

DIGITAL BLACKOUT: INDIVIDUAL RIGHTS v COLLECTIVE SECURITY

Written by *Ms. Pratyusha Kar,*

4th Year BA LLB (Hons.) Student, West Bengal National University of Juridical Sciences

ABSTRACT

Over the last couple of years, several governments have extensively used network interruptions and shutdowns as a pervasive means of information control. State governments in India are issuing network shutdown orders so frequently that the country has become an international hotspot for the digital blackout. But such network disruptions and blackouts encroach into the fundamental rights of human beings. The present research work investigates the overall understanding of network shutdowns or digital blackouts across India and looks over the national and international laws and policy frameworks sponsoring blackouts. This research work also considers the spread of digital blackout cases in India in the period 2015 – 2018 and explores the intentions behind such disruptions. Furthermore, the issue research work critically analyses the impact of digital blackouts on the freedom of expression, association and peaceful assembly; the right to equality and digital division; the right to life; economic rights; the right to education and the right to religious belief. Finally, the research work submits propositions for the multi-stakeholder community to uphold a plausible equilibrium between larger facets of fundamental rights and safeguards for national safety and security.

INTRODUCTION

The outset of the internet has productively transformed our lives. It has become a general purpose technology (GPT)¹ and is a pivotal facilitator for achieving social and economic changes.² World Summit on the Information Society (WSIS) outcome document has clearly indicated that Information and Communication Technologies (ICTs) including the internet have played a vital role in achieving Millennium Development Goals (MDGs).³ *Au contraire*, most of the governments around the globe, particularly developing nation-states like India used to set up contingencies into domestic laws to permit the states to regulate communication networks and to interrupt or shutdown (blackout) networks on the pretext of collective or national security.⁴ 234 network shutdown cases have been reported in India in the period between January 2012 and August 9, 2018, out of which 96 cases are from Kashmir alone followed by 53 cases from Rajasthan.⁵ Nevertheless, under what circumstances the states could exercise these authorities are either not specified distinctly⁶ or could not meet up the doctrine of transparency. These network interruptions and blackouts contravene individual's fundamental right to freedom of expression, right to life, right to education besides social, cultural and economic rights. Such disruptions further repudiate United Nations' 'Sustainable Development Goal' of "increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by

1 Clarke, George et al (2015), "The Internet as General Purpose Technology: Firm Level Evidence from around the World" Policy Research Working Paper, World Bank Group. Available at : <http://documents.worldbank.org/curated/en/630411468338366817/pdf/WPS7192.pdf> , Last visited on July 22, 2018.

2 SFLC.in, "Living in Digital Darkness: A Handbook on Internet Shutdowns in India", May, 2018, New Delhi, India. Available at : <https://sflc.in/sites/default/files/reports/Living%20in%20Digital%20Darkness%20-%20A%20Handbook%20on%20Internet%20Shutdowns%20in%20India%2C%20May%202018%20-%20by%20SFLCin.pdf>, Last visited on July 22, 2018.

3 WSIS, World Summit on the Information Society WSIS+10 High-Level Event, "Outcome Documents", Geneva, 2014. Available at : <http://www.itu.int/net/isis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf>, Last visited on July 22, 2018.

4 See *supra* note 2.

5 Internet Shutdown Tracker, 2018. Available at : <https://internetshutdowns.in/> , Last visited on August 15, 2018.

6 Article 35, International Telecommunication Union (ITU) Constitution. Available at : http://www.itu.int/dms_pub/itu-s/oth/02/09/S02090000115201PDFE.PDF, Last visited on July 22, 2018.

2020”.⁷ But an integration of the rights of an individual citizen into the collective security or national security is the true symbol of democracy.⁸ Given the significance of individual rights at the time of digital blackouts, Part II focuses on the understanding of the digital blackout and examines the legal mechanisms and policy frameworks which entrust powers to the state to issue orders for the digital blackout. Part III reviews digital blackout cases in the period 2015 – 2018 in India and evaluates the motives behind such network outages. Part IV critically analyses the effect of the shutdown on fundamental rights and Part V confers that the collective security or national security could only be further ensured by reconciling individual rights with the collective security. Part VI proposes some recommendations for subsequent deliberations on the digital blackout. Part VII concludes by noting that the issue of digital blackout needs to be addressed in an effective and balanced way through meaningful collaborations and focused dialogues.

DIGITAL BLACKOUT AND LAW

What is Digital Blackout?

Digital blackout is the interruption or shutdown of the digital or electronic network in a particular region to regulate the free flow of information and thereby, pestering a preordained group of people. Such digital blackouts are purposeful and are imposed by the government agency to exert blanket ban of network services including internet access, mobile phone services, electronic broadcasting etc. for the purpose of collective or national security.

When Digital Blackouts take place?

7 United Nations, “Transforming our world: the 2030 Agenda for Sustainable Development”, 2015. Available at : <https://sustainabledevelopment.un.org/post2015/transformingourworld>, Last visited on July 22, 2018.

8 Commonwealth Human Rights Initiative (CHRI), “The need to reconcile Security and Human Rights”, 2006. Available at: http://humanrightsinitiative.org/old/publications/chogm/chogm_2007/docs/the_need_to_reconcile_security_&_human_rights.pdf, Last visited on July 22, 2018.

The government usually induces cessation of the communication network on the issues provoking regional or national insecurity like political instability⁹, contentious elections,¹⁰ mass events,¹¹ spreading of rumours that might engender concerted movement against government¹², following terrorist attack¹³ etc. The national security argument is the most expansive and most nebulous mode of justification towards the imposition of the digital blackout or network shutdown. For example, in Pakistan, digital blackouts including mobile internets,¹⁴ fixed-line broadband, short message service (SMS), voice service etc. are most common phenomena to pull off the fight against terrorism and national safety¹⁵. In order to suppress or end protests and to maintain law and order many governments like India,¹⁶ US,¹⁷

9 Belson David, "The Migration of Political Internet Shutdowns", Oracle Internet Intelligence, November 27, 2017. Available at <https://blogs.oracle.com/internetintelligence/the-migration-of-political-internet-shutdowns>, Last visited on August 8, 2018.

10 Keepiton, "Bleeding lives and money: the cost of internet shutdowns from Turkey to Bahrain", Accessnow, October 27, 2016. Available at <https://www.accessnow.org/bleeding-lives-money-cost-internet-shutdowns-turkey-bahrain/>, Last visited on August 8, 2018.

11 Ahuja M, "Rajasthan's Jaitaran town tense after communal violence; 10 detained, curfew till April 6", Hindustan Times, April 1, 2018. Available at <https://www.hindustantimes.com/jaipur/rajasthan-s-jaitaran-town-tense-after-communal-violence-10-detained-curfew-till-april-6/story-v2baPcM1XLU7THWmvZE7vO.html>; Aljazeera.com, "Four Indians killed in communal clashes at Hindu festival", Aljazeera.com, March 31, 2018. Available at <https://www.aljazeera.com/news/2018/03/indians-killed-communal-clashes-hindu-festival-180330122720303.html>, Last visited on August 9, 2018.

12 Sarkhel, A, "India shut down Internet 29 times in 2017", Economic Times, July 17, 2017. Available at <https://tech.economictimes.indiatimes.com/news/internet/india-shut-down-internet-29-times-in-2017/59627417>, Last visited on August 9, 2018.

13 Fung B, "After London attacks, British Prime Minister calls for worldwide Internet regulations to fight terrorism", The Washington Post, June 7, 2017,. Available at https://www.washingtonpost.com/news/the-switch/wp/2017/06/05/british-prime-minister-calls-for-worldwide-internet-regulations-to-fight-terrorism/?noredirect=on&utm_term=.c08e4a5edd1c, Last visited on August 9, 2018.

14 Killswitch, "Kill switch in Pakistan". Available at <https://killswitch.pk/>, Last visited on August 10, 2018.

15 IHRB (Institute for Human Rights and Business), "Security v Access: The Impact of Mobile Network Shutdowns Case Study: Telenor Pakistan", September, 2015. Available at <https://www.ihrb.org/pdf/2015-09-Telenor-Pakistan-Case-Study.pdf>, Last visited on August 10, 2018.

