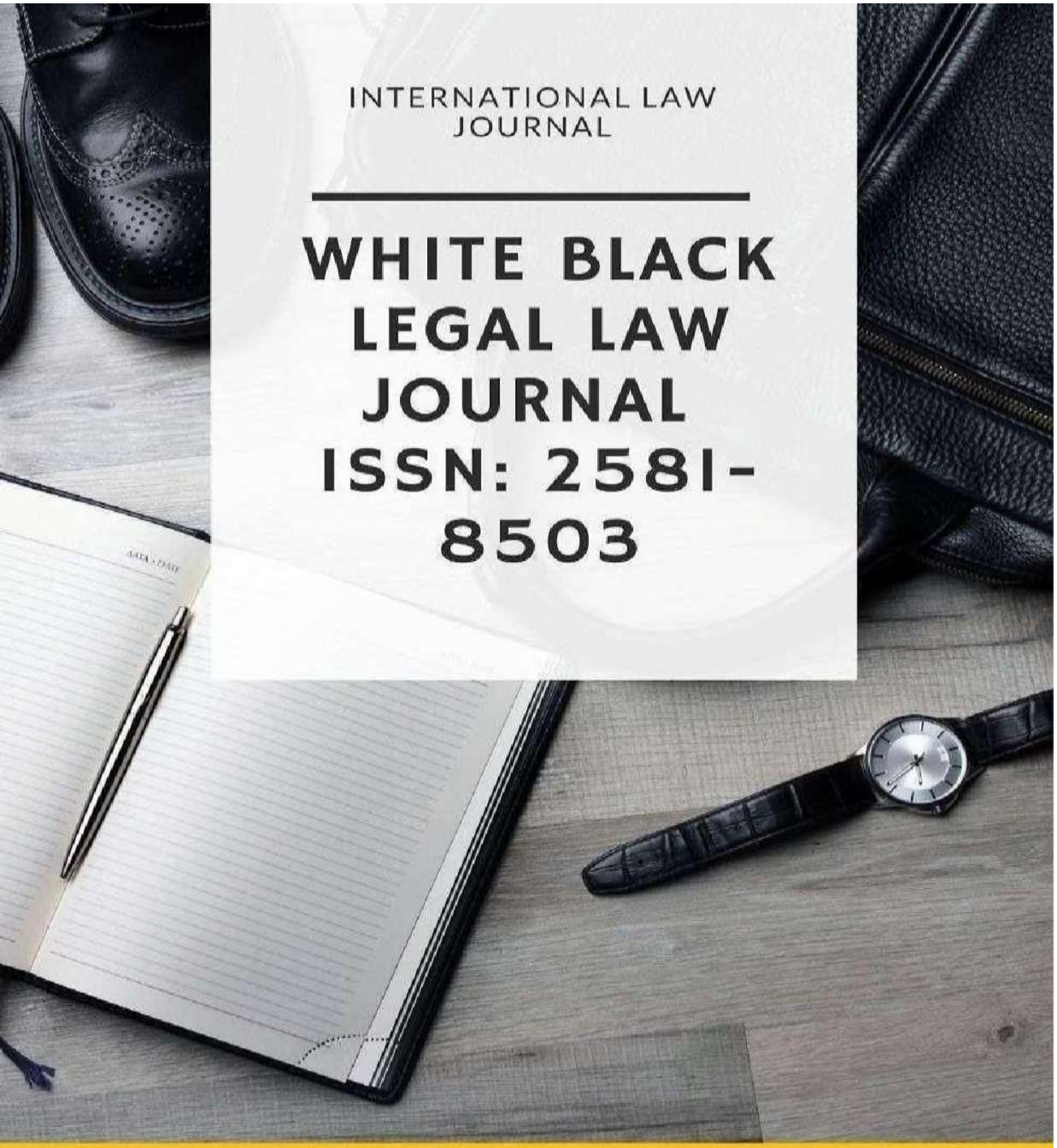

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

STATE CONTROL IN CYBERSPACE: INTERNET SHUTDOWNS, SURVEILLANCE, AND CENSORSHIP AS CHALLENGES TO HUMAN RIGHTS

AUTHORED BY - SUDESHNAMERCY. M
LLM Department Of Cyber Space Law And Justice,
The Tamil Nadu Dr. Ambedkar Law University
School Of Excellence In Law

ABSTRACT

The way that fundamental rights are used, understood, and limited has changed in the digital age. Internet shutdowns, state monitoring systems, and online censorship present complicated constitutional issues in this changing environment. In order to evaluate the constitutional restrictions on state power in the digital sphere, this study employs a purely doctrinal and analytical approach, looking at legislative frameworks, judicial doctrines, constitutional provisions, and significant Supreme Court rulings. With an emphasis on how these clauses govern digital restrictions, the study assesses the reach and interaction of Articles 19(1)(a), 19(2), 21, and 14 of the Indian Constitution.

