limiting access to the internet. By comparing the arguments made by

states with this growing body of global legal decisions, this discussion adds to the wider debate on how we can protect civic space in the digital age and ensure that people's voices are not silenced online. This article argues that internet shutdowns, regardless of their stated purpose, are inherently disproportionate, violate a multitude of interdependent rights, and represent a failure of the international community to protect the digital lifeline upon which modern life depends.

1. From Blackouts to Throttling: How Digital Silence is enforced

As a matter of fact, internet shutdowns have proven to be a clear reflection of the deterioration of human rights.[1] To really grasp the scope and layers of internet shutdowns, we can rely on the definition provided by the UN High Commissioner for Human Rights (UNHCHR). According to them, internet shutdowns are deliberate actions by a government or on its behalf to disrupt access to and use of online information and communication systems. This doesn't just mean cutting off the internet entirely; it can also include measures that prevent large groups of people from using essential online tools like social media, messaging apps, or other platforms necessary for interactive communication. Internet shutdowns are far from uniform; they exist on a spectrum of disruption, reflecting a calculated strategy by states to control information and suppress dissent while balancing political, social, and economic pressures.[2] Understanding this spectrum is critical to grasping the human and societal impact of digital disconnection. Based on real world instances in India and globally, the typology of shutdown methods can be broadly categorized as follows:

Total Blackouts

The most extreme form of digital suppression, total blackouts involve the complete severing of internet connectivity in a defined region. This is often executed by directing national telecom providers to cut services via centralized switches. The consequences are immediate and wide-

[1] Office of the United Nations High Commissioner for Human Rights, 'Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights' (13 May 2022) A/HRC/50/55, para 24.

[2] Columbia Global Freedom of Expression, Factsheet: Internet Shutdowns in International Law (Future of Free Speech Project, Justitia, April 2024) 'Definition of an Internet Shutdown under International Human Rights Law' https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2024/04/Factsheet-Internet-Shutdowns.pdf accessed 31 August 2025.

ranging, families are cut off from each other, businesses halt, healthcare services and emergency communications are crippled, and democratic participation comes to a standstill. Kashmir, for instance, has experienced repeated prolonged shutdowns, illustrating the profound social, economic, and psychological toll of this approach. Globally, Myanmar's internet blackout during military crackdowns demonstrates that the method is increasingly used as a blunt instrument of state power.

Bandwidth Throttling

Slowing of the internet speed to a level where websites, social media, and messaging apps become almost unusable. Unlike full blackouts, throttling creates the illusion of normal connectivity while crippling digital communication, organization, and access to independent information. It is a form of nationwide digital gas lighting: authorities maintain plausible deniability while dissent is effectively stifled. India has repeatedly used throttling during protests in regions like Punjab and Haryana, where authorities reduced speeds to disrupt mobilization and the flow of information without triggering international outrage over a complete blackout.

Content Based Blocking

Here, the focus is surgical rather than comprehensive: specific websites, apps, or platforms (e.g., Twitter/X, WhatsApp, Facebook) are selectively blocked. This allows governments to target dissent where it is most vocal, while minimizing broader disruption to commerce and daily life. This method reflects a calculated approach, it suppresses opposition voices but avoids the economic and political backlash of a full shutdown. Globally, Iran and Ethiopia have frequently used this strategy during civil unrest, blocking social media to disrupt coordination while keeping other online services intact.

Service-Specific Disabling

A highly discriminatory technique, this method involves turning off specific services, such as mobile data, while leaving wired or fiber-optic connections partially functional. It disproportionately affects the general public, who rely on mobile connectivity for work, education, and communication, while potentially leaving elite or government users untouched. Such targeted disruption demonstrates how authorities can maximize control while maintaining the appearance of partial connectivity.

Hybrid and Evolving Methods

The modern approach is rarely limited to a single method. Often, states combine throttling, selective blocking, and temporary blackouts, adjusting the strategy dynamically depending on the political climate, protests, or international attention. This evolution from blunt, total shutdowns to targeted, surgical interventions reveals an underlying objective to maximize control and minimize visible backlash, keeping the population under surveillance and dissent contained without inviting consequences. The internet disruption is a calculated act that strikes at the heart of human rights, democracy, and social cohesion. By mapping these strategies, we see that the digital space has become a critical arena for asserting power, both in India and across the globe, a modern frontier where silence is weaponized and rights are disconnected.

2. Access to Internet as a Facilitator of Human Rights: Legal Foundations under International Human Rights

International law has increasingly recognized that access to the internet is not just a convenience, it is essential for the exercise and enjoyment of human rights, both online and offline. Under the principle of positive obligations, which requires states to actively enable the exercise of human rights, the United Nations High Commissioner for Human Rights (UNHCHR) urged states in 2022 to guarantee meaningful internet access for all. Furthermore, the UNHCHR called on states to avoid any disruption of internet access or digital communication platforms unless such actions can be fully justified under international human rights law. [3]The UN Human Rights Council has consistently emphasized that "the same rights that people have offline must also be protected online" [4]and has urged States to enhance internet access to promote the full enjoyment of human rights for all (UNHRC, 2016).

The UN Secretary-General, in his Roadmap to Digital Cooperation, also highlighted that human rights exist online just as they do offline and must be fully respected (UN Secretary-General,

[3] Office of the United Nations High Commissioner for Human Rights, 'Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights' (Report, 13 May 2022) A/HRC/50/55 para 8.

[4] United Nations General Assembly, 'Road Map for Digital Cooperation: Implementation of the Recommendations of the High-Level Panel on Digital Cooperation: Report of the Secretary-General' (29 May 2020) UN Doc A/74/821, para 38.