16 Live Mint, "Curfew like restrictions in Kashmir Valley, mobile internet suspended" Live Mint, February 9, 2014. Available at <http://www.livemint.com/Politics/rI4LLwxLZE8sgMGVHTse0M/Curfewlike-restrictions-in-Kashmir-Valley-mobile-Internet.html>, Last visited on August 11, 2018.

17 Kravets D, "San Francisco Subway shuts Cell Service to foil protest; Legal Debate ignites", Wired, August 15, 2011. Available at <https://www.wired.com/2011/08/subway-internet-shuttering/>, Last visited on August 11, 2018.

China,¹⁸ Iran,¹⁹ Bahrain,²⁰ Sudan,²¹ Syria²² etc. use digital blackouts as an absolute tool of censorship.

But what governments do not understand is that as for offline exchange of information, shutdown or blackout of online information network could not achieve the desired result since citizens often explore alternative ways of communication bypassing the government-sponsored digital blackouts just as the case of Ethiopia – during network blockade virtual private networks (VPNs) based on foreign countries were used.²³ Governments even did not pick up lessons from Egypt's incident of 2011 when internet blackout could not break the momentum of the dissents and ultimate throwing off of a thirty-year-old government resulted.²⁴ Moreover, such prohibitions can revoke citizens' fundamental rights, endanger means of living and cripple economic development.

Digital Blackout: Legal Framework

International Legal Framework:

A. INTERNATIONAL LEGAL STRUCTURE UNDER HUMAN RIGHTS

In 2014, the then UN Secretary-General in a conference on internet security while highlighting the need for digital network freedom emphasised that curtailment of “freedoms to preserve order” should not be the objective of a state rather the protection of digital freedom to establish

18 Economy C E, “The great firewall of China: Xi Jinping’s internet shutdown”, The Guardian, June 29, 2018. Available at <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown>, Last visited on August 10, 2018.

19 MIT Technology Review, “First Evidence of Iranian Internet Throttling as a Form of Censorship”, June 24, 2013. Available at <https://www.technologyreview.com/s/516361/first-evidence-of-iranian-internet-throttling-as-a-form-of-censorship/>, Last visited on August 11, 2018.

20 Access Now, “Internet disrupted in Bahrain around protests as wrestling match sparks shutdown in India”, June 24, 2016. Available at <https://www.accessnow.org/internet-disrupted-bahrain-around-protests-wrestling-match-sparks-shutdown-india/>, Last visited on August 11, 2018.

21 Access Now, “Update: Mass internet shutdown in Sudan follows days of protest”, October 15, 2013. Available at <https://www.accessnow.org/mass-internet-shutdown-in-sudan-follows-days-of-protest/>, Last visited on August 11, 2018.

22 Dyn Research, “Syrian Internet Shutdown”, June 3, 2011. Available at <http://research.dyn.com/2011/06/syrian-internet-shutdown/>, Last visited on August 11, 2018.

23 Kode D, “Internet shutdowns: the “new normal” in government repression”? Available at <https://www.opendemocracy.net/democraciaabierta/CIVICUS/david-kode/internet-shutdowns-new-normal-in-government-repression>, Last visited on August 10, 2018.

24 Cohen N, “Egyptians Were Unplugged, and Uncowed”, The New York Times, February 20, 2011. Available at <https://www.nytimes.com/2011/02/21/business/media/21link.html>, Last visited on August 10, 2018.

order is the appropriate approach.²⁵ Thus, a balance between freedom and security is of utmost importance. But the right to network access is not an absolute right instead it is an outcome of the combination of a number of fundamental rights like “freedom of expression, freedom to assemble and associate, right to livelihood, right to religion and right to information, among others”.²⁶

Article 19 of the Universal Declaration of Human Rights (UDHR), 1948 however, defines pervasive right to freedom of expression by ensuring that “[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers”.²⁷ This Article thus, affirms two elements of freedom of expression, one – the right to express and the other – right “to seek, receive and impart information”.²⁸ Moreover, this Article is technologically unbiased when it mentions “any media and regardless of frontiers”.²⁹ Article 19 of the International Covenant on Civil and Political Rights (ICCPR) states that –

- “1. Everyone shall have the right to hold opinions without interference.*
- 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
- 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
 - (a) For respect of the rights or reputations of others;*

25 UN Secretary-General, “Curtailling Freedom Does Not Preserve Order, But Undermines It”, transcript of video message to the fourth annual Freedom Online Coalition Conference: Free and Secure Internet for All, Tallinn, Estonia, SG/SM/15808, PI/2088, April 29, 2014. Available at <https://watermark.silverchair.com/chv021.pdf>, Last visited on August 11, 2018.

26 Srivastava R and Abraham B, “Anatomy of virtual curfews: Human rights vs. national security”, Association for Progressive Communications (APC), March 2017. Available at <https://www.apc.org/en/pubs/anatomy-virtual-curfews-human-rights-vs-national-security>, Last visited on August 11, 2018.

27 The Universal Declaration of Human Rights (UDHR), 1948. Available at <http://www.un.org/en/universal-declarationhuman-rights/>, Last visited on August 11, 2018.

28 *Ibid.*

29 *Ibid.*

*(b) For the protection of national security or of public order (ordre public), or of public health or morals”.*³⁰

The clause “media” here in the Article 19(2) also administers a firm base in favour of “freedom to connect” based on “the idea that governments should not prevent people from connecting to the internet, to websites, or to each other” that US State Secretary, Hillary Clinton enunciated in January 2010.³¹

Albeit, ICCPR in its 2009-10 report never mentioned about internet or online communication but only remained confined within the rights of the NGOs, human rights activists, journalists and other media persons.³² It is the Special Rapporteur, La Rue who for the first time highlighted in its May 2011 Report about the significance of Internet access as a right to express and proscribed the traditions those “cut off access to the Internet entirely” violating Article 19.³³ Subsequently, in the revised General Comments No. 34 of the Human Rights Committee, it was submitted that “[s]tates parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto.”³⁴ The right to freedom of expression for access to digital communication is thus, a state obligation as envisaged by the general comments.

In June 2012, the United Nations Human Rights Council (UNHRC) in its resolution called for the states “to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries”.³⁵

In June 2014, UNHRC in its resolution called on the states to protect and promote “right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of

30 International Covenant on Civil and Political Rights (ICCPR), 1966. Available at <https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf>, Last visited on August 11, 2018.

31 Land M, “Toward an International Law of the Internet”, 54(2) Harvard International Law Journal (2013) 410.

32 Human Rights Comm., Rep. of the Human Rights Comm., Aug. 1, 2009–Jul. 31, 2010, ¶¶ 65(26), 68(24), 68(28), 70(20), 72(24), 75(9), U.N. Doc. A/65/40 (Vol. 1); GAOR, 65th Sess., Supp. No. 40 (2010).

33 Frank La Rue, Special Rapporteur on the “Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Human Rights Council, U.N. Doc. A/HRC/17/27, May 16, 2011.

34 Human Rights Comm., General Comment No. 34 on Article 19: Freedoms of Opinion and Expression, ¶15, U.N. Doc. CCPR/C/GC/34 Sep. 12, 2011.

35 Human Rights Council Res. 20, “The Promotion, Protection and Enjoyment of Human Rights on the Internet”, 20th Session, June 18–July 6, 2012, 67th Sess., Supp. No. 53, A/HRC/20/L13 ¶ 3 June 29, 2012.

digital communications”.³⁶ In July 2016, UNHRC on its 32nd session re-established “promotion, protection and enjoyment of human rights on the Internet” and at the same time condemned any State action causing disruption and intentional prevention of “access to or dissemination of” online information.³⁷ This resolution is of great importance as it unequivocally addressed the issue of the digital blackout.

But how far should we extend this right to freedom of expression? Hillary Clinton, the 67th US Secretary of States, articulated that “free expression has its limits” represented under the circumstances of hate speech, terror terms, intellectual property theft etc.³⁸ Thus, there is a need to balance freedom of expression.

B. THE INTERNATIONAL TELECOMMUNICATION UNION (ITU)

Article 34/181 of the ITU, a treaty-based organisation under UN, restricts digital communication as the “[m]ember States also reserve the right to cut off, in accordance with their national law, any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency.”³⁹ Article 35/182 allows the member States “the right to suspend international telecommunication service.”⁴⁰

But conversely, the UN Special Rapporteur, David Kaye has asserted that “internet kill switches are absolutely impermissible under international human rights law, even in times of conflict.”⁴¹ Moreover, the clauses ‘public order’ and ‘decency’ in the Article 34 are not defined.

