International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0545
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3435-3441

Global Digital Repression: Internet Shutdowns as Tools to Suppress Dissent and Violate Human Rights in 2025

Avanthiga J[1], Shalini S[2], Anusiyadevi G B[3], Santhiya K[4], Saranya M[5], Dhanush Priyan G B[6]
[1]PG, Government Law College, Tiruchirappalli, Tamil Nadu, India.
[2]B.BA.LLB (Hons), LL.M- Practicing Advocate, Hosur, Tamil Nadu, India.
[3]PG – The Tamilnadu Dr. Ambedkar Law University, (SOEL), Chennai, Tamil Nadu, India.
[4]B.BA.LLB (Hons) - Practicing Advocate, Salem, Tamil Nadu, India.
[5]PG - Government Law College, Tiruchirappalli, Tamil Nadu, India.
[6]B.C.A.LLB (Hons), LL.M (UK) - Advocate
Emails: *avanthij.2001@gmail.com[1], advocateshalinishivabalan@gmail.com[2], anubaskar642002@gmail.com[3], santhiyalawyerbballb@gmail.com[4], mssaranya0702@gmail.com[5], dhanushbaskar2000@gmail.com[6]*

Abstract
In 2025, internet shutdowns are increasingly employed as instruments of digital repression, with 296 recorded instances across 54 countries, representing a 35% rise compared to prior yearsenabling governments to suppress dissent, manipulate the flow of information, and infringe upon civil liberties. This study critically examines the legal, human-rights, and governance challenges posed by such shutdowns at both international and national levels. On the international front, indiscriminate internet restrictions violate rights protected under the International Covenant on Civil and Political Rights (ICCPR), particularly Article 19 concerning freedom of expression, and contravene United Nations resolutions that condemn arbitrary limitations on online access. At the national level, the protection of digital rights is inconsistent: while certain judiciaries have recognized the internet as a medium through which fundamental rights can be exercised, statutory frameworks often lack clarity, procedural safeguards, and transparency. Through an in-depth analysis of the landmark case Anuradha Bhasin v. Union of India (2020), this research illustrates how courts have begun to implement safeguards, including the principles of legality, necessity, proportionality, publication of shutdown orders, and periodic review, while also highlighting gaps in enforcement and compliance. Key issues addressed in this study include the legal standards governing internet suspensions, the effectiveness of judicial and institutional oversight, and the social, economic, and political consequences of prolonged shutdowns. Furthermore, the study explores how international human-rights norms can be incorporated into domestic legislation. By examining comparative legal frameworks, case law, and policy responses, this research proposes a normative approach to strengthen accountability, protect digital rights, and prevent the misuse of internet shutdowns as a tool of repression.

Keywords: *Digital Freedoms; Digital Repression; Human Rights; Internet Shutdowns; Suppression of Dissent.*

1. Introduction
Around the world, access to the internet has become essential for everyday life from education and work to communication, healthcare, and financial services. Yet Internet Shutdowns deliberate disruptions that

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0545
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3435-3441

cut off online communication for certain groups or regions are increasingly being used by governments as a tool to control the flow of information. Governments often claim that such measures are necessary during emergencies, such as preventing violence or stopping the spread of harmful content. One well-known example occurred in Sri Lanka in 2018, when anti-Muslim riots escalated through posts and coordination on Facebook. In that moment, a temporary block on social media was viewed as a way to slow the violence and protect vulnerable communities. However, these cases are rare. In recent years, internet shutdowns have more often been used in ways that are disproportionate and harmful. Instead of solving underlying problems, they tend to hide them, while creating significant disruptions to daily life. When the internet goes dark, students lose access to education, workers cannot perform their jobs, patients struggle to reach healthcare, and financial systems are interrupted. Shutdowns also undermine press freedom, obstruct humanitarian assistance, restrict community organizing, and prevent the documentation of human rights violations. As the use of shutdowns grows worldwide, it becomes increasingly important for the international community to examine their impacts, question their justification, and consider how to protect both public safety and fundamental rights in the digital era. Advances in Cyber Surveillance and Monitoring Technologies have brought about a paradigm shift in how activities and individual can be observed (Erica Harper *et al*, 2024). A network disruption is the intentional, significant disruption of electronic communication within a given area and/or affecting a predetermined group of citizens (Jan Rydzak, 2025). Essentially, Al systems employed by Government to monitor, influence and suppress opposition or dissent as well as respective information and data flows, often with high degrees of efficiency and minimal transparency. These methods of control appear in various forms, ranging from expansive surveillance networks or electoral manipulation to more subtle methods of managing information and spreading propaganda online. Such technologies' impact is profound, affecting individual rights and the critical functioning of democratic societies, all of which are expected to become more technically complicated and nuanced over the next decade (H.Akin Unver, 2024).