It critically examines important legal precedents set in Anuradha Bhasin v. Union of India regarding proportionality and internet suspension regulations; K.S. Puttaswamy v. Union of India, which established safeguards for informational privacy and surveillance; and Shreya Singhal v. Union of India, which defined acceptable limits for online expression. Furthermore, the procedural protections outlined in the PUCL Telephone Tapping Case offer crucial constitutional standards for determining whether surveillance methods are lawful.

The study makes the case that any type of digital restriction must strictly adhere to the principles of legality, legitimate State purpose, necessity, proportionality, and minimal infringement through a thorough analysis of these doctrines and judicial interpretations. Constitutional guarantees of liberty, privacy, and freedom of expression must continue to be strong and unchangeable even as technological governance develops. In order to guarantee that fundamental freedoms maintain their importance and enforceability in the digital age, this doctrinal analysis emphasizes the necessity of a rights-centric constitutional approach.

KEYWORDS: Internet Shutdowns, Surveillance, Censorship, Digital Rights, Constitutional Law, Human Rights, Digital Governance.

INTRODUCTION

Everything has changed with the emergence of the digital state. Rights are no longer just about paper and courts. Today, the internet is life. We work, learn, protest, and interact there. Governments are aware of this. And they are watching. Slowly, quietly, sometimes openly. Digital power is growing. These days, internet regulation, data collection, surveillance, and online content control are more than just legal terms. They exist. And they touch our lives every day. Take internet shutdowns, for example. India tops the world in this. During protests, exams, rumours even small social media flare-ups connections vanish. People panic. Companies suffer. Students scramble. However, the State claims, "It's for security, public order, efficiency." Well, perhaps. But at what price? Our freedom? Our entitlement to know? Then there's surveillance. Fancy stuff facial recognition, AI monitoring, metadata tracking. It sounds futuristic. But it's here. Watching. capturing. evaluating. And confidentiality? It turns into this brittle notion that you hope endures. Censorship on the internet is more difficult. The IT Act. orders for government blocking. Vague rules. People confused, rights blurred.
The Constitution tries to keep up. Articles 19, 21, 14 they stand like pillars. And courts, sometimes, try to protect us. Puttaswamy (2017) made privacy a fundamental right. Online free speech was defended by Shreya Singhal (2015). Anuradha Bhasin (2020) and PUCL Telephone Tapping (1997) added layers of procedural safeguards. However, it's disorganized. Technology moves faster than law.[1] This study? It examines all of this mayhem. shutting down the internet. Digital spying. censorship. It poses difficult queries, such as what is necessary, what is legal, and what is excessive. We examine laws, court rulings, and even global standards. The goal? to determine whether rights can withstand the digital storm. or if they will simply disappear into data streams.

IMPORTANCE OF STUDY

Studying internet shutdowns, surveillance, and digital censorship is a constitutional requirement because the citizen-state relationship has changed due to the swift digitization of governance. Shutdowns affect fundamental rights like speech, trade, and education, demanding scrutiny of their legality and proportionality. Surveillance technologies, following Puttaswamy,

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

raise privacy and overreach concerns under Articles 21 and 14. Under the IT Act and Rules 2021, online censorship affects political participation, dissent, and free expression (Article 19). This study bridges technology and constitutional liberties, guiding judges, attorneys, and policymakers while bringing India's digital governance into compliance with international human rights standards.

AIM AND OBJECTIVES

To critically evaluate whether India's existing laws and constitutional doctrines adequately protect fundamental rights especially Articles 14, 19, and 21 against internet shutdowns, State surveillance, and online censorship, and to propose rights-centric reforms for digital governance.

Objectives of the Study

1. Analyse how internet shutdowns, surveillance, and censorship affect fundamental rights under Articles 14, 19, and 21.
2. Examine the statutory and regulatory framework governing digital restrictions in India.
3. Evaluate key judicial precedents that shape digital rights and constitutional protections.
4. Identify major gaps, risks, and constitutional inconsistencies in the current digital governance system.
5. Propose strong rights-centric reforms and safeguards for accountable and constitutional digital regulation.

REVIEW OF LITERATURE

Current literature indicates that digital governance, especially internet shutdowns, surveillance, and online censorship has been extensively examined, but mainly from technological or policy angles, with scant doctrinal constitutional evaluation.