36 Human Rights Council Res. 27, “The right to privacy in the digital age”, 27th Session, A/HRC/27/37 June 30, 2014. Available at https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf, Last visited on August 11, 2018.

37 The Centre for Internet and Society, “UNHRC Resolution on The Promotion, Protection and Enjoyment of Human Rights on the Internet (A/HRC/32/L.20)”. Available at <https://cis-india.org/internet-governance/resources/unhrc-resolution-on-the-promotion-protection-and-enjoyment-of-human-rights-on-the-internet-a-hrc-32-l-20/view>, Last visited on August 11, 2018.

38 Clinton R H, Remarks on Internet Freedom, 21 January 2010. Available at <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>, Last visited on August 11, 2018.

39 Article 34/181, International Telecommunication Union (ITU). Available at <https://www.itu.int/council/pd/constitution.html>, Last visited on August 11, 2018.

40 Article 35/182, International Telecommunication Union (ITU). Available at <https://www.itu.int/council/pd/constitution.html>, Last visited on August 11, 2018.

41 Micek P, “Internet kill switches are a violation of human rights law, declare major UN and rights experts”, Access Now, May 4, 2015. Available at <https://www.accessnow.org/internet-kill-switches-are-a-violation-of-human-rights-law-declare-major-un/>, Last visited on August 11, 2018.

Furthermore, a number of countries are misusing the provisions of the ITU Constitution and as many as forty-two countries filter and blackout the online materials.⁴² UN Special Rapporteur La Rue has directly criticised China “for controlling information on the Internet”⁴³ through the great firewall of China.⁴⁴ Robert M. McDowell has rightly addressed the problem in his article titled ‘The UN Threat to Internet Freedom’ declared that “a top-down, centralized, international regulatory overlay is antithetical to the architecture of the Net, which is a global network of networks without borders.”⁴⁵ He also asserted that any endeavour to increase intergovernmental influence on the internet (since China, Russia and its allies are trying to revise the 1988 ITU treaty for achieving greater access to the formerly unmonitored arena) should be countered as the engineering and economic decisions would then “become politically paralyzed within a global regulatory body” and “productivity, rising living standards, and spread of freedom” would become standstill particularly for the developing countries.⁴⁶ Thus, ITU Constitution needs amendments only to ensure constructive reforms with greater transparency at par with human rights law and without the emergence on any fresh global bureaucracy. Moreover, a non-regulatory role of the ITU should flow from those reforms. The forthcoming ITU Plenipotentiary Conference, 2018⁴⁷ might be an appropriate occasion in this regard.

Indian Legal Framework:

42 Take Action, “What’s at stake?” Available at <https://www.google.com/intl/en/takeaction/whats-at-stake/>, Last visited on August 12, 2018.

43 Frank La Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Special Rapporteur’s Report), Human Rights Council, A/HRC/17/27, May 16, 2011

44 ICANNWiki, “International Telecommunication Union”. Available at https://icannwiki.org/International_Telecommunication_Union, Last visited on August 12, 2018.

45 McDowell M R, “The U.N. Threat to Internet Freedom”, The Wall Street Journal, February 12, 2012. Available at <https://www.wsj.com/articles/SB10001424052970204792404577229074023195322>, Last visited on August 12, 2018.

46 *Ibid.*

47 ITU Plenipotentiary Conference, 2018. Available at <https://www.itu.int/web/pp-18/en/>, Last visited on August 11, 2018.

In order to surmise legal framework for the digital blackout in India we have to go through two statutes namely Code of Criminal Procedure, 1973⁴⁸ and Indian Telegraph Act, 1885⁴⁹ and the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017.⁵⁰ These Acts and Rule deliver authority to direct network shutdowns in the Indian States.

A. CODE OF CRIMINAL PROCEDURE (CrPC), 1973, §144

Although specific information related to the provisions applied during digital blackout are not available, it can safely be said that a vast majority of digital shutdowns have transpired in India between January 2015 to August 5, 2018, because of the imposition of Section 144 of CrPC, 1973. In Chapter X of the CrPC, 1973 under the content “Maintenance of Public Order and Tranquillity” Section 144 confers State governments “ [p]ower to issue order in urgent cases of nuisance or apprehended danger”.⁵¹ This order can be issued by the District Magistrate, Sub-Divisional Magistrate or by an Executive Magistrate based on the special power provided by the State government. This power allows the concerned Executive to “direct any person to do or to abstain from a certain Act”⁵² in order “to prevent, or tends to prevent, obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety or a disturbance of the public tranquillity, or a riot, or an affray”.⁵³ The order although is basically for maintaining law and order by inhibiting unlawful assembly and issuing curfews at the time of civil unrest but has been used in a broader sense to effectuate network shutdowns by ordering the Telecommunications Service Providers (TSPs). This Section, however, does not possess adequate checks and balances to avoid misuse of power and the clauses like “obstruction”, “annoyance” and “disturbance to public tranquillity ... or an affray” are not defined under any legislation. Furthermore, use of Section 144 for the blanket ban of digital

48 THE CODE OF CRIMINAL PROCEDURE, 1973, §144. Available at <https://indiacode.nic.in/acts/11.%20Code%20of%20Criminal%20Procedure,%201973.pdf>, Last visited on August 12, 2018.

49 THE INDIAN TELEGRAPH ACT, 1885, §5(2). <http://www.ijlt.in/pdf/Indian-Telegraph-Act-1885.pdf>, Last visited on August 12, 2018.

50 Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017. Available at <http://www.dot.gov.in/circulars/temporary-suspension-telecom-services-public-emergency-or-public-safety-rules-2017>, Last visited on August 12, 2018.

51 See *supra* note 48.

52 *Ibid.*

53 *Ibid.*

communication contravenes Article 19(1)⁵⁴ of the Constitution of India which guarantees freedom of expression.

The habitual use of Section 144 to impose digital blackout was challenged in the Gujarat High Court in the 2015 Public Interest Litigation (PIL) case of Gaurav Sureshbhai Vyas v State of Gujarat⁵⁵ where it was contended that the authority to restrict online information remained in the Section 69A of the IT ACT, 2000⁵⁶ and the State governments are not capable to apply Section 144 for network blockage. The Court, however, inferred that the State governments do have the authority to use Section 144 in case of emergency. Subsequently, the Apex Court also dismissed the Special Leave Petition (SLP) and held that ‘it becomes very necessary sometimes for law and order’.⁵⁷

B. INDIAN TELEGRAPH ACT, 1885, §5(2)

The term ‘telegraph’ under the purview of the Telegraph Act has its wider application including digital communication services since Section 3(1AA) defines the term ‘telegraph’ as for –

*“any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, radio waves or Hertzian waves, galvanic, electric or magnetic means”.*⁵⁸

Additionally, Section 5(2) of the Indian Telegraph Act, 1885 states that –

“On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government ... may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, ... public order or for preventing incitement to the commission of an offence, for reasons to be recorded in

54 Article 19(1), The Constitution Of India 1949. Available at <https://indiankanoon.org/doc/1142233/>, Last visited on August 12, 2018.

55 Gaurav Sureshbhai Vyas v State of Gujarat, Writ Petition (PIL) No. 191 of 2015. Available at <https://indiankanoon.org/doc/29352399/>, Last visited on August 12, 2018.

56 Information Technology (IT) Act 2000, §69A. Available at <https://indiankanoon.org/doc/10190353/>, Last visited on August 12, 2018.

57 Rautray S, “Supreme Court Upholds Internet Ban by States”, Economic Times, February 12, 2016. Available at <https://tech.economictimes.indiatimes.com/news/internet/supreme-court-upholds-internet-ban-by-states/50955292>, Last visited on august 12, 2018.

58 *Ibid.*

*writing, by order, direct that any message ... shall not be transmitted, or shall be intercepted or detained ...*⁵⁹

But the phrases “public emergency” and “public safety” are not interpreted under the legislation and though interpreted expressly by the Apex Court in the case of *People’s Union for Civil Liberties v Union of India*⁶⁰ are not followed by the State governments.⁶¹ Furthermore, the terms “sovereignty and integrity of India”, “the security of the State” and “preventing incitement to the commission of an offence” are also not defined under the law which paved the way for misuse of the Act by way of subjective explanation. Further, there is no standard protocol administering the issuance of network shutdown orders under the Telegraph Act, 1885.