1.1 Methodology

This study adopts a qualitative research approach, drawing on comparative case analysis of recent internet shutdowns across multiple regions. Data were collected from policy reports, academic literature, and documented incidents by digital rights organizations. The findings were examined to identify common patterns, impacts, and state justifications. Insights were synthesized to assess broader implications for human rights and global governance [1-4].

2. Causes and Mechanism of Internet Shutdown

2.1 Causes of Internet Shutdown

In 2025, Internet Shutdowns were increasingly rooted in Government's strategic aims to control political narratives and stifle collective action during times of turmoil. Many regimes deploy shutdowns as a defensive measure to retain power amid growing public dissent, anti-Government demonstrations, or opposition movements that thrive on digital platforms. Elections particularly serve as a significant catalyst, as ruling entities seek to curtail online campaigning, hinder real-time exposure of electoral fraud, and diminish the organizational strength of rival factions. Additionally, a major factor is the state's attempt to manage crises like ethnic strife, communal unrest, or separatist disputes, with authorities asserting that shutdowns are essential to limit misinformation or avert escalation. In reality, they frequently silence victims and obscure military or police activities. The global rise of digital authoritarianism has also contributed, as some Governments embrace the concept of "digital sovereignty," promoting state control over internet governance and legitimizing sudden shutdown orders. Furthermore, shutdowns are used to lessen international scrutiny in conflict regions, inhibit access to independent media, and obstruct the documentation of human rights abuses [5-6].

2.2 Mechanism of Internet Shutdown

The Indian Government's authority to suspend

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0545
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3435-3441

telecommunications and Internet services has developed through a complex mix of legal frameworks, delegated rules, and judicial examination. Initially, before the existence of specific telecom suspension regulations, authorities mainly leaned on broadly framed statutory provisions that were not specifically designed for digital communication. The most commonly cited Section 144 of the Code of Criminal Procedure, 1973, mirrored as Section 163 of the Bharatiya Nagarik Suraksha Sanhita, 2023. This section allows executive magistrates to issue urgent orders aimed at preventing imminent threats to public order, safety, or tranquility. Although intended for immediate law enforcement scenarios, this provision began to be used as a justification for disabling Internet access, based on the notion that digital communication could incite unrest, spread misinformation, or facilitate mass mobilization. Its broad discretionary terms conferred substantial authority to the Government, yet it lacked essential procedural safeguards for decisions impacting fundamental rights in today's digital era. Simultaneously, officials also relied on Section 5(2) of the Indian Telegraph Act, 1885, a remnant of colonial governance. This section granted the state control over telegraph and later telecommunications systems during public emergencies or to avert incitement to crime. Despite being technologically outdated, the Telegraph Act provided a legal basis for Internet suspensions for decades, illustrating how outdated legislation struggled to address the challenges posed by modern digital networks. Acknowledging the necessity for a specific regulatory framework, the Union Government enacted the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017. These regulations marked a significant attempt to formalize the process of telecommunications and Internet service suspensions, mandating that any shutdown order be issued or sanctioned by the Union or state Home Secretary, and thereby centralizing authority in senior administrative officials. These limitations were laid bare during the 2019 Internet shutdown in Jammu and Kashmir, which followed the abrogation of Article 370. The Union Government justified the pre-emptive shutdown based on national security and the need to maintain order. This restriction lasted nearly 18 months, becoming one of the longest continuous Internet shutdowns in democratic history, occurring at a time when the COVID-19 pandemic heightened reliance on digital communication. Most importantly, the Court ruled that indefinite shutdowns are unconstitutional, rejecting the practice of implementing open-ended suspension orders without regular review. While the Court did not invalidate the 2017 Rules, it reinterpreted them through a constitutional framework, instituting procedural and substantive limits that had previously been lacking. In response, the Government modified the regulatory framework by introducing the Temporary Suspension of Telecom Services Rules, 2020, which explicitly restricted the duration of any suspension order to 15 days. Although this represented progress in curtailing indefinite shutdowns, it did not satisfactorily address concerns surrounding transparency, proportionality, or independent oversight. A more thorough legal overhaul occurred with the Telecommunications Act, 2023, which abolished the outdated Telegraph Act and aimed to update the regulatory structure overseeing telecom services. Under Section 20(2)(b) of the new Act, the Government retained the authority to suspend telecommunications services during public emergencies or in the interest of public safety, effectively adapting previous powers within a contemporary legislative framework. Following this, the Government enacted the Telecommunications (Temporary Suspension of Services) Rules, 2024, which superseded both the 2017 and 2020 rules. These new regulations align the suspension process with the revised statutory framework. However, despite this formal modernisation, the 2024 Rules have faced criticism for not adequately addressing the foundational issues that have plagued India's shutdown policies. The phrases "public emergency" and "public safety" remain ambiguous, allowing for broad interpretation by executive entities. The review mechanism stays internal rather than independent, diminishing effective oversight. Additionally, the rules do not significantly improve transparency or

