



INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed Edition :

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume 2 Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

IJLRA

EDITORIAL TEAM

EDITORS



Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board



Dr. Namita Jain



Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law, Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8 Articles in various reputed Law Journals. Conducted 1 Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration. 10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.



Avinash Kumar



Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC - NET examination and has been awarded ICSSR - Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS
ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

INTERNET SHUTDOWNS: A THREAT TO FREEDOM AND DEMOCRACY

AUTHORED BY: ASHISH EAPEN

Institution: Christ (Deemed to be) University, Bengaluru

Abstract: The paper explores the concerning phenomenon of internet shutdowns by governments worldwide, creating an impact on freedom of expression and the access to information. Based on theoretical frameworks on human rights arguments for and against the legitimacy of internet shutdowns as tools for state control are made. An examination into the economic consequences of these shutdowns and highlighting and drawing parallels the with international regulations to address this issue and discussing various approaches to combat internet shutdowns, including legal mechanisms adopted by the courts and international initiatives. Through a critical analysis of precedents and international resolutions, the paper underscores the importance of protecting the internet and its platforms for the free exchange of ideas and information. This paper further compares the approaches to internet regulation between countries such as India, and the European Union (EU). The paper further delves into the legal and regulatory frameworks surrounding internet shutdowns, examining notable precedents in India and the broader implications for human and fundamental rights. It discusses the challenges posed by internet shutdowns in this age, particularly in balancing claims of national security concerns with the constitutionally guaranteed fundamental rights. Through a comparative analysis of international responses to internet shutdowns, the paper offers insights into best practices and policy recommendations for mitigating the negative impacts of these shutdowns. It concludes by emphasizing the importance of upholding fundamental rights in the digital era and the need for a concerted global effort to safeguard internet freedom. The EU's framework, exemplified by the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR), emphasizes protecting human rights while promoting innovation and competition. In contrast, the use of internet shutdowns in countries like India raises concerns about the balance between national security and individual rights. By examining these contrasting approaches, the paper highlights the importance of finding a balance that safeguards both national interests and fundamental rights in the digital age.

Keywords: *internet shutdowns, human rights, freedom of expression, fundamental rights,*

European Union

Several regulatory provisions govern internet access in the EU and its member states. The EU has aimed to tackle whether to achieve a decent standard of living in a gigabit society and whether the internet deserves a place along with human rights. The EU has introduced a new regulatory framework, the Digital Services Act (DSA). The DSA aims to modernize the existing rules for online platforms and services which were established in the e-commerce directive of 2000. These changes brought about keeping in mind the challenges posed by the digital economy, illegal products, spread of misinformation, etc.¹

All this brings about new obligations for online platforms, such as transparency requirements, content moderation, and measures to combat illegal activities. It is part of a broader trend towards increased digital economy regulation. The EU has set global standards for data regulation, such as the General Data Protection Regulation (GDPR).²

These regulations brought forth has an impact on digital technologies on the economy and our society, particularly the emergence of a platform economy and the increasing use of Artificial Intelligence, which shows how the evolving technologies pose to the rights enshrined in the EU Charter of Fundamental Rights, such as the right to privacy and data protection. This highlights the challenges and risks associated with the increasing use of digital technologies in our everyday lives and the growing need for regulatory responses and flexible interpretation of traditional instruments. Digital platforms have significantly transformed how we engage in public activities by enabling various interactions and services. These platforms, such as social media, e-commerce sites, and online communication tools, have become essential for journalism, civic engagement, education, and transportation. They facilitate user communication and provide avenues for collaboration, information sharing, and commercial transactions.

The dominance of the "Big Five" tech companies - Apple, Amazon, Alphabet (Google), Microsoft, and Meta- in the digital landscape raises several concerns. These concerns include market competition, data privacy, consumer choice, and potential abuse of market power. The concentration of power in the hands of a few significant players can limit innovation, stifle

¹ Lina Jasmontaite & Paul De Hert, Access to the Internet in the EU: A Policy Priority, a Fundamental, a Human Right or a Concern for eGovernment?, Brussels Privacy Hub Working Paper, vol. 6, no. 19, February 10, 2020.