C. TEMPORARY SUSPENSION OF TELECOM SERVICES (PUBLIC EMERGENCY OR PUBLIC SAFETY) RULES, 2017

In absence of any procedural guidelines under the original Telegraph Act, 1885, suspension of the digital network was broadly interpreted under Section 5(2). In order to overcome the situation Government of India notified Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 [hereinafter, Shutdown Rules, 2017] on 7th August under Section 7 of the original Act.⁶² The schematic guidelines are delineated in Figure 1 below. The Rule regulates “temporary suspension of telecom services due to public emergency or public safety”⁶³ but the terms “public emergency” and “public safety” are not defined anywhere leading to the apprehension that the right to express and other related human rights may be jeopardized. Under this Rule, the Executives who may order temporary suspension are referred to as ‘competent authority’.⁶⁴ In case of Central government, the Secretary under Home Ministry and in case of State governments, the Secretaries under Home Departments are the respective competent authorities. The rule also states that “in unavoidable circumstances”

⁵⁹ See *supra* note 49.

⁶⁰ *People’s Union for Civil Liberties v Union of India*, AIR 1997 SC 568.

⁶¹ See *supra* note 2, at 13.

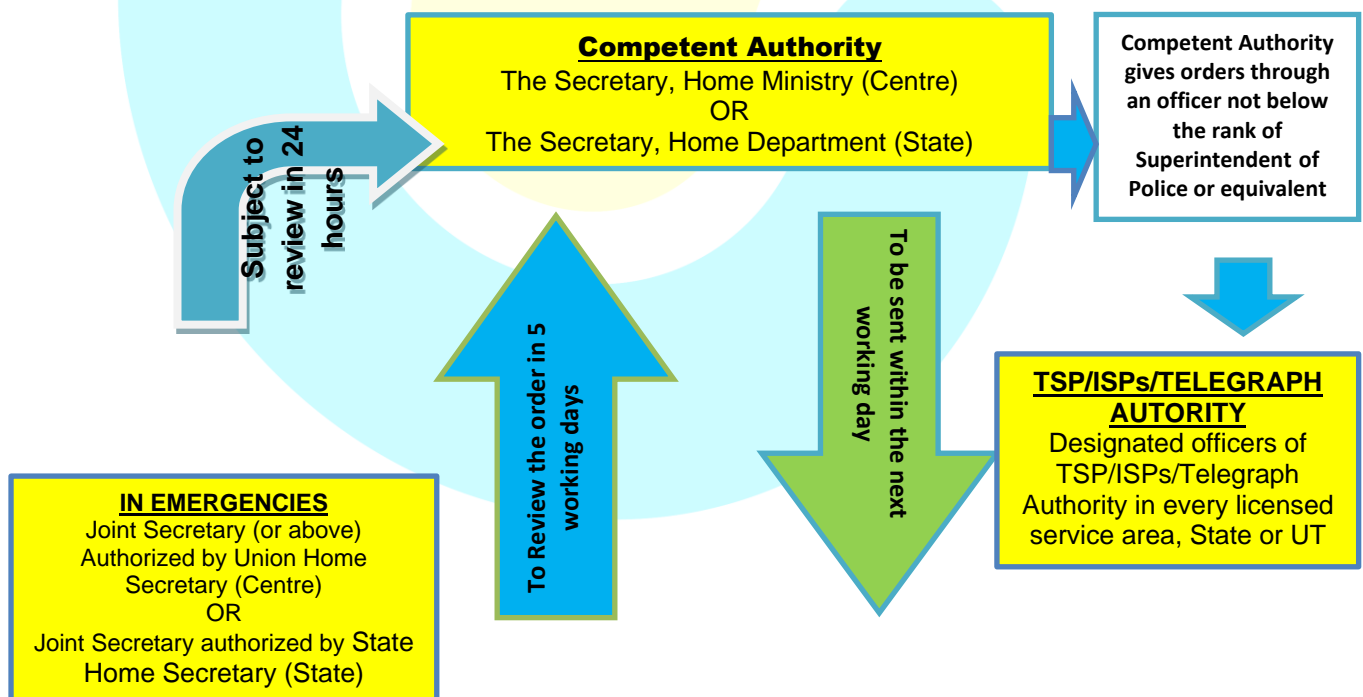
⁶² See *supra* note 50.

⁶³ *Ibid.*

⁶⁴ *Ibid.*

order may be issued by an Executive not below the rank of Joint Secretary.⁶⁵ But nowhere under this Rule or Telegraph Act or under any legislation or under any case law is the term “unavoidable circumstances” defined. Therefore, a legal vacuum exists – who to decide, how to decide unavoidable circumstances? The Rule then specifies that within 24 hours of issuance of an order under unavoidable circumstances approval from the competent authority is required to ensure its validity. The Rule further directs that the order given must have adequate reasonability and shall be sent to the review committee in the next working day and the review committee will report its findings within five working days. But what is the composition of this review committee? The review committee is constituted entirely by the executives and thus, autonomy and neutrality of the committee have become questionable as the doctrine of public oversight has been compromised. The Rule also lacks the transparency principle since there is no provision for gazette notification or press notification of shutdowns. Furthermore, the Rule never mentioned the period of such “temporary suspension”.

Fig. 1 Procedural Guidelines under *Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017* ^{66**}



⁶⁵ *Ibid.*

⁶⁶ *Ibid.*

REVIEW COMMITTEE

The Central Government Review Committee
(Cabinet Secretary, Secretaries of Legal Affairs & Deptt. Of Telecommunication)
OR

The State Government Review Committee
(Chief Secretary, Law Secretary or Legal Remembrance In-Charge, Legal Affairs
& Secretary to the State Government other than Home Secretary)

**Source: Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017. Available at <http://www.dot.gov.in/circulars/temporary-suspension-telecom-services-public-emergency-or-public-safety-rules-2017>, Last visited on August 12, 2018.

EVALUATION OF DIGITAL BLACKOUT CASES IN INDIA

Among the South Asian Countries, India eclipsed others in network shutdown incidents in 2017 – 18 (Fig – 2). The numbers of digital blackout cases in India are upsurging at a rapid pace (Fig – 3). In 2015 it was only 14, in 2016 it became 31 and in 2017 after the High Court as well as the Apex Court verdict in favour of application of Section 144 in digital shutdown orders in the case of *Gaurav Sureshbhai Vyas v State of Gujarat*⁶⁷ the numbers soared as high as 79 and in 2018 up-to 5th August it is 95 as against 43 up-to April, 2018.⁶⁸ The Shutdown Rules, 2017, in one hand have set an alarming precedence⁶⁹ by allowing network shutdown in the name of undefined terms like “public emergency”, “public safety” and “unavoidable circumstance” and on the other hand “both Section 144 and Shutdown Rules, 2017 were being used concurrently across the country”.⁷⁰

Fig – 2 India Topped in Digital Shutdowns in South Asia in 2017-18^{71**}

⁶⁷ See *supra* note 55 & 57.

⁶⁸ See *supra* note 2.

⁶⁹ Murthy A, “Internet Shutdowns: A Modern-day Siege”, The Centre for Internet and Society, December 19, 2017. Available at <https://cis-india.org/internet-governance/blog/internet-shutdowns-a-modern-day-siege>, Last visited on August 13, 2018.

⁷⁰ Gupta A, “The Worst Aspect of India’s Internet Shutdowns Is the Official Secrecy about It”, The Wire, July 5, 2018. Available in <https://thewire.in/tech/secrecy-abounds-the-creation-of-of-indias-internet-shutdown-law-why>, Last visited on August 13, 2018.