Academics such as ***Raman Jit Singh Chima,[2] Apar Gupta,[3] and Usha Ramanathan*** [4] emphasizes India's regular shutdowns and their unequal effects on basic rights. Reports from the Internet Freedom Foundation (IFF), Access Now, and the UN Human Rights Council criticize shutdowns as disproportionate and not aligned with international human rights

[2] Raman Jit Singh Chima, Internet Shutdowns in India: A Rights-Based Critique, Internet Freedom Foundation (2020).
[3] Apar Gupta, The Constitutional Costs of Internet Shutdowns, Internet Democracy Project (2019).
[4] Usha Ramanathan, Surveillance, Privacy and the Indian State, 46(8) Econ. & Pol. Weekly 10 (2011).

standards, frequently not meeting the constitutional criteria of necessity and proportionality.

Building on ***K.S. Puttaswamy***, writers like ***Gautam Bhatia*** and ***Vrinda Bhandari*** explore the privacy consequences of government surveillance. Research from SFLC and CIS highlights the absence of transparency, accountability, and judicial scrutiny in regulations such as the Telegraph Act, in addition to the rise of new technologies like facial recognition and predictive policing. International scholarship, encompassing Shoshana Zuboff's research, addresses these issues. Analyses centered on the Shreya Singhal and Section 69A of the IT Act highlight the importance of transparency, due process, and the protection of free speech. Scholars like Lawrence Liang argue that digital forms of expression need to be protected with more constitutional securities.

Works of ***Justice B.N. Srikrishna and Prof. Madhav Khosla*** emphasizes that liberty, privacy, equality, and proportionality shall be the guiding principles of digital governance.[5]

Although there are some judicial doctrines, implementation gaps still exist, and few studies offer a holistic constitutional analysis of shutdowns, surveillance, and censorship combined.

RESEARCH GAP

Because most studies focus on shutdowns, surveillance, or censorship separately, the current body of research on digital rights is dispersed. Doctrinal analysis evaluating their combined effect on constitutional rights under Articles 14, 19, and 21 is scarce. Important laws like the IT Rules 2021, the Telegraph Act, and the Suspension Rules 2017 have not been thoroughly examined by academics. Questions of legality, necessity, proportionality, and due process remain underexplored. International standards under UDHR and ICCPR are rarely integrated into Indian scholarship. Socio-economic and democratic consequences of digital restrictions receive minimal attention. The literature currently in publication offers sporadic and insufficient policy recommendations. This study uses a thorough doctrinal and rights-based evaluation to close these gaps.

RESEARCH QUESTIONS

1. How do internet shutdowns, State surveillance, and online censorship in India affect fundamental rights under Articles 14, 19, and 21?
2. Do existing statutory frameworks—Telegraph Act, Suspension Rules 2017, IT Act, and

[5] Justice B.N. Srikrishna Committee, Report of the Committee of Experts on a Data Protection Framework for India (2018).

IT Rules 2021 provide adequate safeguards, transparency, and procedural checks for digital restrictions?

1. How effectively are judicial principles on proportionality, due process, and oversight implemented in regulating digital governance?
2. To what extent does India's approach to digital restrictions align with international human rights standards, and what reforms are needed to protect constitutional and democratic rights?

HYPOTHESIS

India's internet shutdowns, surveillance practices, and online censorship often exceed constitutional limits due to outdated laws and weak safeguards, and stronger judicial oversight, updated legal frameworks, and alignment with international human rights standards are necessary to protect fundamental rights in digital governance.

RESEARCH METHODOLOGY

This study adopts a purely doctrinal research methodology, relying entirely on legal reasoning, constitutional interpretation, and analysis of authoritative sources. The research is based on a systematic examination of primary legal materials such as constitutional provisions, statutory frameworks, government rules, and landmark judicial decisions of the Supreme Court of India. Secondary sources including books, journal articles, scholarly commentaries, international reports, and credible digital rights research publications are also examined to support doctrinal interpretation. The methodology involves qualitative analysis, comparative study with international human rights norms, and critical evaluation of the legality and proportionality of digital restrictions. No empirical or field based data is used.

CONCEPTUAL FRAMEWORK

INTERNET SHUTDOWNS

An internet shutdown refers to the intentional disruption of internet services by a government authority, making the internet either completely inaccessible or partially unusable for the public. Shutdowns are typically imposed under the justification of national security, public order, or preventing misinformation. In practice, however, they often lead to disproportionate restrictions on fundamental rights such as freedom of speech, trade, education, and access to information. India has experienced the highest number of shutdowns globally in recent years, raising concerns about legality, transparency, and constitutional compliance.

FORMS OF SHUTDOWNS

Internet shutdowns can occur in several forms, depending on the scope and technological method used:

a. Complete Shutdowns

Full suspension of internet access in a region, disabling both mobile data and broadband services.

b. Mobile Data Shutdowns

Only mobile internet is disabled, while broadband continues to operate.

c. Throttling

Slowdown of internet speed to such a degree that access becomes practically unusable.

d. Platform Specific Blocking

Blocking of particular applications or platforms such as WhatsApp, Facebook, Telegram, or YouTube.

e. Regional Shutdowns

Suspension limited to sensitive areas such as border districts or conflict zones.