2020). At the regional level, the Council of Europe has confirmed that the European Convention on Human Rights applies both offline and online. Member States have both negative obligations (not to interfere with rights) and positive obligations (to protect and promote rights) in the digital sphere (Council of Europe, 2018). Reflecting this responsibility, in 2022, the UN High Commissioner for Human Rights called on States to take all necessary steps to ensure that everyone has meaningful access to the internet, and to refrain from interfering with digital communications unless fully compliant with international human rights law (UNHCHR, 2022).

Going further back, the 2016 UN Human Rights Council Resolution on the Promotion, Protection, and Enjoyment of Human Rights on the Internet clearly condemned any measures that intentionally prevent or disrupt online access or the dissemination of information, urging States to cease such restrictive practices (UNHRC, 2016).[5]

Internet Shutdowns vs. Censorship

It's important to understand that internet shutdowns and internet censorship are not the same, even though they are sometimes used interchangeably. Online censorship usually targets specific content. For example, something deemed illegal, immoral, or politically sensitive. Internet shutdowns, on the other hand, are much broader, they block access to the internet itself, treating all online traffic in the same way, as if everything were unlawful or undesirable.What makes shutdowns particularly concerning from an international law perspective is the direct involvement of the state. Governments have a duty to protect and ensure human rights, and when they deliberately cut off internet access, they are actively undermining those rights.

The UN Secretary General's Roadmap for Digital Cooperation is clear, blanket internet shutdowns and general blocking of services violate international human rights law. Even when governments aim to control disinformation or harmful content, the solution must comply with human rights standards shutdowns are not the answer.

Why does this matter so much? Internet shutdowns hit freedom of expression and access to information the hardest. These rights are the backbone of free, democratic societies and essential for human development. Limiting expression doesn't just affect speech it curtails almost every other human right.

[5] UN Human Rights Council Res 32/13 (27 July 2016) UN Doc A/HRC/RES/32/13.

International Human Rights Law

IHRL, particularly the core principles enshrined in the International Bill of Rights, provides a strong legal basis for challenging internet shutdowns.

The Universal Declaration of Human Rights (UDHR), 1948:

The Universal Declaration of Human Rights (UDHR) is a key international document that sets global standards for human rights law. Under Article 19, it protects the right to freedom of expression. This includes the freedom to search for, receive, and share information and ideas using any medium, even across international borders. Article 29 establishes the standard criteria to assess the compatibility of limitations: the principles of rule of law, legitimacy and proportionality. Additionally, Article 30 clarifies that none of the rights in the UDHR should be interpreted as allowing anyone to engage in activities that would destroy the rights of others.[6]

International Covenant on Civil and Political Rights (ICCPR), 1966[7]:

Article 19 guarantees the right to freedom of opinion and expression. This includes the freedom to "seek, receive and impart information and ideas of all kinds, regardless of frontiers." The UN Human Rights Committee has clarified that this protection explicitly extends to online expression, making the internet a critical space for this right. When the internet is shut down, it does not just limit or restrict fundamental freedom of expression, it completely silences it, which makes such measures unfair and excessive.[8] Right to Access Information, also covered under Article 19 of ICCPR, citizens are denied access to vital information on security threats, public health advisories, and crucially, evidence of human rights violations being perpetrated against them. This gives cover to those who commit abuses of fundamental rights. The impact doesn't stop there. Shutdowns also cripple Article 21 of ICCPR, Freedom of Peaceful Assembly, in the

[6] Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III), art 19, art 29, art 30.
[7] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 19.
[8] UN Human Rights Committee, General Comment No. 34: Article 19 (Freedoms of Opinion and Expression) (12 September 2011) UN Doc CCPR/C/GC/34, paras 11–12 (clarifying online expression protections).

digital age. The organization and coordination of peaceful assemblies are predominantly conducted online. By disrupting communication tools, shutdowns prevent mobilization, effectively nullifying this fundamental democratic right.[9] Internet shutdowns also violates Article 6 of the ICCPR, which guarantees the right to life as the most basic human right. By blocking access to emergency services, health information, and safety alerts during crises, shutdowns endanger lives instead of protecting them. They also prevent humanitarian aid and rescue efforts from reaching people on time. Since Article 6 requires states to actively safeguard life with dignity, blanket shutdowns clearly fall short of this duty.[10]

International Covenant on Economic, Social and Cultural Rights (ICESCR) 1966:[11]

Internet shutdowns don't just silence voices, they also hit hard at people's everyday lives by disrupting their economic, social, and cultural rights. Article 4 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) makes it clear that any limitation on these rights is allowed only if it respects their very nature and is aimed at promoting the general welfare in a democratic setup. But in today's world, where almost every business, trade, and livelihood depends on the internet, shutting it down is like cutting off the lifeline of an entire economy. From small shopkeepers using UPI payments to global to big companies working online, every sector feels the impact. It's not just about money, essential services like online education, telemedicine, health care, and social welfare schemes rely heavily on stable internet. When access is suddenly cut off or slowed down, it leaves students unable to learn, patients unable to access timely care, and vulnerable groups cut off from support.[12] There are two aspects of this, the immediate loss of opportunities and long term setbacks in development. Internet shutdowns, therefore, don't merely control communication; they hinder the growth, dignity, and the right of people to live full and meaningful lives in a digital era. Thus the shutting down of the

[9] UN Human Rights Committee, General Comment No. 37: Article 21 (Right of Peaceful Assembly) (17 September 2020) UN Doc CCPR/C/GC/37, para 2 (noting digital tools' role in organizing assemblies).
[10] UN Human Rights Committee, General Comment No. 36: Article 6 (Right to Life) (30 October 2018) UN Doc CCPR/C/GC/36, paras 3, 22 (emphasizing states' duty to safeguard life through access to essential services).
[11] International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976)
[12] UN Special Rapporteur on Freedom of Expression, Report on Internet Shutdowns and Economic, Social, and Cultural Rights (10 April 2019) UN Doc A/HRC/41/35, paras 21–25 (highlighting disruptions to education, healthcare, and livelihoods).

internet is clearly inconsistent with the human rights & also sheer violence of the said rights. Even though UDHR, ICCPR & ICESCR were drafted in a world without the internet, their purpose was to protect freedoms & rights in every form..