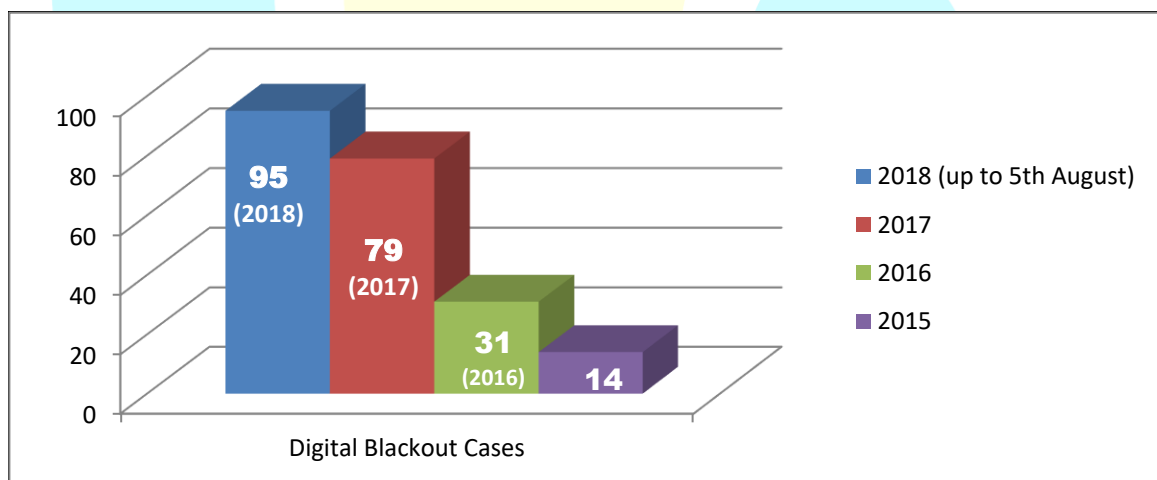
⁷¹ Times of India, “2018 is the worst year for internet shutdowns in India”, TOI, August 9, 2018. Available at <https://timesofindia.indiatimes.com/india/2018-is-the-worst-year-for-internet-shutdowns-in-india/articleshow/65333497.cms>, Last visited on August 13, 2018.



**Source: Times of India, “2018 is the worst year for internet shutdowns in India”, TOI, August 9, 2018

Available at <https://timesofindia.indiatimes.com/india/2018-is-the-worst-year-for-internet-shutdowns-in-india/articleshow/65333497.cms>

*Fig – 3 Digital Blackout cases from 2015 to 5th August 2018***



**Source: sflc.in, “Living in Digital Darkness: A Handbook on Internet Shutdowns in India”, May 2018, New Delhi, India

There are several incidents where Section 144 has been used to shutdown digital communication albeit Rule 2(1) under the Shutdown Rules, 2017 “implies that directions for suspension of telecom services, consequently network shutdowns, may not be ordered under

any other provision of law, including Section 144 of CrPC 1973”⁷² – from March 28 to March 30 midday, 2018, the District Magistrate of Paschim Bardhaman in West Bengal imposed blanket ban on mobile and broadband internet using Section 144; from April 2 to 3, 2018, the District Magistrate of Meerut, Uttar Pradesh terminated Mobile internet services applying Section 144; similarly from April 2 to 3, 2018, the District Magistrate of Barmer, Rajasthan blocked mobile internet services under Section 144 of CrPC.⁷³

Furthermore, there are ample evidence that even when the Shutdown Rules, 2017 have been used, the shutdowns have been ordered by the District Magistrates or by the District Police Commissioners instead of Home Secretary of the respective State as per rule.⁷⁴

Thus instead of one legislation two legal mechanisms are working now to exercise blockage of digital communication services.

Table – 1 List of Digital Blackout Incidents in India from 2015 to 5th August, 2018^{75}**

Sl. No.	Name of the State	2018	2017	2016	2015	Total
1.	J & K	36	32	10	5	83
2.	Rajasthan	27	19	6	1	53
3.	Bihar	4	3	2	-	9
4.	Haryana	-	8	4	-	12
5.	Uttar Pradesh	7	2	2	-	11
6.	Chandigarh	-	1	-	-	1
7.	Punjab	3	1	-	-	4
8.	Uttarakhand	1	-	-	-	1
9.	West Bengal	1	3	-	-	4
10.	Arunachal Pradesh	1	-	1	-	2

72 sflc.in, “Parliament’s last opportunity to Modify/Annul Telecom Suspension Rules 2017?” August 9, 2018. Available at <https://sflc.in/parliament-s-last-opportunity-modifyannul-telecom-suspension-rules-2017>, Last visited on August 13, 2018.

73 Saikia A, “India's Internet shutdown: Most states block services without following Centre’s new rules”, Scroll.in, April 7, 2018. Available at <https://scroll.in/article/874565/internet-shutdown-most-states-continue-to-block-services-without-adhering-to-the-centres-new-rules>, Last visited on August 13, 2018.

74 See *supra* note 71.

75 sflc.in, “Internet Shutdown Tracker”. Available in <https://www.internetshutdowns.in/>, Last visited on August 12, 2018.

11.	Nagaland	-	2	-	1	3
12.	Manipur	1	-	1	1	3
13.	Tripura	1	2	-	-	3
14.	Assam	1	-	-	-	1
15.	Maharashtra	5	1	1	-	7
16.	Gujarat	-	1	3	5	9
17.	Madhya Pradesh	2	1	-	-	3
18.	Tamil Nadu	1	-	-	-	1
19.	Andhra Pradesh	-	1	-	-	1
20.	Meghalaya	3	-	-	1	4
21.	Odisha	1	2	-	-	3
22.	Jharkhand	-	-	1	-	1
		95	79	31	14	219

** Source: sfle.in, "Internet Shutdown Tracker". Available in <https://www.internetshutdowns.in/>, Last visited on August 12, 2018.

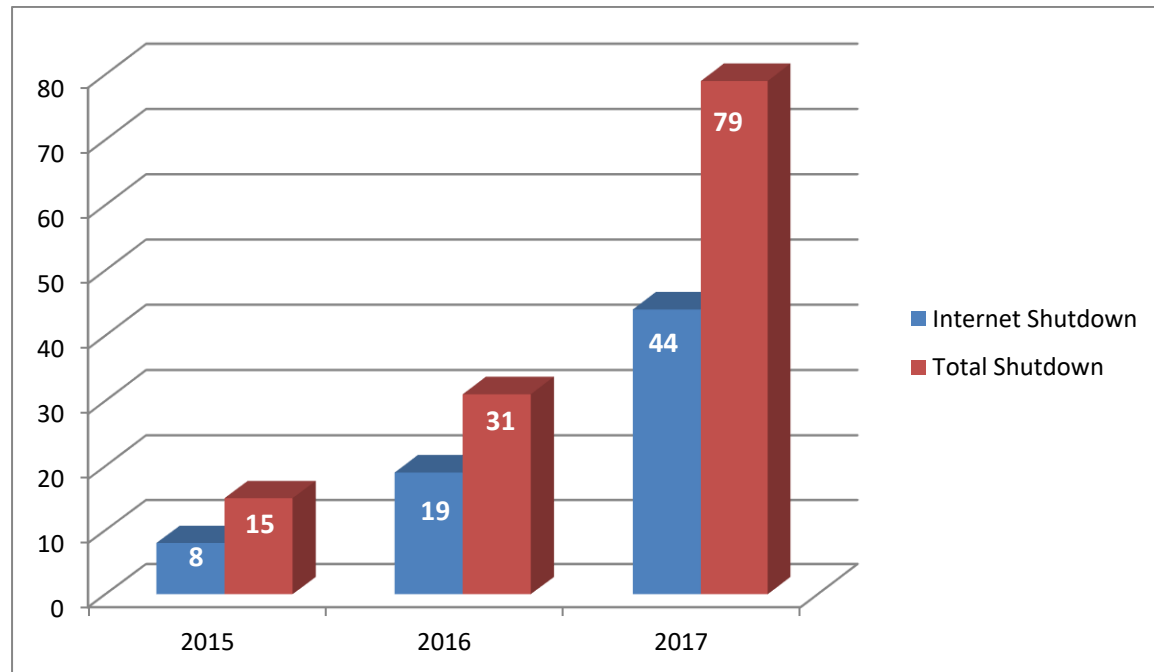
From the above Table – 1, it is clear that incidents of digital shutdown are growing at a faster rate in India and the growth was 121% in 2016 in comparison to the number of incidents in 2015 whereas parallel growth in 2017 was about 155% with respect to 2016. The highest number of incidents were found in Jammu and Kashmir (83 cases) in the study period of 2015 – 2018 followed by Rajasthan (53 cases). In 2018, rising rate of digital blackout cases in Rajasthan is even higher than Jammu and Kashmir (42% as against 12.5%). Moreover, wherein Jammu and Kashmir maximum shutdown cases are preventive shutdowns, in Rajasthan large percentage of cases are reactive shutdowns.⁷⁶ Similarly, in UP and Maharashtra digital blackout occurrences are also rapidly increasing. The purpose behind digital communication network shutdown is diverse but deeper analysis of the data available from the telecom regulatory Authority of India website⁷⁷ revealed that government agencies rely mostly on the mobile network shutdowns rather than fixed line services (8 mobile network shutdown incidents in 2015 as against 15 total shutdowns, 19 in 2016 as against total of 31 cases and 44

⁷⁶ See *supra* note 2.