Each form has varying levels of rights impact, but all significantly affect communication flows and democratic participation.

SURVEILLANCE

Surveillance refers to the monitoring, collection, and analysis of personal data, communications, online behaviour, and digital activities by the State. Modern surveillance includes not only interception of calls and messages but also tracking through CCTV networks, facial recognition technology (FRT), spyware, social media monitoring, and metadata analysis. Surveillance is justified by the government on grounds such as national security, crime control, and public order. However, without adequate safeguards, such monitoring may intrude upon privacy, autonomy, and freedom of expression.

TYPES OF SURVEILLANCE

a. Telecommunication Surveillance

Interception of phone calls, SMS messages, and mobile data under Section 5(2) of the Telegraph Act.

b. Digital and Internet Surveillance

Monitoring emails, browsing history, online behaviour, and social media under Section 69 of the IT Act.

c. Metadata Surveillance

Collection of non-content data such as call duration, location, device identifiers, and communication patterns.

d. Biometric and Facial Recognition Surveillance

Use of Aadhaar data, facial recognition systems, and biometric databases to identify individuals.

e. Mass Surveillance Systems

Automated systems such as NATGRID, CMS (Central Monitoring System), and NETRA that monitor vast quantities of digital traffic in real time.

ONLINE CENSORSHIP

Online censorship refers to the blocking, removing, or restricting access to digital content, websites, or social media posts. This includes State-directed removal under Section 69A of the IT Act,[6] social media content takedowns, disabling of accounts, or filtering keywords. Censorship may be justified to prevent hate speech or maintain public order, but vague or broad restrictions lead to arbitrary suppression of dissent, journalism, and artistic expression. The Supreme Court in Shreya Singhal highlighted the need for clarity and due process to prevent misuse.

TOOLS OF DIGITAL CONTROL

Digital restrictions are enabled through various technological and legal mechanisms:

a. Deep Packet Inspection (DPI)

Allows authorities to inspect, block, or filter data packets passing through neBlockin

b. IP and DNS Blocking

Used for blocking websites or platforms at the network level.

c. Kill Switch Mechanisms

Allows the government to entirely disable telecom networks in an area.

d. Facial Recognition and AI Systems

Used for tracking individuals through CCTV surveillance grids and crowd-scanning systems.

e. Social Media Monitoring Cells

State agencies monitor public posts, hashtags, messages, and digital activism.

f. Automated Profiling Systems

[6] Information Technology Act, No. 21 of 2000, § 69A

AI-based tools used to analyse patterns and predict "threat" behaviour.

Collectively, these mechanisms expand the State's ability to control, monitor, and restrict digital communication, raising important constitutional concerns.

CONSTITUTIONAL FRAMEWORK

Key constitutional rights related to Internet freedom in India come from the Constitution of India, specifically Articles 14, 19, and 21 of the Constitution. These three articles provide the fundamental foundation for civil liberties for all people and organisations in India relating to the Internet. The increasing importance of the Internet for free speech, education, economic activity and governance is recognised by several Supreme Court decisions over the past ten years (most notably in the cases of Shreya Singhal vs Union of India, Puttaswamy vs Union of India, and Anuradha Bhasin vs Union of India), which extend the Constitution's protections into cyberspace. In addition to discussing the above rights, this chapter will also look at other relevant constitutional doctrines that govern restrictions on the use of the Internet in India, including the Golden Triangle and the Doctrine of Proportionality.

Article 19: Freedom of Speech and Expression[7]

According to Article 19(1)(a), everyone has the right to express themselves freely; now, this means that you have the right to both share and receive information through the internet as well as across any other digital platform. In Shreya Singhal v. Union of India, the Supreme Court affirmed that all forms of free speech (including speech online) are protected under Article 19. As a result of having an internet shutdown (as was seen in recent events), blocking content and censoring information directly impact on someone's ability to access certain information, communicate with other people and thus participate in a democratic conversation; therefore, any time the State would like to impose a restriction on what a person can find or do online, they must adhere to Article 19(2).

The Supreme Court in Anuradha Bhasin v. Union of India ruled that shutting down the internet indefinitely is unconstitutional; as well, when a state restricts access to the internet, the restrictions must be both necessary and proportionate and reviewed regularly.

[7] Id. art. 19(1)(a)

Article 21: Right to Life and Privacy[8]

The Supreme Court has determined that Article 21 gives rise to rights that include life and liberty, privacy, dignity, access to information, and freedom from arbitrary interference through surveillance. In K.S. Puttaswamy v. Union of India (2017), the Supreme Court expressly recognised the right to privacy as a fundamental right under Article 21. Consequently, the Court held that any action taken by the State, through either the collection of data or through means used for surveillance or electronic media, must therefore comply with the requirements of Article 21.