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0545
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3435-3441

offer clear ways for citizens to contest suspension orders [7-9].

3. Role of the Government, ISP and Tech Companies

The Government, Internet Service Providers (ISPs), and technology businesses all have various but related duties to protect human rights in the digital age, especially when it comes to privacy, free speech, and access to information.

3.1 Role of the Government Internet Service Providers (ISP) Regarding Human Rights

Internet service providers (ISPs) provide vital infrastructure and services that enable users to access and use the internet, allowing them to profit from the information society while simultaneously delivering valuable public services. ISPs are well-positioned to promote the exercise and protection of human rights and fundamental freedoms. Furthermore, Internet access is gradually becoming a requirement for a fully participatory democracy. ISPs also play an essential role in the interaction between countries that are committed to safeguarding and advancing fundamental human rights and liberties under international law. ISPs offer a wide range of services to their consumers, including access and other information society services (application, content, and/or hosting). These rules recognize that not all ISPs have the same obligations and responsibilities to their users, which can vary depending on the type of services provided and the consumer category served. Access providers provide users with access to the Internet, and hence to a diverse range of information, culture, and languages; they are frequently the initial point of contact and trust. Their position is crucial in enabling and empowering people to reap the benefits of the information age, particularly the ability to seek and exchange information and ideas, as well as create and access knowledge and education. Access providers, particularly those serving home users and families, can be seen as contributing to public service by enabling their clients to benefit from the information society, so improving the exercise and enjoyment of their rights and liberties. Similarly, access providers, particularly host providers, may impose judgments and actions on service accessibility (such as removing, banning, or filtering content), so compromising rights and freedoms. ISPs access to content and traffic data demonstrates their critical role in safeguarding user's rights and freedoms. ISPs should not be forced to actively monitor content and traffic data; but, in some cases defined by law and according to specific orders, an ISP may be required to help in the surveillance of content or data or to reveal information about a user to third parties. Such events may have an impact on free expression and the right to privacy.

3.2 Role of Tech Companies

Tech businesses (including social media platforms, software developers, and hardware manufacturers) have a significant impact on human rights due to their dominant position in the digital sphere.

Respect Human Rights Due Diligence: Businesses should proactively identify, prevent, and mitigate harmful human rights effects of their business models, products, and services (for example, data collection, AI algorithm use, content moderation).

Privacy by Design: They must include privacy and data security principles into the design and default settings of their products and services. The obligations of all three parties are intertwined, needing cooperation and adherence to agreements such as the United Nations Guiding Principles on Business and Human Rights to ensure that human rights are recognized and respected in the digital realm. Over the previous decade, internet companies have faced greater scrutiny on problems such as censorship, data privacy, digital security, and surveillance protection, among others. These are linked to fundamental human rights treaties like the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights, which establish important privacy and free expression rights.