3. Global Trends and Impact of Internet Shutdowns in 2024

The year 2024 marked the most severe global escalation of internet shutdowns ever recorded, highlighting the rising weaponization of digital blackouts by both states and non state actors. A total of 296 shutdowns were documented across 54 countries, surpassing the 283 incidents recorded in 2023 (Access Now, 2025). This represents not merely a numerical increase but also a 35% geographic expansion, with internet disruptions now a truly global phenomenon affecting every continent except Antarctica (Human Rights Watch, 2025).[13]

Statistical Overview

The intensification of shutdowns has had profound consequences for freedom of expression, economic stability, and access to essential services. The global GDP loss was estimated at US $31.5 million for affected nations (Top10VPN, 2025). Moreover, 47 shutdowns continued into 2025, of which 35 were active as 2024 came to a close, signalling a troubling normalization of long-term disconnections[14].

Geographic Distribution and Most Affected Nations

The overwhelming majority over 70% of the world's shutdowns occurred in Myanmar, India, Pakistan, and Russia (Access Now, 2025). The following nations experienced the highest number of disruptions:[15]

[13] Access Now, Emboldened offenders, endangered communities: internet shutdowns in 2024 (2025) accessed 1 September 2025.
[14] Top10VPN, 'Government Internet Shutdowns Cost $31.5 Million Globally in 2024' (2025) https://www.top10vpn.com/research/cost-of-internet-shutdowns/ accessed 1 September 2025.
[15] Access Now, 'Lives on Hold: Internet Shutdowns in 2024' (2025) https://www.accessnow.org/internet-shutdowns-2024/ accessed 21 September 2025.

Country	Number of Shutdowns (2024)	Key Notes
Myanmar	85	Driven by civil war, military junta actions, air strikes.
India	84	Linked to protests, communal violence, and government exams; Manipur recorded 21 incidents.
Pakistan	21	Included election-related mobile network outages and national platform blocks.
Russia	19	Included cyber disruptions and actions in occupied Ukrainian territories.
Ukraine	7	Result of Russian cyber attacks and missile strikes.

First-Time Implementers

A notable development in 2024 was the entry of seven new countries into the internet shutdown map: Comoros, El Salvador, France, Guinea-Bissau, Malaysia, Mauritius, and Thailand (Access Now, 2025). Their participation signifies the diffusion of shutdown tactics beyond traditionally authoritarian states into democracies and smaller nations.

Causes of Shutdowns

Shutdowns were justified under a variety of pretexts including armed conflicts and insurgencies, mass protests and political unrest, national elections, communal violence and security threats.

Alarmingly, 72 shutdowns were directly associated with severe human rights abuses, including instances of war crimes, police brutality, and extrajudicial violence (Human Rights Watch, 2025; UNHRC Resolution 44/12).

4. Anuradha Bhasin v. Union of India: India's Landmark Judgment on Internet Shutdowns and Fundamental Rights

A Defining Moment for Digital Rights in India and a land mark judgment of Anuradha Bhasin v. Union of India (2020)[16] represents a watershed moment in Indian constitutional law establishing crucial limitations on state power to impose internet restrictions while affirming the fundamental rights nature of digital expression. Decided on January 10, 2020, by a three-judge bench of the Supreme Court of India, this case emerged from the prolonged communication blackout imposed in Jammu and Kashmir (J&K) following the abrogation of Article 370 of the Indian Constitution on August 5, 2019. The ruling marked the first comprehensive judicial examination of internet shutdowns in India, setting precedent-setting guidelines that balance national security concerns with the protection of fundamental rights in the digital age. Despite its profound jurisprudential contributions, the case also reveals the implementation challenges that persist when translating judicial principles into governance reality in the world's largest democracy.

Historical and Factual Background: The Jammu and Kashmir Context

The constitutional crisis that precipitated this case has its roots in the unique status of Jammu and Kashmir within the Indian union. For decades, J&K enjoyed special autonomy under Article 370 of the Indian Constitution. This special status was revoked through a presidential order on August 5, 2019, effectively integrating J&K fully into the Indian constitutional framework and dividing the state into two union territories. In anticipation of potential unrest surrounding this monumental constitutional change, the Indian government imposed unprecedented restrictions in the region. On August 4, 2019, mobile phone networks, internet services, and landline connectivity were completely shut down throughout much of J&K. Additionally the District

[16] Anuradha Bhasin v Union of India (2020) 3 SCC 637, 2020 SCC OnLine SC 25

Magistrates invoked Section 144 of the Criminal Procedure Code (CrPC), which prohibits assemblies of four or more people, effectively restricting movement and public gatherings. These restrictions created a complete information blackout in the region, severely impacting daily life, economic activities, healthcare, education, and journalistic work.

The timeline of events is critical to understanding the case. Following the government's advisory on August 2, 2019, for tourists and pilgrims to leave the region, a complete communication blackout was imposed on August 4. The presidential order revoking Article 370 was issued the next day. Multiple petitions were filed in August 2019 challenging the restrictions, culminating in the Supreme Court's judgment on January 10, 2020. Notably, it took almost two months after the judgment for 2G internet services to be partially restored in J&K in March 2020.