In addition to their potential to erode the ability of people to exercise their autonomy, many of these technologies have a tendency to create a "chilling" effect on people's ability to express themselves freely. Because of the constraints imposed by Article 21, the State must pursue a fair and lawful process when limiting someone's autonomy. Likewise, in addition to having long-lasting implications for an individual or organisation's ability to earn a living or pursue an education, the decision to shut down the internet can impede the ability of the individual or organisation to maintain optimal health.

Article 14: Equality and Non-Arbitrariness[9]

The right to equality before the law is enshrined in Article 14 of the Indian Constitution and prohibits State action from being arbitrary. Restrictions imposed through digital technology often fail the Article 14 test when they are implemented without transparency, unevenly across geographic areas, or disproportionately impact certain populations (for example: students, other disadvantaged groups and those with lower income levels).

In cases where mass shut downs or blanket surveillance orders have been issued, the Supreme Court has consistently affirmed that arbitrary action is a violation of Article 14. This principle will be a critical vehicle to counter executive overreach in the digital age.

The Golden Triangle (Articles 14, 19, 21)

Together, Articles 14, 19, and 21 form the Golden Triangle, safeguarding equality, freedoms, and personal liberty. Any restriction on the Internet must satisfy all three simultaneously.

For instance, a shutdown order must:

Be non-arbitrary (Article 14), fall under reasonable restrictions (Article 19(2)), and respect

[8] Id. art. 21

[9] India Const. art. 14

procedural fairness and dignity (Article 21).

This doctrine ensures checks and balances when the State exercises its power over digital platforms.

Doctrine of Proportionality

The doctrine of proportionality, reaffirmed in Puttaswamy and Anuradha Bhasin, requires that any restriction on rights must:

1. Pursue a legitimate state aim,
2. Be necessary,
3. Be the least restrictive measure, and
4. Balance individual rights with state interests.

This doctrine is now the central standard for evaluating internet shutdowns, censorship orders, and surveillance frameworks. The State must justify that no milder alternative could achieve the same goal.

STATUTORY & REGULATORY FRAMEWORK

India uses a combination of colonial-era laws and contemporary tech statutes, such as the Telegraph Act 1885, Suspension Rules 2017, IT Act 2000, IT Rules 2021, CrPC, and Aadhaar Act 2016, to regulate internet access, shutdowns, and surveillance. These laws give the State the authority to collect data, verify identity, intercept communications, block content, and suspend internet services. However, there are significant questions regarding privacy, transparency, and constitutional validity raised by their wide and unclear powers. Together, they highlight the need for clearer, rights-protective digital governance.

Indian Telegraph Act, 1885[10]

The Telegraph Act provides the legal basis for the Government to regulate Telecoms in India. Section 5(2) provides for State interception or detention of Messages in the event of a Public Emergency or where there is a need for Public Safety. While it was enacted during Colonial times, today, it remains the primary legislative support of the Government's current strategy of Pimking (internet) shut downs.

Although courts have expressed concerns regarding the lack of procedural safeguards under

[10] The Indian Telegraph Act, No. 13 of 1885, § 5(2).

this authorisation, the current status of the Act continues to provide the basis for any future shutdown until such time as Parliament adopts a modern statute regulating surveillance. The broad terms of this Act gives the executive significant discretionary authority.

Suspension Rules, 2017[11]

The Suspension Rules, or Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017, are the rules established under the Telegraph Act that govern the Temporary Suspension of Telecom Services. These rules state that:

1. Shutdown Orders shall be issued by the Home Secretary.
2. Internet Shutdown Orders shall be temporary in nature.
3. The order shall be reviewed by a Review Committee within five days of completing suspension.
4. Internet Shutdowns shall have to be proportionate to the events leading to the need for suspension.

The state government in Jammu and Kashmir has had several indefinite internet shutdowns, although the AAP (Anuradha Bhasin) sought that the ruling on the constitutionality of Internet Shutdowns be reviewed on a periodic basis and all orders be published; however, implementation of the rulings continue to be inconsistent.

Information Technology Act, 2000[12]

The IT Act governs electronic communication, cybersecurity, intermediaries, and digital offences.

Key provisions include:

Section 69 – government power to intercept, monitor, or decrypt any information,

Section 69A – blocking of websites/content, implemented through secretive orders,

Section 79 – safe harbour protection for intermediaries.

The Act forms the statutory backbone for content takedowns, monitoring, and digital restrictions, but courts have cautioned that these powers must align with Articles 19 and 21.