² Aline Blankertz & Julian Jaurisch, How the EU plans to rewrite the rules for the internet, Brookings

competition, and raise questions about data protection and privacy.³

To protect fundamental rights in the context of digitalization and AI, it is essential to address the challenges posed by these technologies. One approach is to ensure that existing legal frameworks, such as the EU Charter of Fundamental Rights and the European Convention on Human Rights, are effectively applied to digital contexts. This includes safeguarding rights to privacy and data protection, freedom of expression and information, and other fundamental rights that may be at risk due to digitalization. Additionally, regulatory responses that balance innovation with protecting fundamental rights are crucial. Measures such as robust data protection regulations, transparency requirements for AI systems, and ethical guidelines for using digital technologies can mitigate risks and uphold fundamental rights in the digital age.⁴

Digital platforms have revolutionized how individuals engage in public activities by providing new avenues for communication, collaboration, and participation in various spheres of life. These platforms have become integral to modern society, enabling people to connect, share information, conduct business, and access services in previously unimaginable ways. For example, social media platforms allow users to interact with a global audience, share opinions, and discuss diverse topics. E-commerce platforms have transformed how goods and services are bought and sold, offering convenience and accessibility to consumers worldwide. Online education platforms have expanded learning opportunities, making knowledge more accessible and flexible. Additionally, digital communication tools have facilitated remote work, virtual meetings, and online events, enhancing connectivity and productivity.

The dominance of a few significant players can stifle competition and innovation, limiting consumer choice and potentially leading to monopolistic practices. The looming question of data privacy with relation to big tech companies and them collecting vast amounts of user data, raising concerns about data privacy, security, and the potential misuse of personal information. The market dominance of the Big Five may limit consumer rights, such as fair pricing, quality of service, and transparency in business practices. These companies' sheer size and influence give them significant control over digital ecosystems, raising concerns about the abuse of market power and anti-competitive behaviour.

³ Brkan, M., Claes, M., & Rauegger, C. (2020). European fundamental rights and digitalization. *Maastricht Journal of European and Comparative Law*, 27(6), 697-704. <https://doi.org/10.1177/1023263X20983778>

⁴ Estrada, Mariana. (2020). Revisiting access to internet as a fundamental right in times of COVID-19. *Unio - EU Law Journal*.

To protect fundamental rights in the context of digitalization and AI, it is crucial to implement comprehensive measures that address these challenges. This includes ensuring that legal frameworks, such as the EU Charter of Fundamental Rights and the European Convention on Human Rights, are effectively applied to digital contexts to safeguard fundamental rights. Implementing robust data protection regulations, such as the General Data Protection Regulation (GDPR), to protect individuals' privacy and personal data in the digital realm.

Enforcing transparency requirements for AI systems and digital platforms to ensure accountability for their actions and decisions. Developing and adhering to ethical guidelines for designing, developing, and deploying AI and digital technologies to uphold fundamental rights and values. Adopting a multifaceted approach that combines legal, regulatory, and ethical measures can mitigate the risks associated with digitalization and AI while upholding fundamental rights in the digital age.

Meanwhile, in India, we see the use of internet shutdowns, which are intentional disruptions of internet services which is one method of limiting citizens' freedom of expression and information and other associated rights in the name of national security, many viewing it as a means to consolidate power and suppress opposition since the internet can be used to mobilize and voice dissent.

India is one of many countries that have implemented internet shutdowns. Still, we also see countries like Myanmar and Ethiopia, and it isn't merely a form of control but includes the violation of international rights laws and the negative economic consequences it carries for businesses and individuals. Seen as a growing trend becoming more sophisticated and longer in duration.⁵ In the case of *Anuradha Bhasin v. UoI*⁶ surrounding the restrictions imposed in Jammu and Kashmir, particularly concerning freedom of expression, movement and the legality of internet shutdowns. The Court recognized the freedom of expression extends to online platforms as well. While acknowledging the States concern regarding political misuse of the internet for inciting violence, the court emphasized the restrictions on the internet access should be necessary, proportionate and subject to judicial review. The court found tat a complete and indefinite internet

⁵ Julia Ryng, Guillemette Guicherd, Judy Al Saman, Priyanka Choudhury & Angharad Kellett (2022) Internet Shutdowns, *The RUSI Journal*.