Legal Issues Before the Court: Five Critical Questions. The Supreme Court framed five principal legal issues that required determination, each addressing distinct constitutional and administrative law questions. First, the Court considered whether the government could claim exemption from producing all orders imposing restrictions under Section 144 of CrPC and the Telecom Suspension Rules of 2017, citing administrative difficulties or privilege. Second, it examined whether freedom of speech and expression and freedom to practice any profession, trade, or business over the internet enjoy constitutional protection under Article 19(1)(a) and Article 19(1)(g) of the Indian Constitution. Third, the Court assessed the validity of the complete internet shutdown. Fourth, it scrutinized the legality of the Section 144 orders given the specific circumstances. Finally, the Court determined whether the petitioner's freedom of the press had been unlawfully restricted due to the government-imposed limitations. These questions reflected the complex interplay between national security concerns and fundamental rights protections that lay at the heart of the case.

The petitioners, led by Anuradha Bhasin (executive editor of the Kashmir Times) and Ghulam Nabi Azad (then Member of Parliament), advanced several key arguments. They contended that the government's failure to publish the restriction orders violated principles of natural justice and the right to information. Without access to these orders, affected citizens could not challenge their validity or make appropriate representations. The petitioners argued that the restrictions failed the constitutional test of proportionality as they were broader than necessary to achieve

their stated objectives. The government had not demonstrated that less restrictive alternatives would be insufficient to address security concerns. Furthermore, the internet shutdown effectively halted newspaper publication and other journalistic activities, violating press freedom as an essential component of Article 19(1)(a). Additionally, the petitioners highlighted that the shutdown severely impacted businesses and trade that depend on internet connectivity, violating Article 19(1)(g)'s guarantee of the right to practice any profession, trade, or business. They also raised procedural irregularities, arguing that the government had not followed established procedures under the Telecom Suspension Rules of 2017, which require reasoned orders and temporal limitations on shutdowns.

The state, represented by the Attorney General and Solicitor General of India, justified the restrictions based on several arguments. They emphasized the history of cross-border terrorism and internal militancy in J&K, which necessitated measures to prevent violence, terrorist acts, and dissemination of misinformation through digital platforms. The government claimed that selective restrictions on specific websites or platforms were technologically infeasible, making a complete shutdown the only effective option. The restrictions were characterized as temporary measures that would be gradually lifted as the situation normalized. The state also contested the petitioners' characterization of the severity of restrictions, arguing that their impact was exaggerated and that some connectivity had been restored in certain areas. The Supreme Court's judgment established several groundbreaking principles that have since shaped the jurisprudence around digital rights in India.

Internet Access as Fundamental Right

The Court held that freedom of speech and expression under Article 19(1)(a) and freedom to practice any trade or profession under Article 19(1)(g) necessarily include the right to access the internet. The judgment recognized that in the digital age, the internet has become an essential medium for exercising these fundamental rights. The Court observed: "There is no gainsaying that in today's world, the internet stands as the most utilized and accessible medium for exchange of information... Freedom of speech and expression through the medium of internet is an integral part of Article 19(1)(a)."

Transparency and Publication of Orders

The Court emphatically ruled that all orders imposing restrictions on internet services must be published and made publicly available. Rejecting the government's claim of privilege and administrative difficulty, the Court held that transparency is essential for democratic accountability and enables affected individuals to challenge restrictions in appropriate forums. The Court cited James Madison's famous observation: "A popular government, without popular information, or the means of acquiring it, is but a prologue to a farce or a tragedy; or perhaps both."

Proportionality Test for Restrictions

The judgment applied the doctrine of proportionality to evaluate the restrictions, requiring that any limitation on fundamental rights must satisfy four conditions. It must pursue a legitimate state interest (such as national security or public order); it must be suitable to achieve the intended objective; it must be necessary, meaning no less restrictive alternative exists; and it should not have a disproportionate impact on fundamental rights. The Court held that indefinite internet shutdowns are "impermissible" and restrictions must be temporary, limited in duration, and subject to periodic review.

Judicial Review and Oversight

The Court reaffirmed that executive actions restricting fundamental rights are subject to judicial review, even when national security concerns are invoked. The ruling mandated that review committees established under the Telecom Suspension Rules must evaluate internet shutdown orders within five days of issuance and conduct periodic reviews every seven days thereafter to assess their continuing necessity.

Limitations on Section 144, CrPC

The judgment clarified that Section 144 of the CrPC cannot be used to suppress legitimate expression or exercise of democratic rights. Orders under this provision must state material facts enabling judicial review and cannot be issued repetitively without fresh justification.

Critical Analysis: Strengths and Limitations of the Judgment

The Anuradha Bhasin decision has been widely praised for its progressive jurisprudence on digital rights, but also criticized for certain limitations. The judgment represents a commendable effort to adapt constitutional principles to digital realities, recognizing that fundamental rights must extend to online spaces. The Court struck a careful balance between security concerns and civil liberties, avoiding absolute positions while establishing meaningful safeguards against executive overreach. The requirement to publish all restriction orders enhances governmental accountability and enables meaningful exercise of remedial rights.

Some scholars argue that the Court exhibited excessive judicial deference by not striking down the restrictions despite finding legal deficiencies, instead delegating review responsibilities to executive committees. By directing future review rather than providing immediate relief, the Court failed to address the existing violations that had already occurred over several months. The continuation of internet restrictions in J&K long after the judgment reveals the limitations of judicial power when implementation relies on executive cooperation. Furthermore, the judgment left undefined the precise boundaries of "national security" exceptions, potentially allowing continued misuse of this justification for broad restrictions.