IT Rules, 2021[13]

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,

[11] Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, Rule 2(1).
[12] Information Technology Act, No. 21 of 2000, § 69.
[13] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3.

2021 increase government control over platforms.

Key features:

1. mandatory traceability of messages for social media platforms,
2. strict content takedown obligations,
3. oversight of digital news and OTT platforms,
4. appointment of grievance and compliance officers.
5. The rules have been challenged for enabling excessive surveillance and undermining privacy, as traceability may break end-to-end encryption.

Criminal Procedure Code (CrPC)

CrPC provisions, such as Sections 91, 92, 93, allow police or courts to demand information, documents, or data from service providers. These are often used during criminal investigations involving digital evidence. CrPC also provides the procedure for search and seizure of electronic devices, though concerns remain about lack of data protection standards and the risk of self-incrimination.

Aadhaar Act, 2016[14]

The Aadhaar Act regulates biometric identification and mandates authentication for various services. While the Supreme Court limited compulsory Aadhaar usage, the system still enables extensive data collection. The Act raises concerns about mass surveillance, centralization of personal data, and potential misuse.

In the digital rights context, Aadhaar's mandatory linking with mobile SIM cards, bank accounts, or welfare schemes has implications for autonomy and informational privacy.

JUDICIAL ANALYSIS

The limits that the Constitution places upon internet shutdowns, surveillance and censorship come from judicial interpretation. These limits are set out by precedent established by the Supreme Court of India, which has consistently held that digital rights are an extension of the fundamental rights guaranteed by the Constitution. The Supreme Court has defined the principles of proportionality, privacy, freedom of expression, due process and accountability as key principles that must guide how the State exercises its powers in an increasingly digital world.

[14] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18 of 2016, Acts of Parliament, 2016 (India).

JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA[15]

The right to privacy was recognized as a fundamental right under Article 21 of the Constitution in the Puttaswamy (2017) judgment. Privacy is defined by the Supreme Court to include informational privacy; data protection; bodily integrity; and autonomy are all aspects of privacy.

Some of the major implications for digital governance include:

- Any surveillance measure must meet the test of legality, necessity, proportionality, and provide for procedural safeguards;
- Mass surveillance or indiscriminate collection of people's personal data is not permissible;
- Citizens have a right to control how their personal data is used.

This judgment will serve as the basis for determining whether surveillance powers provided by the Telegraph Act, IT Act and Aadhaar system are lawful.

SHREYA SINGHAL V. UNION OF INDIA[16]

In the landmark judgment Shreya Singhal v. Union of India (2015), the Supreme Court struck down Section 66A of the Information Technology Act, which made it a crime to post "offensive" messages on the internet. The key contributions of the judgment were:

The Court held that the right to freedom of speech and expression under Article 19(1)(a) of the Indian Constitution extends to the digital medium. The Court held that any limitation on the right to freedom of speech and expression under Article 19(1)(a) must strictly be in accordance with the provisions of Article 19(2) of the Constitution. The Court held that overly vague and broad limitations that result in self-censorship are unconstitutional. The Court established that online speech enjoys the same constitutional protections as offline speech.

ANURADHA BHASIN V. UNION OF INDIA[17]

The Supreme Court of India declared that Internet access is a fundamental right within the ambit of Articles 19(1)(a) and 19(1)(g) of the Constitution of India in the case of Anuradha Bhasin v. Union of India on 10 January, 2020. In addition to defining the scope of a **'RIGHT TO ACCESS THE INTERNET'**, the Court also outlined the constitutional and procedural framework that must be adhered to by the Executive Branch of the Government of India when

[15] 5. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

[16] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (striking down Section 66A IT Act for violating Article 19(1)(a)).

[17] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637

it orders an Internet shutdown. Anuradha Bhasin also reinforced the concept that Internet shutdowns should be based upon the tests of 'necessity' and 'proportionality' and that they must be published. Further, the Court determined that Internet shutdowns cannot be indefinite, and must be periodically reviewed by the Government.

PUCL V. UNION OF INDIA[18]

The Supreme Court of India also ruled on the legality of the Government of India conducting telephone surveillance under the Telegraph Act in 'PUCL v. Union of India' in 1996. The ruling established that telephone surveillance is a serious infringement on an individual's right to privacy and that the Government must follow strict procedures when conducting telephone surveillance, including keeping written records as to why they are conducting the surveillance, and conducting periodic reviews of these records. The judgment created the foundation upon which the Government of India must create and implement due process regarding telephone and digital surveillance.