4. Impact of Internet Shutdown on Human Rights

4.1 Implications On Free Speech and Expression

Internet shutdowns have a clear influence on the fundamental right to 'Freedom of Speech and Expression'. In the recent landmark judgment of 'Anuradha Bhasin v. Union of India' of 2020, the

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0545
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3435-3441

Supreme Court of India ruled that internet shutdown under any circumstances restricts one's right to 'Freedom of Speech and Expression', which is guaranteed to every citizen by the Indian Constitution under Article 19(1)(a). The "freedom of speech and expression" guaranteed by Article 19(1)(a) is not "absolute." It is limited in some ways. One of them is the "Doctrine of Reasonable Restrictions," which asserts that any restriction put in place by the government to protect national security and maintain peace and order can be considered acceptable. Furthermore, the right to use the internet has evolved into an extension of the right to freedom of speech and expression due to the growing use of the internet in all areas of employment. Kerala was the first state to recognize internet access as a fundamental right.

4.2 Impact On Journalism and Media

For the collection and distribution of news, journalism and the media heavily rely on the internet. During these cyber shutdowns, the industry suffers a number of difficulties. The public's access to important information is restricted since reporters and journalists are unable to deliver updates at the same time. In the cases of "Indian Express v. Union of India" and "Bennett Coleman v. Union of India," the Supreme Court of India emphasized that "freedom of press and media" is a basic right guaranteed by the Constitution, and that Internet shutdowns have clearly limited this freedom. As a result, creating an environment that encourages gossip and false information.

4.3 Violation of the Right to Information

The court acknowledged the "Right to Information" as a basic right under Article 19 of the Indian Constitution in the seminal decision of "Raj Narain v. State of Uttar Pradesh" in 1975. According to the court, people's "Right to Information" is violated when internet or online information sources are restricted and they are left without the necessary continuous updates. Furthermore, in the historic ruling of "Faheema Shirin v. State of Kerala" in 2020, the Kerala High Court ruled that the "Right to Internet" is a basic right under Article 21 of the Indian Constitution, and internet shutdowns even violate this right.

4.4 Social Isolation

Internet outages not only directly affect the right to information and the freedom of speech and expression, but they also exacerbate social isolation. Networking platforms are essential online venues that support communities, professional networking, and family connections. Cyber shutdowns cause people to cut themselves off from these online communities, which makes them feel socially alienated.

4.5 Disruption of Education

Internet shutdowns impede the process of online learning in a time when education is becoming more and more digitalized, depriving students of education and online educational resources. This worsens the educational gap by disproportionately impacting children in remote areas where the internet is an important learning tool.

4.6 Economic Consequences

Internet outages can have detrimental effects on the economy. Companies that depend on the internet for sales, operations, and communication may experience financial losses. Small companies and startups may be especially susceptible.

4.7 Disruption in Health Care

Research has demonstrated the substantial effects of shutdowns on health systems, such as the mobilization of urgent medical care, the disruption of equipment maintenance and the delivery of necessary medications, the restriction of medical personnel's ability to exchange health information, and the disruption of critical mental health services.

4.8 Protest and Violence

When the internet is shut down, people are cut off from the outside world, which leads to confusion and annoyance. This may lead to potentially violent protests or strikes.

4.9 Human Rights Abuse

When perpetrators use the disruption to conceal their crimes, such as murder, arson, gender-based assault, etc., shutdowns hamper accountability.

5. International Response to Internet Shutdown

5.1 Contextualizing Internet Shutdowns Within International Law

International law does not (yet) guarantee the right to

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0545
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3435-3441

access the Internet. It is, nevertheless, closely linked to other essential rights, such the right to free speech. The rights most immediately affected by shutdowns are listed in Article 19 of the International Covenant on Civil and Political Rights (ICCPR): the freedom of expression, the right to "hold opinions without interference," and the right to access and disseminate information. A significant proviso is included in Article 19, which enables restrictions on the exercise of the aforementioned rights, but only where "provided by law" and required "for respect of the rights or reputations of others" or "for the protection of national security or of public order."According to the HRC, because governments rarely specify the legal basis for a shutdown or even formally recognize its occurrence, Internet shutdowns frequently violate Article 19(3). The legal foundations are typically too general and ambiguous to justify the closure under Article 19(3) when nations do make reference to national security or laws. Additional constraints on any rights under the ICCPR are clarified in the Human Rights Committee's General Comment No. 31 from 2004: "States must prove their necessity and only take actions that are proportionate to the pursuit of legitimate aims." Because Internet shutdowns are so widespread, it is unlikely that they will ever be proportionate to their declared goal because they intrinsically violate protected rights and obstruct lawful activity. A UN organization dedicated to advancing international standards for information and communication technologies (ICT), such as the Internet, is the International Telecommunication Union (ITU). The ITU Constitution's Articles 34 and 35 specify when governments have the right to halt telecommunications. According to domestic law, Member States may discontinue private communications for reasons of national security under Article 34. Article 35 allows Member States to halt international telecommunications service, either generally or specifically, as long as they notify the ITU Secretary-General right away. National security is a prominent and ambiguous defense used by states to restrict rights and ICTs in both the ITU Constitution and the ICCPR.