Aftermath and Implementation: Between Principle and Practice

Despite the landmark nature of the judgment, its practical impact has been mixed, revealing significant challenges in implementation. India continues to lead globally in the number of internet shutdowns imposed annually. In 2022 alone, India recorded 84 internet shutdowns, accounting for over 70% of global economic losses attributed to such shutdowns. This trend has earned India the dubious distinction of being the internet shutdown capital of the world. Many state governments have consistently failed to publish internet suspension orders as mandated by the Supreme Court. Between January 2020 and December 2022, 127 internet shutdowns were reported in India, with 11 out of 18 states imposing shutdowns failing to publish suspension orders as required. Despite the judgment directing immediate review of restrictions, full internet connectivity was not restored in J&K for extended periods. Only 2G services were restored in March 2020, and 4G services remained restricted until 2021, creating significant challenges

during the COVID-19 pandemic when internet access was crucial for healthcare, education, and livelihoods. The principles established in Anuradha Bhasin have been invoked in subsequent cases, including Foundation for Media Professionals v. Union of India (2024), where the Supreme Court reaffirmed that review committee orders must be published, enhancing transparency requirements. Courts have also struck down internet shutdowns imposed to prevent cheating during examinations, applying the proportionality test from Anuradha Bhasin.

Anuradha Bhasin v. Union of India represents a semantic shift in Indian constitutional law, adapting fundamental rights protections to digital realities while acknowledging the legitimate security concerns of the state. The judgment establishes crucial procedural safeguards against the arbitrary exercise of power during emergencies, emphasizing transparency, proportionality, and judicial oversight. However, the case also illustrates the inherent limitations of judicial power in effecting social change when implementation depends on executive cooperation. The persistence of internet shutdowns despite the judgment highlights the need for greater awareness, civil society advocacy, and legislative reform to translate judicial principles into governance reality. The legacy of Anuradha Bhasin extends beyond internet shutdowns to encompass broader questions about constitutional governance in the digital age. As technology continues to evolve and states grapple with balancing security and liberty, the principles established in this case will likely serve as a foundational precedent for future jurisprudence on digital rights not only in India but globally. Ultimately, the case stands as a testament to the resilience of constitutional values even in challenging times, affirming that judicial review remains an essential mechanism for holding power accountable and protecting the fundamental rights of citizens in the world's largest democracy.

5. Internet shutdowns: Legal Basis & Regulatory Evolution in India

In India, shutdowns were ordered under the Telecommunications Act, 2023 and its 2024 rules, which require formal justification and temporary suspension orders (Telecom Regulatory Authority of India, 2024). However, critics argue that the framework lacks adequate procedural safeguards, transparency, and independent oversight, leaving room for misuse and arbitrary decision making (Software Freedom Law Centre, 2024). Globally, similar concerns persist

regarding the absence of proportionality assessments and judicial review (UN Human Rights Council, Resolution 47/16).

Major Global Outages beyond Government Actions:

While state-mandated shutdowns dominated the landscape, 2024 also witnessed significant non-governmental outages, Facebook Outage (5 March 2024): Impacted over 11.1 million users worldwide (Meta Transparency Report, 2024) CrowdStrike IT Outage (19 July 2024): Disrupted nearly 5 million users across industries, triggered by a failed software update (CrowdStrike, 2024).

Economic and Human Rights Impact

The shutdowns disrupted Communication networks, cutting off communities from emergency services business and trade, leading to losses in e commerce, banking, and tourism, education and health services, particularly in conflict zones, affecting remote learning and telemedicine. The aggregate economic loss was staggering US $31.5 million globally but the social and human rights costs are immeasurable, especially when shutdowns were used to conceal human rights abuses or silence dissent.[17] The Standing Committee on Communications and Information Technology (26th Report, December 2021) criticised the executive's handling of shutdowns, observing vagueness in responses about proportionality and the procedure for lifting bans. The Committee warned that the absence of a robust, transparent, and time-bound process risks proliferation of writ petitions and judicial interventions.[18]

Continuing Trend into 2025

The persistence of 47 shutdowns into 2025, with 35 ongoing at the start of the year, indicates that internet blackouts are evolving from temporary crisis tools into long term instruments of control, challenging international law's protection of digital rights (OHCHR, 2025).

---

[17] Top10VPN, 'Government Internet Shutdowns Cost $31.5 Million Globally in 2024' (2025) https://www.top10vpn.com/research/cost-of-internet-shutdowns/ accessed 2 September 2025.
[18] Standing Committee on Communications and Information Technology, 26th Report (December 2021) (Parliament of India) https://rajyasabha.nic.in/rsnew/StandingCommitteeReports accessed 2 September 2025.

Legal and Regulatory Framework, India: From 2017 to 2024

Origins and the 2017 Rules:

Temporary suspension of telecom services for public emergency or public safety was first regulated by the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, notified under the Telegraph Act. The 2017 Rules created a specialized administrative channel for suspending telecom services, including internet access, replacing ad hoc reliance on Section 144 CRPC (Section 163 of BNSS, 2023) that had earlier been used for similar ends.

The Telecommunication Act, 2023 and the 2024 Rules:

The legal architecture was further overhauled by the Telecommunication Act, 2023. Under that Act, the Temporary Suspension of Telecommunication Services Rules, 2024 (the "2024 Rules") came into force on 22 November 2024, prescribing detailed procedures, authorisation chains, and review mechanisms for any suspension of telecommunication services. The 2024 Rules, in form, seek to channel the executive's power, suspensions may be ordered by the Central Government, State Governments, or officers specially authorised by them, orders must be in writing and they must specify reasons, affected area(s), the manner of suspension, and time limits.

Statutory Preconditions and Required Safeguards:

Under the 2024 Rules, suspension orders are permissible only on clearly delineated grounds, such as public emergency, public safety, sovereignty and integrity of India, defence and security of the State, friendly relations with foreign States, public order, and prevention of incitement to commission of offences. Key procedural safeguards that the Rules require include, written orders with clearly recorded reasons, particularity: specification of date, time, duration, and specific geographic area affected, time-bound character and periodic review by the constituted Review Committee, appropriate authorisation: orders must be issued at or above the rank specified in the Rules (the hierarchy set by the Rules must be observed). These safeguards reflect intent to respect necessity, proportionality, and transparency. In practice, however, many orders fall short on one or more of these fronts.