OTHER RELEVANT CASES

1. Faheema Shirin v. State of Kerala (2019) – Kerala High Court recognized the right to internet access as part of the right to education and privacy.
2. Anvar P.V. v. P.K. Basheer (2014) – established rules for admissibility of electronic evidence, strengthening digital due process.
3. Maneka Gandhi v. Union of India (1978) – though not digital, it expanded Articles 14, 19, and 21 by establishing the “just, fair, and reasonable” standard, now essential for evaluating digital restrictions.
4. Romesh Thappar & Brij Bhushan – early free speech cases that continue to guide internet censorship issues.

INTERNATIONAL HUMAN RIGHTS PERSPECTIVE

The global human rights framework mandates that rights protected offline must equally apply online, shaping standards on internet freedom and digital surveillance. As a signatory to major international instruments, India is expected to align its digital laws with norms under the UDHR, ICCPR, and UN reports. This chapter also draws on comparative developments from jurisdictions like the USA, UK, EU, and South Africa.

[18] PUCL v. Union of India, (1997) 1 SCC 301

Universal Declaration of Human Rights (UDHR)[19]

The UDHR (1948) articulates foundational rights that directly apply to the digital sphere.

Article 19 guarantees freedom of opinion and expression, including the right to "seek, receive and impart information" through any medium.

Article 12 protects against arbitrary interference with privacy, reputation, or correspondence.

The principles of UDHR have guided global debates on internet shutdowns and state surveillance. Shutdowns infringe the right to receive information, while unwarranted surveillance violates privacy and personal autonomy.

International Covenant on Civil and Political Rights (ICCPR)[20]

India is a party to the ICCPR, which provides binding obligations.

Key provisions include:

Article 17 – protection from arbitrary or unlawful interference with privacy and correspondence,

Article 19 – freedom of expression subject only to restrictions that are necessary and proportionate,

Article 21 & 22 – freedom of assembly and association, which can be restricted only under strict conditions.

The UN Human Rights Committee has repeatedly clarified that internet restrictions must meet tests of legality, legitimate aim, and necessity, aligning closely with Indian constitutional doctrine.

UN Special Rapporteur Reports

The UN Special Rapporteur on Freedom of Expression (David Kaye and Irene Khan) has issued landmark reports condemning internet shutdowns and excessive surveillance.

Major observations include:

blanket internet shutdowns are inherently disproportionate, states must ensure transparency and judicial oversight for surveillance orders, encryption is essential for privacy and should not be weakened through traceability mandates, censorship must be narrowly tailored and consistent with democratic standards. These reports carry persuasive value in domestic courts and policy-making.

[19] Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/810 (1948).
[20] International Covenant on Civil and Political Rights art. 19, Dec. 16, 1966, 999 U.N.T.S. 171.

Comparative Study

United States

The US Constitution's First Amendment robustly protects online speech. Surveillance is primarily regulated under the Foreign Intelligence Surveillance Act (FISA). Courts emphasize due process and judicial authorization.

United Kingdom

The UK follows the Investigatory Powers Act 2016, which requires warrants, oversight commissioners, and proportionality in surveillance activities. While criticized, it still provides clearer safeguards compared to India's Telegraph Act.

European Union (EU)

The EU's approach is guided by the GDPR, European Convention on Human Rights (ECHR), and rulings of the European Court of Human Rights (ECtHR). The EU strongly prioritizes data protection, transparency, and minimal interference.

South Africa

The South African Constitution explicitly includes the rights to dignity, freedom of expression, and privacy. The RICA Act was amended after court rulings to include stricter safeguards for surveillance and metadata collection.

Through these global perspectives, it is clear that international human rights standards emphasize necessity, proportionality, judicial oversight, and transparency. These principles are directly relevant to India's ongoing legal reforms on internet shutdowns, censorship, and surveillance.

IMPACT ANALYSIS

Internet shutdowns, surveillance systems, and other forms of online censorship translate into far-reaching human, economic, educational, and democratic impacts in India.

Free speech, access to information, and online participation are directly connected with human rights. Shutdowns mute dissent, prevent communication during crises, and disrupt public debate. The practice of surveillance serves to weaken a right to privacy, creates fear, and discourages free expression. Rights regarding movement, association, and access to legal remedies are also hampered since many essential civic functions depend on online platforms.[21]

The economic impact is severe. During shutdowns, the big losers are India's e-commerce,

[21] Internet Freedom Foundation, Internet Shutdowns in India: Trends and Analysis, https://internetfreedom.in.

financial services, banking, logistics, and small businesses operating online. The most affected are local traders, who rely heavily on UPI and social media marketing. Frequent restrictions create uncertainty for investors and bring down digital-market confidence.

Education is disrupted because students can no longer access classes, exams, and other study materials online. Finally, shutdowns affect rural and marginalized learners disproportionately, which causes the digital divide to perpetuate. Education institutions' surveillance also puts a child's privacy and self-determination at stake.