⁷⁷ Telecom Regulatory Authority of India, *Yearly Performance Indicators of Indian Telecom Sector (Second Edition)*, May 4, 2018. Available at <http://traf.gov.in/sites/default/files/YPIRReport04052018.pdf>, Last visited on August 13, 2018.

in 2017 as against total of 79 shutdown cases) and thereby affecting large number of people (Fig. – 4).

Fig – 4 Mode of Digital Blackout incidents



EFFECT OF SHUTDOWN ON FUNDAMENTAL RIGHTS

In order to maintain an equitable constitutional equilibrium between the State power to infringe the rights of the citizens for maintaining law and order and the fundamental rights of the citizens, the act of the State should be ‘proportionate’ – infringement of rights by the State must not be greater than what is required to just attain the State’s objective. Seemingly, the network shutdown could not pass this test of proportionality.⁷⁸ In light of this, the author will discuss about the effect of the shutdown on fundamental rights.

Right to Freedom of Expression, Freedom of Association and Assembly

⁷⁸ Bhatia G, “Courts must take into account the exceptional character of Net shutdowns and their impact on civil liberties”, The Hindu, October 18, 2017. Available at <https://www.thehindu.com/todays-paper/tp-opinion/making-the-internet-disappear/article19879182.ece>, Last visited on August 15, 2018.

The shutdown of digital communication network circumvents the right to freedom of expression, association and assembly. As mentioned earlier that Article 19 of the UDHR⁷⁹ and Article 19 of the ICCPR⁸⁰ both guarantee freedom of expression. The resolution that was taken by the United Nations Human Rights Council in 2016 also asserts that “the same rights that people have offline must also be protected online, in particular, freedom of expression”.⁸¹ The effect of the shutdown on the freedom of expression becomes deeply perceptive when it continues for a longer period. In June 2017, in the district, Darjeeling, West Bengal, the internet services were suspended for a period of long hundred days during the strike of Gorkha Janmukti Morcha (GJM) strike for an independent Gorkhaland.⁸² Here both the mobile network and fixed-line networks were blocked. In July 2016 Jammu and Kashmir internet shutdown, cable network shutdown, and newspaper circulation disruptions for a long period of fifteen days were enforced curbing the right to expression at a zero level.⁸³

Right to freedom of association is guaranteed under Article 20 of the UDHR⁸⁴ and Article 22 of the ICCPR⁸⁵ and freedom of peaceful assembly is a right conferred under Article 20 of the UDHR⁸⁶ and Article 21 of the ICCPR.⁸⁷ Digital shutdowns directed by the government frequently point to the suppression of freedom of association and peaceful assembly particularly in fear of unchecked rumour mongering and to control organising the online

79 See *supra* note 27. <https://www.thehindu.com/todays-paper/tp-opinion/making-the-internet-disappear/article19879182.ece>, Last visited on August 15, 2018.

80 See *Supra* Note 30.

81 See *Supra* Note 37.

82 See *Supra* Note 2.

83 Rydzak J, “Disconnected: A Human Rights-Based Approach to Network Disruptions”, The Global Network Initiative, June 22, 2018. Available at https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf, Last visited on August 14, 2018.

84 Article 20, The Universal Declaration of Human Rights (UDHR), 1948. Available at http://www.claiminghumanrights.org/udhr_article_20.html#at21, Last visited on August 14, 2018.

85 Article 22, International Covenant on Civil and Political Rights (ICCPR), 1966. Available at <https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf>, Last visited on August 14, 2018.

86 See *supra* note 82.

87 Article 21, International Covenant on Civil and Political Rights (ICCPR), 1966. Available at <https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf>, Last visited on August 14, 2018.

exchange of views to provoke potent protests. For example, mobile internet services and SMS services were suspended for three days starting from 14th April, 2018 to 26th April 2018 in the Kapurthala, Jalandhar, Hoshiarpur and Shaheed Bhagat Singh (SBS) Nagar (Nawanshahr) districts of Punjab to restrain spread of rumour on social media following a clash between the Dalit members and Hindu groups.⁸⁸ Similarly internet services were blocked for several days by different State governments like Madhya Pradesh (from 9th April, 2018 for 24 hours), Rajasthan (31st March, 2018 for two days), Bihar (26th March and 29th March, 2018 for more than three days), West Bengal (28th March, 2018 for seven days), Haryana (8th September, 2017 for couple of days) etc. on the issues of rumour mongering.⁸⁹ But in any of the cases government ever considered that such a blanket ban is not only a menace to the freedom of expression, association and assembly on the social media for those who are making comments on the particular relevant issue but also for those who are not concerned with that issue albeit wish to use the online media for other important and/or emergency purposes.

Right to Equality and Digital Inequality

Article 14 of the Indian Constitution states that “(t)he State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India”.⁹⁰ This connotes that any person living in India shall enjoy the right to equality before the law. Equality before law thus forbids any division or discrimination. These clauses right to “equality before the law” and “equal protection of the laws” are also established under Article 7 of the UDHR⁹¹ and Article 26 of the ICCPR.⁹² This implies equality between persons considering both vertical and horizontal elements and any discrimination or division based on disparate ingress to the digital network due to the blanket ban undermines the fundamental concept of equality.

88 ET Telecom, Mobile internet services suspended for 24 hrs in 4 districts of Punjab”, The Economic Times, April 16, 2018. Available at <https://telecom.economictimes.indiatimes.com/news/mobile-internet-services-suspended-for-24-hrs-in-4-districts-of-punjab/63777929>, Last visited on August 14, 2018.

89 See *supra* note 2.

90 Article 14, The Indian Constitution 1949. Available at <https://indiankanoon.org/doc/367586/>, Last visited on August 14, 2018.

91 Article 7, The Universal Declaration of Human Rights (UDHR), 1948. Available at http://www.claiminghumanrights.org/udhr_article_7.html, Last visited on August 15, 2018.

92 Article 26, International Covenant on Civil and Political Rights (ICCPR), 1966. Available at <https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf>, Last visited on August 15, 2018.

Right to Life

Right to life is protected under Article 6 of the ICCPR.⁹³ Article 3 of the UDHR ensures “right to life, liberty and security of a person”.⁹⁴ Likewise, Indian Constitution also guarantees right to life under Article 21.⁹⁵ ‘Life’ here does not simply mean the physical existence of the human body; it is used in a much wider sense which includes right to human health, right to dignity, and right to livelihood. It encompasses all explicit facets of life which induce the life purposeful, brimming and worth living. But blocking digital networks greatly affects the capacity of the inhabitants to communicate comfortably with the friends and relatives in the event of unsafe, uncertain, precarious and conceivably life-threatening circumstances.⁹⁶ In a report published in 2017 on the effect of internet shutdown in Kashmir indicates that it restricts citizens from getting online health advice, deny doctors to access patient information and to have the second opinion.⁹⁷

Economic Rights

Economic rights as an objective come out unequivocally from the Constitution of India in its directive principles which “shall not be enforceable by any court,”⁹⁸ but an essential requirement of the State in lawmaking where the State shall “direct its policy towards securing that ... men and women equally have the right to have an adequate means of livelihood”⁹⁹ and,

93 Article 6, International Covenant on Civil and Political Rights (ICCPR), 1966. Available at <https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf>, Last visited on August 15, 2018.

94 Article 3, The Universal Declaration of Human Rights (UDHR), 1948. Available at http://www.claiminghumanrights.org/udhr_article_7.html, Last visited on August 15, 2018.