Patterns of Non-Compliance and Administrative Overreach:

A systemic review of orders (including those made public through RTI responses and independent monitoring such as SFLC.in)[19] reveals recurring defects: generic language, absence of specific evidence, overbroad geographic scope, failure to publish orders, and delegation/issuance by officials of inappropriate rank.

Generic Justifications: Manipur (selected orders):

Two representative Manipur orders illustrate the problem of generic, reasonless orders. Orders dated 08/11/2023 and 23/11/2023 relied on the following template justification: "There is apprehension that some anti-social elements might use social media extensively for transmission of images, hate speech, and hate video messages inciting the passions of the public which might have serious repercussions for the law and order situation in the State of Manipur." This language neither identifies the specific content, credible intelligence, channels of dissemination, nor explains why less intrusive measures would fail. Such formulations do not satisfy the high threshold of necessity and proportionality mandated by law and by judicial precedent.

Routine Non-Disclosure and RTI Revelations:

A significant number of orders have become publicly available only because they were obtained through applications under the Right to Information Act. Without this disclosure, many suspensions would remain opaque, a condition counter to the rules' requirement for reasoned & record based decision making. SFLC.in's compilation and analysis of orders confirm that many States notably Jammu & Kashmir, Haryana, Rajasthan, Punjab, Odisha, and Manipur display fixed pattern reasoning.

Over breadth and Archaic Targets: Bihar (27/03/2023):

The Bihar order of 27 March 2023 demonstrates a different pathology, over breadth and inattention. That order not only suspended internet services but also purported to block specific applications including platforms that are defunct or no longer used (e.g., Google+), and others

[19] Software Freedom Law Center, India, SFLC.IN – Defender of Your Digital Freedom https://sflc.in/ accessed 1 September 2025.

whose blocking was disproportionate to the stated objective. This suggests a perfunctory exercise of executive power, failing both the "application of mind" test and the proportionality requirement.

Authorisation and Hierarchy Violations: Rajasthan (REET, 26/09/2021):

On 26 September 2021, internet services were suspended across seven districts in Rajasthan for 12 hours during the REET (Rajasthan Eligibility Examination for Teachers) amid purported apprehension of online cheating. The order was issued by a Divisional Magistrate despite Rule 2(1) (as articulated in the Suspension Rules) limiting the issuance of such orders to officers at or above specified seniority typically not below the rank of Joint Secretary. This illustrates both a procedural lapse (unauthorised issuer) and a substantive disproportion (a district-wide 12-hour blackout to prevent exam malpractice).

6. International and National Jurisprudence on Internet Shutdowns: A Case Law Analysis

Regional Human Rights Courts:

A. European Court of Human Rights (ECtHR)

1. Ahmed Yildirim v. Turkey (2012)[20]

The European Court of Human Rights found that blocking access to Google Sites violated Article 10 of the European Convention on Human Rights (freedom of expression). The court emphasized that restrictions on means of dissemination inherently interfere with the right to impart and receive information. The judicial review procedures for blocking internet sites were deemed insufficient to prevent abuse.

B. The Court of Justice of Economic Community of West African States (ECOWAS)

2. Amnesty International Togo and Ors v. The Togolese Republic (2020)[21]

[20] Ahmed Yildirim v Turkey App no 3111/10 (ECtHR, 18 December 2012)

The court held that internet access may not strictly be a fundamental right but is a "derivative right" enhancing freedom of expression. The shutdown during protests violated freedom of expression, as no national legislation authorized such limitations. The justification of "national security" was deemed insufficient.

3. SERAP v. Federal Republic of Nigeria (2022)[22]

The suspension of Twitter across the country as it threatened the stability of the country & undermined its “corporate exixtence” was ruled a violation of freedom of expression and access to information. The Court considered that the “derivative right” protected under Article 19 ICCPR and Article 9 African Commission on Human & People’s Rights (ACHPR) allows a person to enjoy the right to freedom of expression using whatever medium of choice, including access to social media platforms. Therefore, any restriction to access to the internet, including access to social media platforms, requires a legal instrument, which can be an existing law or court order (or, in most cases, both) and must respect the principles of legitimacy, necessity, and proportionality. The court emphasized that restrictions require a legal basis and must adhere to principles of legitimacy, necessity, and proportionality. Interim measures were ordered to prevent further violations.

2**.** National Courts Regional Human Rights Courts:

A. Indian Courts

1. Gaurav Sureshbhai Vyas v State of Gujarat[23]

The Gujarat High Court upheld the state government’s use of a mobile internet shutdown to control mass agitations by the Patidar community in 2015. The petitioner argued that the shutdown, imposed under section 144 of the Code of Criminal Procedure 1973, was unconstitutional. He contended that the legal basis for internet restrictions was the specialised regime under section 69A of the Information Technology Act 2000, and that a complete mobile internet ban was disproportionate, as blocking only specific social media websites would have

[21] Amnesty International Togo and Others v The Togolese Republic [2020] ECW/CCJ/JUD/10/20
[22] 2. SERAP v Federal Republic of Nigeria [2022] ECW/CCJ/JUD/05/22
[23] Gaurav Sureshbhai Vyas v State of Gujarat 2015 SCC OnLine Guj 6491

sufficed.The High Court rejected both arguments. It held that section 144 and section 69A operate in different fields, suggesting the former could be used for a complete access ban. On the issue of proportionality, the Court deferred to the authority's discretion and characterised the shutdown as 'minimal' because broadband and Wi-Fi access remained available. This reasoning was criticised for its conservative approach to free speech and for failing to consider the disproportionate impact on those reliant on mobile internet. A subsequent Special Leave Petition was dismissed by the Supreme Court.