Shutdowns hamper transparency, participation, and access to news, weakening democracy and governance. Censorship and surveillance engender fear, suppress criticism, and undermine confidence in institutions.

Overall, digital restrictions harm fundamental freedoms, development, and democratic functioning, and this necessitates a much stronger reinforcement of its legal safeguarding.[22]

CRITICAL ANALYSIS

The structural weaknesses in India's digital governance framework, spanning shutdowns, surveillance, and censorship, are striking. The misuse of powers arises from the issuance of shutdown and censorship orders that appear to be without due cause, often by way of executive directions rather than judicial oversight. A general lack of transparency has been reported; very few shutdown orders and surveillance authorizations are published, even when publication is statutorily required. Oversight bodies are dominated by executive officials and tend to be relatively weak.[23]

Expanding facial recognition, social media monitoring, and large-scale databases significantly heighten privacy risks. These enable mass and metadata surveillance in clear violation of the principles laid down in Puttaswamy. Integration of databases further increases the risk of profiling without sufficient safeguards.

It creates new forms of arbitrary governance through technological control: automated censorship, algorithmic filtering, and predictive policing. Finally, legal loopholes such as reliance on an outdated law like the Telegraph Act and weak IT Rules oversight leave citizens vulnerable.

Overall, digital restrictions in India work with disproportionate executive powers and limited

[22] Access Now, #KeepItOn Shutdown Tracker Report (2022) https://www.accessnow.org.
[23] U.N. Human Rights Council, Report on Internet Shutdowns, U.N. Doc. A/HRC/47/35 (2021).

constitutional checks.

SUGGESTIONS & REFORMS

1. Enact a comprehensive surveillance law with clear definitions, judicial pre-approval, a ban on mass surveillance, and an independent oversight authority.
2. Strengthen the internet shutdown framework by requiring judicial approval, publishing shutdown orders, limiting duration, and ensuring periodic reviews as per Anuradha Bhasin.
3. Reform the IT Act and IT Rules 2021 to restrict executive discretion, narrow takedown powers, protect encryption, and ensure independent grievance redressal.
4. Strengthen data protection measures by enforcing data minimization, restricting government exemptions, and regulating Puttaswamy-aligned biometric systems.
5. Make sure there is more transparency through independent audits, annual reports, and the disclosure of censorship justifications.
6. Improve digital rights literacy and judicial capacity to strengthen democratic oversight.
7. Maintain a balanced approach that protects national security without compromising constitutional freedoms.

CONCLUSION

How India regulates internet access, conducts surveillance, and secures digital rights has reached an important juncture, wherein constitutional freedoms need to be safeguarded without eroding legitimate State interests. The strong rights-based foundation built on Articles 14, 19, and 21 and leading judgments such as Puttaswamy, Anuradha Bhasin, Shreya Singhal, and PUCL is still offset by the overbroad powers and weak safeguards that exist in extant laws like the Telegraph Act, Suspension Rules 2017, IT Act 2000, IT Rules 2021, and Aadhaar Act. International best standards from the UDHR and ICCPR, as well as global best practices, attach great importance to oversight, transparency, and data protection in digital governance. What is required to protect digital freedoms in India is a rights-centered approach based on proportionality, accountability, and independent oversight. Strengthening legal frameworks by adopting privacy-focused policies ensures a secure, open, and democratic digital society.

BIBLIOGRAPHY

BOOKS

1. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (Basic Books 1999).
2. RICHARD A. POSNER, NOT A SUITABLE CASE FOR TREATMENT: SURVEILLANCE AND PRIVACY (Oxford Univ. Press 2008).
3. GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS (Oxford Univ. Press 2014).
4. ANDREW MURRAY, INFORMATION TECHNOLOGY LAW (Oxford Univ. Press 4th ed. 2019)

JOURNAL ARTICLES

1. Apar Gupta, Internet Shutdowns and the Constitution, 12(3) NUJS L. Rev. 523 (2020).
2. Gautam Bhatia, State Surveillance and the Right to Privacy, 31 Nat'l L. Sch. India Rev. 1 (2019).
3. Vrinda Bhandari & Renuka Sane, Regulating Digital Privacy in India, 54 Econ. & Pol. Wkly. 30 (2019).
4. Usha Ramanathan, Aadhaar: Constitutional Complications of a Digital ID System, 50 Econ. & Pol. Wkly. 35 (2015).

CASE LAW

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
2. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
3. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
4. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (Telephone Tapping Case).

WEBSITES & ONLINE RESOURCES

1. Internet Freedom Foundation, Internet Shutdowns in India, https://internetfreedom.in.
2. Software Freedom Law Center, Surveillance Law Compendium, https://sflc.in.
3. UN Human Rights Office, Digital Rights & Online Freedoms, https://ohchr.org.