5.2 International Shutdowns in Different Countries

Other countries intend to shut off the internet in 2023. India, Ukraine, and Iran will see the largest percentage of internet outages in 2023. They are the only countries experiencing double-digit Internet shutdowns. Other countries, however, have frequent internet outages. Myanmar (7), Bangladesh (6), Jordan (4), Libya (4), Sudan (4), and Turkmenistan (4) each experienced multiple internet disruptions in 2022. Ethiopia has also had a number of recent shutdowns, with some lasting months or even years.

Ukraine: Under normal circumstances, Ukraine would not be on the list of countries to shut down the internet in 2023. However, the country's continuing war with Russia has caused frequent internet outages over the last year. In 2022, Ukraine experienced 22 internet interruptions. The country has worked hard to get it back up and running each time, but it may not be able to adequately address the problem until the war with Russia is over.

Iran: During major protests in Iran in 2019, the internet was notoriously shut down. Iran's Supreme National Security Council has ordered that the internet be turned off for a week, with people only able to access the National Information Network during that period. Iran has also continued to censor the internet in recent years. In 2022, the country experienced 18 internet disruptions

Suggestions and Conclusion

Countries should enact strict legislation that specify when and how a shutdown may occur in order to stop the abuse of internet shutdowns. In order for the public to comprehend and, if necessary, challenge the action, governments should also publicly disclose information about each closure, including the cause, duration, and affected areas. In order for citizens to remain connected during emergencies, it is equally vital to develop more robust and adaptable communication technologies, such as community networks and satellite internet. Technology firms must abide by human rights norms and refrain from endorsing politically driven shutdowns. Human rights principles must be adhered to by technology businesses, and they must refrain from endorsing

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0545
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3435-3441

politically driven shutdowns. In order to help society resist digital repression, researchers, non-governmental organizations, and digital rights organizations should keep recording shutdown incidents and educating the public about their detrimental impacts. Internet shutdowns have become a regular tool for governments to exert control over the people. Many shutdowns are used to suppress criticism, limit protests, or influence political events rather than to preserve public safety. Shutdowns also undermine democracy by prohibiting open discussion and concealing important events from the public. This breeds distrust between the public and the government. Clear legislation, international cooperation, robust technology, and regular monitoring can be used to restrict the abuse of shutdowns and defend everyone's digital freedom.

Reference

[1]. Vide G.S.R. 998(E), dated 7th August 2017, published in the Gazette of India, Extra., Pt. II, Sec. 3(i), No. 679, dated 8th August, 2017.
[2]. Vide G.S.R. 724(E), dated 22nd November 2024, published in the Gazette of India, Extra., Pt. II, Sec. 3(i), No. 665, dated 22nd November, 2024.
[3]. https://www.berkeleyjournalofinternationallaw.com/post/iran-and-internet-shutdowns-does-international-law-have-an-answer
[4]. Anuradha Bhasin v. Union of India (2020) 3 SCC 63
[5]. Analyzing the Impact of Internet Shutdowns on Freedom of Expression and Access to Information – Juris Centre https://share.google/LjP4TPyuSG59diLSF
[6]. Indian Express v. Union of India (1985)1 SCC 641.
[7]. Faheema Shirin v. State of Kerala, (2019) 4 KER LT 301.
[8]. Raj Narain v. State of Uttar Pradesh, 1975 AIR 865.
[9]. Bennett Coleman v. Union of India, 1973 AIR 106.