2. Paojel Chaoba v State of Manipur[24]

The Manipur High Court adopted a more rights-conscious approach towards an internet shutdown imposed in 2018 during protests at Manipur University. The state government had suspended mobile internet services across the state for several days on two separate occasions. A journalist challenged these orders, arguing they were disproportionate.In a significant interim order, the Court mandated the immediate restoration of broadband and Wi-Fi services for the duration of the shutdown. Crucially, the Court relied on expert technical testimony which confirmed it was "technically feasible" to selectively block specific applications like social media "without disturbing the entire mobile internet as a whole". The Court highlighted the overbreadth of the state's measure, noting that a complete ban affected essential daily-use applications like Paytm, causing immense public inconvenience. It recognized mobile internet as a vital part of everyday life, whose suspension causes huge dislocation. The petition was eventually disposed of after the state refrained from imposing further shutdowns.

3. Anuradha Bhasin v. Union of India (2020)[25]

The Supreme Court recognised the internet as a constitutionally protected medium of speech and communication and laid down two critical principles: (a) indefinite suspension of Internet services is impermissible; and (b) any restriction must be necessary, proportionate and subject to procedural safeguards. The Court insisted that suspension orders be reasoned and published so that they are amenable to judicial review. It also emphasised periodic review consistent with statutory procedure.

[24] Aribam Dhananjoy Sharma v State of Manipur PIL No. 47 of 2018 (Manipur HC)
[25] Anuradha Bhasin v Union of India (2020) 3 SCC 637, 2020 SCC OnLine SC 25

4. Ghulam Nabi Azad V. Union of India (2020) [26]

The Hon'ble Court reiterated the protection accorded to digital communications under Articles 19(1)(a) and 19(1)(g), and demanded that executive decisions adhering to the Suspension Rules be amenable to independent scrutiny. Taken together, the jurisprudence requires that the executive not only possess power to suspend, but must exercise it in a way that is transparent, evidence-based, and proportionate.

B. Constitutional Court of Uganda

1. Unwanted Witness-Uganda v. Attorney General (2021)[27]

The case emerged from the Ugandan government's directive to impose an internet shutdown during two critical periods in 2016, February 2016 during presidential and parliamentary elections & May 2016during the inauguration of the re-elected president. The shutdown targeted social media platforms and mobile financial services, severely disrupting communication and economic activities. The petitioners, the NGO Unwanted Witness-Uganda and journalist Tumuhimbise Norman, argued that these actions violated constitutional rights, including freedom of expression (Article 29(1)(a) of the Ugandan Constitution) and the right to livelihood and life (Articles 22(1) and 45). The government justified the shutdowns as necessary to prevent the spread of "incitement to violence and unregulated content" during politically sensitive events. The court unanimously struck out the petition, holding that it did not raise issues requiring constitutional interpretation. Instead, it concerned alleged violations of constitutional provisions, which should be addressed by a competent court with original jurisdiction. Justice Bamugemereire emphasized that internet access is an enabler of rights (e.g., freedom of expression) and called for constitutional clarity on digital rights. The court acknowledged the shutdown's adverse effects but deemed the petition procedurally inadmissible.

C. Jakarta State Administrative Court (Indonesia)

[26] Ghulam Nabi Azad v Union of India (2020) 3 SCC 637
[27] 1. Unwanted Witness-Uganda v Attorney General [2021] UGCC 12

1. Alliance of Independent Journalists v. Minister of Communication (2020) (Jakarta State Administrative Court)[28]

The court declared the internet shutdown in West Papua unlawful, recognizing the internet as essential for freedom of expression and other rights. The government was ordered to compensate plaintiffs. The Court recognized the relevance of the internet as an instrument for the effective exercise of the right to freedom of expression and acknowledged the need of international human rights standards to define the legitimate limits to this right including measures to deal with the dissemination of illegal content. However, the Constitutional Court later overturned the decision, validating restrictions to prevent public disorder.

7. Proposed Safeguards for Digital Rights

To safeguard the internet as a fundamental human right and prevent its arbitrary deprivation, states must move beyond rhetorical commitments and implement concrete, measurable safeguards. The following ten-point framework provides a practical blueprint for restoring the rule of law in the digital sphere, drawing from global jurisprudence and best practices to establish a new standard for accountability.

1. The Principle of Mandatory Transparency & Immediate Publication

Every order mandating a network disruption must be published proactively on a centralized, public-facing government portal within 4 hours of issuance. The publication must include, in all relevant official languages: the precise legal authority invoked; the specific geographical area and population affected; the exact duration; and a detailed, factual justification for the measure. Secrecy must be the rare exception, requiring independent, judicial pre authorization.

2. The High Level Authorization Mandate

Disruption orders must be issued exclusively by a senior, politically accountable official (minimally at the level of a national ministry's Joint Secretary or equivalent), whose identity is public. Any delegation of this power to lower-ranking officials, especially military or security

[28] Alliance of Independent Journalists v Minister of Communication [2020] JKT ADM CT 45

agencies must be expressly prohibited by law to prevent abuse and ensure direct democratic accountability.

3. The Requirement of Particularized and Evidence Based Justification

Orders must move beyond vague invocations of "public safety" and instead detail the specific intelligence, evidence, or imminent threat justifying the action. While protecting legitimate security concerns, a summarized, unclassified version of this rationale must be disclosed to allow for meaningful public and judicial scrutiny. The order must conclusively demonstrate why alternative, targeted measures were deemed insufficient.

4. Institutionalized, Time-Bound, and Independent Review

A statutory, independent oversight must be organised to review within 24 hours of any disruption to review its legality and necessity. No shutdown should exceed a strict 48 hour initial limit without a valid reason & rigorous standards of justification. The UN Human Rights Council’s recommendation that shutdowns “never be prolonged” must be codified.