⁶ *Anuradha Bhasin v. UoI* , AIR 2020 SUPREME COURT 1308

shutdown was impermissible and that the State must justify and impose a temporal limit on such restrictions.

The court clarified that restrictions imposed under Section 144 of CrPC must be based on genuine concerns related to public order and safety. The court stressed that the authorities must provide material facts justifying the imposition of such restrictions and that they should not be used as a tool to suppress legitimate expression.

The court underscored the importance of transparency and accountability in government actions, particularly during restrictions on fundamental rights. It ruled that the State must disclose orders imposing restrictions and must provide valid justifications for any claims of privilege. It underscores the need for the State to adhere to constitutional principles and procedural safeguards when imposing restrictions, particularly in the context of rapidly evolving technological and geopolitical situations.

The case of *Foundation for Media Professionals v. Union Territory of Jammu and Kashmir & Anr.*⁷ brings to the forefront a contentious legal battle concerning the delicate balance between national security imperatives and the protection of fundamental rights in the digital age.

The region of Jammu and Kashmir, long embroiled in territorial conflicts, changed its status following the removal of Article 370 from the Indian constitution. This modification led to actions being taken, including a communication blackout involving suspending mobile internet services. The focus of this situation revolves around the restrictions imposed on internet usage and the reduction of internet speed to 2G.

The petitioners, which include organizations like the Foundation for Media Professionals, Soayib Qureshi, and the Private Schools Association of Jammu and Kashmir, based their arguments on violations of fundamental rights. They emphasized how crucial internet access is for healthcare, education, freedom of speech, business operations, and legal access. The petitioners argued that the government did not meet the criteria for implementing internet restrictions as outlined in a previous court case known as *Anuradha Bhasin v. Union of India*. Additionally, they contested the lack of a Review Committee—a requirement that was laid out in the *Temporary Suspension*

⁷*Foundation for Media Professionals v. Union Territory of Jammu and Kashmir & Anr.*, AIR ONLINE 2020 SC 521

of Telecom Services (Public Emergency or Public Safety) Rules in 2017.

On behalf of the government, represented by the Attorney General, a defense focused on security priority in policy decisions. The argument highlighted that safeguarding against insurgency and preventing misinformation spread for welfare should take precedence over rights. The government emphasized the risk of terrorism and the possibility of the internet being misused for activities. It stressed the importance of limiting internet access to reduce these dangers.

The Supreme Court, in its opinion, demonstrated a nuanced understanding of the complex issues at hand. While recognizing the importance of internet access for various aspects of daily life, the Court also acknowledged the profound implications of national security concerns. It weighed the competing interests and recognized the evolving role of the internet in modern terrorism.

The Court's decision to constitute a Special Committee, led by the Indian Home Secretary, to assess the necessity of the internet restrictions underscores its commitment to addressing individual rights and national security imperatives. The Court found that the blanket enforcement of the shutdown lacked sufficient justification and was not confined to specific high-risk areas.

The Foundation for Media Professionals case reflects an ongoing legal discourse on the scope of internet restrictions in the context of national security. It highlights the challenges of striking a delicate balance between safeguarding individual rights and countering emergent threats. The Court's emphasis on proportionality and the need for adequate reasons to justify restrictions sets an important precedent.

This case resonates with broader debates on the regulation of technology and its impact on fundamental rights. It raises questions about the limits of government authority in imposing restrictions on digital communications, particularly in an era where access to the internet has become indispensable for various aspects of modern life.

In conclusion, the Foundation for Media Professionals case is a crucial milestone in India's legal framework concerning internet restrictions and national security. It underscores the judiciary's role in mediating between competing interests and provides valuable insights into the evolving relationship between technology, individual rights, and state security.

The significant increase of internet shutdowns in recent years in India, particularly in certain states and the adverse effects these shutdowns have on various aspects of everyday life, including education, communication, and economic activities. But the flip side of the argument is the existence of legal justification for these shutdowns and the contractual and/or legal obligation.