95 Article 21, The Constitution Of India 1949. Available at <https://indiankanoon.org/doc/1199182/>, Last visited on August 15, 2018.

96 Centre for Civil Society, “India Has The Highest Number Of Internet Shutdowns In The World”, Spontaneous Order. May 28, 2018. Available at <https://spontaneousorder.in/india-has-the-highest-number-of-internet-shutdowns-in-the-world-b09df646c746>, Last visited on August, 2018.

97 Chandran R, “Internet shutdowns rob Kashmiri activists of social media lifeline”, Live Mint, April 28, 2017. Available at <https://www.livemint.com/Politics/wFvulrVPR8GII09HXjkbTI/Internet-shutdowns-rob-Kashmiri-activists-of-social-media-li.html>, Last visited on August 15, 2018.

98 Article 37, The Constitution of India 1949. Available at <https://indiankanoon.org/doc/76375/>, Last visited on August 15, 2018.

99 Article 39 (a), The Constitution of India 1949. Available at <https://indiankanoon.org/doc/555882/>, Last visited on August 15, 2018.

“within the limits of its economic capacity and development, make effective provision for securing the right to work, to education”¹⁰⁰ and to governmental assistance. Article 25 of the UDHR¹⁰¹ and Articles 6 and 11 of the ICESCR¹⁰² also recognize the right to work and an acceptable standard of living for someone and his family. A study conducted by the Indian Council for Research on International Economic Relations (ICRIER) reveals that economic loss to India due to internet shutdown in the period 2012 to 2017 is US \$3.04 billion.¹⁰³ A Times of India Report unveils that Gujarat suffered a loss of US\$70 Billion for a six-day internet and SMS blocking in 2015.¹⁰⁴ Similarly, a report submitted by the Brookings Institute while quantifying the economic losses to India in 2016 for such network shutdown adjudged it to be US \$968 Million.¹⁰⁵ Under digital India campaign with a rapid push towards cashless transaction, every policy decision in favour of network shutdown is a real threat as it affects the rights of the citizens including economic rights. Moreover, a number of businesses like e-commerce, e-trading, e-banking, online trading etc. exclusively depend on the digital network. A habitual assertion of exigency through network shutdowns could not be the sufficient ground for limiting the rights of the citizens of India.

Right to Education

100 Article 41, The Constitution of India 1949. Available at <https://indiankanoon.org/doc/1975922/>, Last visited on August 15, 2018.

101 Article 25, The Universal Declaration of Human Rights (UDHR), 1948. Available at http://www.claiminghumanrights.org/udhr_article_20.html#at21, Last visited on August 15, 2018.

102 Article 6 and Article 11, International Covenant on Economic, Social and Cultural Rights (ICESCR), 1966. Available at http://www.pwescr.org/PWESCR_Handbook_on_ESCR.pdf, Last visited on August 15, 2018.

103 Kathuria R, Kedia M, Varma G, Bagchi K and Sekhani R, “The Anatomy of an INTERNET BLACKOUT: Measuring the Economic Impact of Internet Shutdowns in India”, ICRIER, April, 2018. Available at http://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf, Last visited on August 15, 2018.

104 Mishra P, “Mobile Internet shut down: Over ` 7000 crore losses to banks in Gujarat”, Times of India, September 1, 2015. Available at <http://timesofindia.indiatimes.com/city/ahmedabad/Mobile-Internet-shut-down-Over-Rs-7000-crorelosses-to-banks-in-Gujarat/articleshow/48760311.cms>, Last visited on August 15, 2018.

105 West M D, “ Internet shutdowns cost countries \$2.4 billion last year”, Center for Technology and Innovation at Brookings, October, 2016. Available at [https://](https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf)

www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf , Last visited on August 15, 2018.

The right to education is enumerated in the Article 13 of the ICESCR.¹⁰⁶ Article 26 of the UDHR also ensures the right to education.¹⁰⁷ Article 21(a) of the Indian Constitution further guarantees that “(t)he State shall provide free and compulsory education to all children of the age of six to fourteen years in such manner as the State may, by law, determine”.¹⁰⁸ During protracted digital blackouts students could not achieve academic success and it is evident from Kashmir¹⁰⁹ to Ethiopia.¹¹⁰ The situation is much alarming for those who have enrolled themselves for online courses.

Freedom of Religious Practice

Article 18 of the UDHR articulates “right to freedom of thought, conscience and religion”.¹¹¹ Article 18 of the ICCPR also secures the same rights.¹¹² Article 25 (1) of the Indian Constitution assures the “right freely to profess, practise and propagate religion”.¹¹³ The digital networking system is presently playing an important role in promoting different types of religious traditions through suggestions, counselling and approach to religious connoisseurs.¹¹⁴ Although sometimes abuses of digital network tools to spread hateful religious beliefs targeting disbelievers instigate governmental censorships and restrictions but if such repressions are not cautiously tailored may cause a serious violation of fundamental rights.

106 Article 13, International Covenant on Economic, Social and Cultural Rights (ICESCR), 1966. Available at http://www.pwescr.org/PWESCR_Handbook_on_ESCR.pdf, Last visited on August 15, 2018.

107 Article 26, The Universal Declaration of Human Rights (UDHR), 1948. Available at http://www.claiminghumanrights.org/udhr_article_20.html#at21, Last visited on August 15, 2018.

108 Article 21 (a), The Constitution of India 1949. Available at <http://constitution.onelawstreet.com/article-21a-right-to-education/>, Last visited on August 15, 2018.

109 Qureshi A, “The new normal of living with no Internet in Kashmir”, *Feminism in India*, June 6, 2017. Available at <https://feminisminindia.com/2017/06/06/living-no-internet-kashmir/>, Last visited on August 15, 2018.

110 Jeffrey J, “Internet blackout forces young Ethiopians to go retro”, *Deutsche Welle*, November 23, 2016. Available at <http://www.dw.com/en/internet-blackout-forces-young-ethiopians-to-go-retro/a-36490982>, Last visited on August 15, 2018.

111 Article 18, The Universal Declaration of Human Rights (UDHR), 1948. Available at http://www.claiminghumanrights.org/udhr_article_20.html#at21, Last visited on August 15, 2018.

112 Article 18, International Covenant on Civil and Political Rights (ICCPR), 1966. Available at <https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf>, Last visited on August 15, 2018.

113 Article 25 (1), The Constitution of India 1949. Available at <https://indiankanoon.org/doc/631708/>, Last visited on August 15, 2018.

114 See supra note 82.

DISCUSSION

At the international level Control of digital network is principally signified as a multi-stakeholder administration regulated by private, public, national and international players.¹¹⁵ Under this multi-stakeholder governance, there are issues of the right to privacy, data security, the risk of digital disruption and cyber-attacks in one hand and the issues of internet freedom in the other hand.¹¹⁶ Here, regulation and freedom go side by side. But there is ingrained digital divide and global imbalance which undermines the political independence and freedom of expression. China,¹¹⁷ Russia¹¹⁸ and the Middle East may be named in this context. Consequent to this perspective, there is an urgent need for the infusion of non-government organisations and civil societies as part of the international legal framework for the protection of human rights, for inculcating the principles of humanitarianism and for building up of humane relationships beyond borders. Otherwise, ITU directed statutes of global online network regulation to ensure control over multilateral mechanism itself may be kidnapped.¹¹⁹ Under Indian context, every digital shutdown order should be weighed against the Doctrine of proportionality. In order to delineate the doctrine of proportionality Lord Diplock ponderously

115 Malcolm J, "Multi-Stakeholder Governance and the Internet Governance Forum", Terminus Press, Perth, (2008). Available at http://library.uniteddiversity.coop/Cooperatives/Multi-Stakeholder_Co-ops/Multi-Stakeholder_Governance_And_The_Internet_Governance_Forum.pdf, Last visited on August 16, 2018.

116 Rue L F, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", (Special Rapporteur's Report), Human Rights Council, A/HRC/17/27, 16 May 2011; Rue L F." Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion

and Expression", A/HRC/23/40, 17 April 2013.

117 MACASKILL E and DANCE G, "NSA Files Decoded: What the revelations mean for you?" The Guardian, November 1, 2013. Available at <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>, Last visited on August 17, 2018.