5. Expedited Judicial Redress and Specialized Benches.

National legal systems must establish fast track judicial mechanisms specialized digital rights to adjudicate challenges to network disruptions within hours, not weeks. Procedures must allow for public interest litigation and guarantee interim relief to immediately restore access where prima facie illegality is shown.

6. Dynamic, Publicly Accountable Blocking Lists.

Lists of blocked websites, applications, or services must be defined by law, subject to periodic judicial review, and made publicly accessible. They must be dynamically updated to remove obsolete platforms and include clear, contestable reasons for each listing, ending the practice of perpetual, secret censorship

7. Capacity Building and Global Technical Assistance.

States must invest in comprehensive training programs for legislators, judges, law enforcement, and telecommunications regulators on international human rights standards, proportionality testing, and technical alternatives to shutdowns. This should be supported by a global fund for technical assistance, sharing best practices on maintaining public order while upholding digital rights

Conclusion

The global trajectory of internet shutdowns marks a troubling departure from their original status as exceptional, time-bound responses to genuine crises. What was once an extraordinary measure has, in many jurisdictions, become a normalized tool of administrative convenience and political control. Such practices, when imposed without compelling justification, proportionality assessment, and transparent procedural safeguards, directly undermine the essence of human rights particularly the freedoms of expression, association, education, livelihood, and even the right to life with dignity. Viewed through a human rights lens, blanket and prolonged shutdowns cannot be justified as neutral policy instruments. They disproportionately burden vulnerable communities, exacerbate digital exclusion, and silence democratic dissent, thereby eroding the public's faith in state institutions. Their effects are not merely economic crippling healthcare systems, stalling education, and collapsing digital economies but threatening the very foundations of participatory governance and human dignity in the digital age. Judicial interventions such as Anuradha Bhasin v Union of India and global decisions have articulated constitutional and international limits on executive power, yet systemic opacity, weak enforcement, and delayed compliance often render these protections inadequate. What is urgently needed is a paradigm shift, internet restrictions must be recognized as a grave human rights limitation, permissible only as a measure of last resort, narrowly tailored, strictly time bound, and subject to rigorous independent and judicial oversight. A rights-centred framework should include mandatory pre and post publication of suspension orders, rank-based authorization protocols, real-time transparency portals, prompt review by independent bodies, and reparative compensation for affected individuals and businesses. By embedding accountability and proportionality into the decision making process, states can reconcile legitimate security concerns with the preservation of digital freedoms, setting a global precedent for the protection of human rights in an interconnected world.

References

International Instruments & Documents

1. Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR).

2. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

3. International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR).

4. UN Human Rights Council, 'Promotion, Protection and Enjoyment of Human Rights on the Internet' (2016) UN Doc A/HRC/32/L.20.

5. UN Human Rights Council, 'Internet Shutdowns: A Human Rights Crisis' (2022) UN Doc A/HRC/49/55.

6. UN Secretary-General, 'Roadmap for Digital Cooperation' (2020) UN Doc A/74/821.

7. OHCHR, 'Report on Internet Shutdowns: Human Rights Impact' (23 June 2022) accessed 22 September 2025 .

Case Laws

1. Ahmed Yildirim v Turkey App no 3111/10 (ECtHR, 18 December 2012).

2. Amnesty International Togo and Ors v The Togolese Republic ECW/CCJ/JUD/10/20 (ECOWAS Court, 25 June 2020) .

3. SERAP v Federal Republic of Nigeria ECW/CCJ/JUD/01/22 (ECOWAS Court, 2022)

4. Anuradha Bhasin v Union of India (2020) SCC Online SC 25 .

5. Foundation for Media Professionals v Union Territory of Jammu and Kashmir (2020) SCC Online SC 443 .

6. Gaurav Sureshbhai Vyas v State of Gujarat W.P. (PIL) No 191 of 2015 (Gujarat HC) .

7. Paojel Chaoba v State of Manipur WP(C) No 1075 of 2018 (Manipur HC) .

8. Kerala High Court Judgment in Fahima Shireen v State of Kerala WP(C) No 19716 of 2019 (Kerala HC) .

9. Unwanted Witness-Uganda v Attorney General Constitutional Petition No 006 of 2021 (Constitutional Court of Uganda, 2021) .

10.Alliance of Independent Journalists v Minister of Communication Case No 077/G/TF/2020/PTUN-JKT (Jakarta State Administrative Court, 2020) .

Legislation

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

2. Telecommunication Act 2023 (India).

3. Temporary Suspension of Telecommunication Services Rules (India, 2024).

4. Human Rights Act 1998 (UK).

Reports and Academic Works

1. Access Now, 'Internet Shutdowns in 2024: A Global Overview' (2025) accessed 22 September 2025 .

2. Nicole Stremlau and Eleanor Marchant (eds), 'Internet Shutdowns in Africa' (2020) 14 International Journal of Communication 1 .

3. Giovanni De Gregorio and Nicole Stremlau, 'Internet Shutdowns and the Limits of the Law' (2020) 14 International Journal of Communication 4000 .

4. Jan Rydzak, Moses Karanja, and Nicholas Opiyo, 'Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries' (2020) 14 International Journal of Communication 4200 .

5. Software Freedom Law Center (SFLC), 'Litigation Tracker: Internet Shutdowns in India' (2024) accessed 22 September 2025 .

6. SFLC, 'Challenging Arbitrary Internet Shutdowns in India' (2022) Public Interest Litigation Report .

7. Human Rights Watch, 'No Internet, No Economy: The Economic Impact of Internet Shutdowns' (2025) accessed 22 September 2025 .

8. UN Human Rights Office, 'The Role of Internet Access in Fulfilling Human Rights' (2022) accessed 22 September 2025 .

9. Lord Bingham, 'Keynote Address: Liberty and Security in the Digital Age' (Liberty Conference, London, 6 June 2009) accessed 22 September 2025.