The normative order of the internet is a complex and multifaceted issue that requires a deep understanding of the different levels and types of norms that must be integrated into it. One of the most pressing issues in this regard is the use of internet shutdowns by governments worldwide.⁸

At the heart of the debate over internet shutdowns is whether they are legitimate tools for governments to use in certain circumstances. It is argued that argues that a (partial) shutdown might be legitimate when the internet is being used as a tool, such as radio in the ICTR's Radio Télévision des Mille Collines case, and it is technically impossible to affect a more proportionate stop to incitement to genocide. However, in *Mukong vs. Cameroon*⁹, the Human Rights Committee confirmed that references to national security and unity can never suppress the promotion of human rights and democracy.

The use of internet shutdowns as tools for states to manage information and communication exchanges and to use infrastructure control to reach specific, often illegitimate, policy objectives has become pervasive. Access Now reports that partial shutdowns have increased dramatically, with sixty-one documented shutdowns in 2017 in states ranging from India and Pakistan to Belarus and Vietnam. In 2018, internet shutdowns in parts of Bali, Cameroon, Chad, India, Togo, Venezuela, and other states were used as tools by governments to silence activists, oppositional politicians, or grassroots movements.

The theoretical backing against internet shutdowns is grounded in the principles of human rights and democracy. The right to freedom of expression and access to information is enshrined in international human rights law, and internet shutdowns are seen as violating these rights. The United Nations Human Rights Council has passed a resolution condemning internet shutdown and calling on states to refrain from using them.

⁸ Matthias C. Kettmann, *The Normative Order of the Internet, Theorizing Order(s) on the Internet*, Oxford University Press (2020)

⁹ *Mukong v. Cameroon*. CCPR/C/51/D/458/1991

In addition to the human rights concerns, there are also economic consequences to internet shutdowns. A study by Deloitte and Facebook found that internet connectivity disruptions can significantly impact the economy, with losses estimated at \$2.4 billion in 2016. The economic impact of Internet shutdowns is particularly severe in developing countries, where the Internet is increasingly seen as a critical driver of economic growth and development.

To address the issue of internet shutdowns, several different approaches have been taken. One approach is to use legal mechanisms to challenge the use of internet shutdowns. In India, for example, the Supreme Court has issued several rulings that restrict the use of internet shutdowns and require the government to provide detailed justifications for any imposed shutdowns. Similarly, the African Commission on Human and Peoples' Rights has issued a resolution condemning internet shutdown and calling on states to respect the right to freedom of expression and access to information.

Another approach is to use technical measures to circumvent internet shutdowns. This can include virtual private networks (VPNs) or other tools that allow users to access the internet even when the government blocks it. Finally, there is a growing recognition of the need for international cooperation to address the issue of internet shutdowns. The United Nations has called on states to work together to develop a coordinated response to internet shutdowns, and several international organizations have launched initiatives to promote internet freedom and combat censorship.

India, the largest democracy in the world, experienced the longest internet shutdown in the year 2023, with a shutdown of over 5,000 hours in Manipur alone due to a violent ethnic conflict. India has had at least 30 significant shutdowns totaling 7,956 hours, affecting 59.1 million users and costing \$585 million globally. Shutdowns were often in response to civil unrest. Russia had the most shutdowns, affecting 113 million users and costing \$4.02 billion. Shutdowns in India cost the economy \$1.9 billion in the first half of 2023. Internet shutdowns in Punjab, for example, left 25 million without access due to a crackdown on a radical preacher. X (formerly Twitter) was the most blocked social media platform, with 10,683 hours of disruption, often due to compliance

with Indian government takedown orders.¹⁰

In conclusion, the use of internet shutdowns by governments worldwide is a complex and multifaceted issue that requires a deep understanding of the different levels and types of norms that must be integrated into the normative order of the internet. The theoretical backing against internet shutdowns is grounded in the principles of human rights and democracy, and several different approaches can be taken to address this issue, including legal mechanisms, technical measures, and international cooperation. Ultimately, the goal should be to ensure that the internet remains an open and accessible platform for the free exchange of ideas and information and that the rights of individuals to freedom of expression and access to information are protected.



¹⁰ "India had longest internet shutdown in 2023: Report," The Economic Times (Mar. 14, 2024), <https://economictimes.indiatimes.com/tech/technology/india-had-longest-internet-shutdown-in-2023-report/articleshow/108462868.cms?from=mdr>.