118 See *supra* note 116.

119 See *supra* note 38.

commented: “you must not use a steam hammer to crack a nut if a nut cracker would do”.¹²⁰ UN Human Rights Committee in 1999 in its general comments clearly mentioned that “(r)estrictive measures must conform to the principle of proportionality; ... they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected”.¹²¹ Here lies the balance between individual rights v collective security. Indian Apex Court has accepted the principle of proportionality long back in 2000 in the case of *Omkumar v Union of India*.¹²² But digital shutdowns orders are given indiscriminately with no fixed target groups – each citizen of a particular area gets affected including a large number of innocent citizens and its mode of approach is also aimless – irrespective of a large majority of genuine and legitimate users.

The Shutdown Rules, 2017 have come into force; Section 144 under CrPC is no longer applicable for ordering digital shutdowns. The districts magistrates are no longer entitled to restrict online networks in the event of breakdown of law and order situation. But State governments are frequently using Section 144 through their district magistrates violating the rules. Furthermore, even when Shutdown Rules, 2017 are applied, the rules were not enforced by the competent authority. It's a serious flaw on the part of the governments and they must be transparent. It is canonical that present-day governments, particularly democratic governments like India are to provide service to its citizens with the legal framework and not by breaking the law under any pretext.

On the other hand the Shutdown Rules, 2017 there are so many obscurities – the purview of the rule is alarmingly colossal, no prescribed guidelines regarding the end of shutdown period or at least periodic review of its impact on the common people, almost practical absence of the features of accountability, no mandatory provisions for making public announcements and an anomalous review committee with limited capacity. Under extreme situations temporary blockage may be meaningful but who will judge that the doctrine of proportionality is maintained under the circumstances where Internet Service Providers (ISPs) are bound to

120 *R v Goldsmith* (1983) 1 WLR 151, p. 155.

121 UN, International Covenant on Civil and Political Rights (ICCPR), “General comments no. 27, ¶14, 1999. Available at https://www.nichibenren.or.jp/library/ja/kokusai/humanrights_library/treaty/data/HRC_GC_27e.pdf, Last visited on August 15, 2018.

122 *Omkumar v. Union of India* AIR 2000 SC 3689, p. 3689.

follow the government dictate as per unified licence agreement which allows the government to keep “any area out of the operation zone of the service”.¹²³

Comprehensively, regulating the uninterrupted flow of online information is a threat to fundamental rights and a societal catastrophe. Government tries to ensure collective security at the cost of individual rights – the right to freedom of expression, right to association and assembly, right to equality, right to life, right to education, economic rights and freedom of religious practices. Doing so government undermines that collective security would be more protected by safeguarding the individual rights where collective security is merely not the security of the physical territories of the state and its values; it is the people-centric collective security where people should remain protected from the acts of duress (sponsored by the State as in digital shutdown for disbanding of peaceful demonstration in the social media) through promotion of larger aura of individual security. Lloyd Axworthy, an erstwhile Canadian Foreign Affairs Minister has rightly said, “(Human security) in essence, an effort to construct a global society where the safety of the individual is at the centre of the international priorities and a motivating force for international action”.¹²⁴

RECOMMENDATIONS

- A. Surgical Bans on access to the digital network:** Instead of blanket bans surgical approach towards network shutdown although fundamentally undesirable but is respectively a better approach. Government together with the network service providers can ensure emergency services to the citizen even during digital shutdowns. Area-specific IP address mapping could easily be done using local acumen to narrow down the impact of network blockage.
- B. Keep up Transparency:** In order to bring out transparency in the overall system government should reassess the present laws and the undefined clauses and terms of the laws as mentioned earlier should be properly interpreted. Moreover, the government should issue prior public notifications with justifications behind shutdown incidents. The government should also issue published documents periodically showing details of shutdown incidents.

123 Unified Licence Agreement. Available at http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf?download=1, Last visited on August 16, 2018.

124 Axworthy L, “Human Security and Global Governance: Putting People First”, 7(1) Global Governance, (2001) 231-236. Last visited on August 17, 2018.

- C. Policy Review:** Government should act together with the civil society organisations and service providers to explore alternative designs, if any, to narrow down the effects of the shutdown on a case to case basis. Moreover, periodic judicial and parliamentary assessment of the policy should be exercised.
- D. Provision for compensations:** The troubles faced and losses incurred by the individuals should be compensated financially. A customer grievance redressal mechanism addressing the hardship faced by the consumer needs to be maintained.
- E. Capacity building:** Capacity building programmes to strengthen the abilities of the law enforcing authorities need to be introduced at all levels so that the compelling situations do not arise. Under present-day situation the technical skills and the ability for early detection of cybercrimes and identifying the specific offenders are debatable. The State should share and adopt best practices to maintain law and order in more foreseeable situations. Proper training should be also be imparted to the government actors to sensitize them on the impact of disruptions and to pursue alternative measures.
- F. Awareness campaign:** Government and civil societies should organise awareness campaigns to promote psychological changes of the offenders as well as behavioural changes of the common people so that the former group abstains from rumour mongering, propagating hate speech and sending of provocative messages and the latter group shoulders the social responsibility to restrict such harmful practices.
- G. To enact corporate accountability:** Corporate accountability should also be fixed on the service providers. Usually, Indian telecom companies and network operators rarely share and/or disclose data related to the network shutdown and thus, demoting customer satisfaction.
- H. Functions of the civil society organisations:** (a) Defenders against digital shutdown must establish in quantitative terms that such exercises by the government are ineffectual and awfully expensive. (b) They should target the government ministries having high social impact e.g. health, education and economy and illustrate the negative impacts shutdown on the growing digital society. (c) The digital rights activists should activate other civil society actors like faith leaders, philanthropic associations and cultural celebrities to join hands in human rights impact assessments and to push for the exercise of rights. (d) The business community should be made aware of the impact of digital blackouts in tangible terms. (e) Initiatives from civil society organisations to conduct a detailed case study to examine the

complex aftereffects of digital blackout incidents on the economy and human rights in a specific country.

- I. Functions of the Academia:** Academia should take up interdisciplinary research projects to collect, collate and analyse data related to the ineffectiveness or effectiveness of shutdowns and to use it as an instrument to demonstrate dissent.
- J. Evasion of online censorship:** ‘Web-based proxy tools’, ‘Lantern’ – operating with geo-optimised server, ‘Psiphon’ – a circumvention software, ‘Tor’ – an open source software, ‘Virtual Private Networks’ (VPN), use of HTTPS and ‘HTTPS Everywhere’ are the devices to circumvent digital blackout.

CONCLUSION

The significance of information and communication technology (ICT) presently has reached a great height because of its rapid progression and declining costs. This, in turn, has resulted in an extremely beneficial impact on the exercise of civil and political rights – freedom of expression, freedom of association and assembly; freedom of religious practice; the right to life; the right to education; the right to Equality including digital equality; and socio-economic rights. But in the event of the digital shutdown, blockage of the mobile network and granting of restrictive licences to the telecom companies and service providers undermine these civil, political, economic and social rights.

Under Indian context, it also appears paradoxical that on one hand the government is pushing for digitization of trade, commerce, services, building national demographic database for its citizens and have placed great emphasis on the information technology sector to move the nation to the next stage development phase under its flagship programme ‘Digital India’ but on the contrary India is the global hotspot for enforcing the highest number of network shutdowns in the world and in August 15, 2018, total number of digital shutdowns have already surpassed over 2017 by more than 21 percent.

But extreme of none of these two – network shutdown and network freedom or internet freedom – is absolute; equitable, rational, qualificatory and selective use of the former may be beneficial and outright, unlimited and unrestricted freedom for access to digital networks expressed in ICT terms under human rights framework may be dangerous and harmful.

But balancing of this internet freedom in terms of freedom of expression and other fundamental rights with network shutdowns on the security point of view is very sensitive, delicate and challenging. Under these circumstances not only the laws should be reviewed to plug its

loopholes particularly on transparency issues, norms should be set to inhibit blanket bans ensuring emergency services but also the situation demands sensitisation of people to promote psychological and behavioural changes resulting positive attitude. In order to achieve this two-way goal multi-stakeholder society should act collectively for gestating practicable substitutes for network shutdowns to maintain interest equilibrium of all members.

