SOCIAL MEDIA REGULATION AND THE RULE OF LAW

Key Trends in Sri Lanka, India and Bangladesh

KONRAD ADENAUER STIFTUNG

CLJ

SOCIAL MEDIA REGULATION AND THE RULE OF LAW

Key Trends in Sri Lanka, India and Bangladesh

KONRAD ADENAUER STIFTUNG

CLJ

ISBN: 978-967-457-193-1

Published by:

CLJ Malaysia Sdn. Bhd.
(formerly known as The Malaysian Current Law Journal Sdn Bhd)
Unit E1-G, Jalan Selaman 1,
Dataran Palma, 68000 Ampang,
Selangor Darul Ehsan, Malaysia.
Co No 197901006857 (51143 M)
Tel: 603-42705400 Fax: 603-42705401

Printed by:
Perniagaan E.B.K.
No. 20, Taman Mas Satu, Batu 9 Cheras,
43200, Kajang, Selangor, Malaysia.


॥न्यायस्तत्र प्रमाणं स्यात्॥
DELHI
CENTRE FOR
COMMUNICATION
GOVERNANCE


LIRNEasia
Pro-poor. Pro-market.


BRAC
UNIVERSITY
Inspiring Excellence

AUTHOR INFO

This report was authored by the Centre for Communication Governance at National Law University Delhi (CCG), LIRNEasia and BRAC University with guidance from Konrad-Adenauer-Stiftung (KAS). The report was conceptualised by Gunjan Chawla, former Programme Manager at CCG and Jhalak M. Kakkar, Executive Director at CCG, in collaboration with KAS.

Research and Writing Team

Centre for Communication Governance at National Law University Delhi: Tavishi, Archit Lohani, Sidharth Deb;

LIRNEasia: Helani Galpaya, Ramathi Bandaranayake, Ashwini Natesan, Chiranthi Rajapakse;

BRAC University: Md Saimum Reza Talukder, K Shamsuddin Mahmood.

Editing

Sachin Dhawan, Jhalak M. Kakkar, Tavishi, Archit Lohani

Review

Sachin Dhawan, Jhalak M. Kakkar

Copy Editing

Ameya Naik

Research Assistants

Anha Adhlee, Athira Johny, Hannaan Kirmani, Ishita Tulsyan, Mosabbir Hossain, Nafisa Tabassum, Raihan Rahman.

Table of Contents

Note to the Reader

In an increasingly digital world, where social media platforms serve as avenues for communication and connection, social media regulation represents a focal point for the preservation of the rule of law.

Through comprehensive analysis, this report aims to shed light on the critical role social media platforms play in national security and how human rights, including free speech and privacy protection, are being overstepped by Internet shutdowns, online content blocks and control of the information flow. By examining legislative frameworks and enforcement mechanisms, this report provides a holistic understanding of the efforts undertaken, but also further recommendations to safeguard cyberspace and regulate social media platforms.

This report delves into the landscapes of three South Asian countries – India, Sri Lanka and Bangladesh – each with its own set of challenges and opportunities concerning cybersecurity and social media regulation. India, with its burgeoning tech industry and vast online population, navigates the delicate balance between innovation and security. Sri Lanka grapples with the aftermath of social media's role in recent political upheavals, highlighting the urgent need for robust regulations. Bangladesh, on its journey towards digital transformation, faces evolving threats to its cybersecurity infrastructure amidst rapid technological advancements.

These three countries, sharing the same borders, are influencing each other in the shaping of their cybersecurity and social media platforms regulation, which makes this report a relevant vehicle for a comparative analysis on those issues.

The KAS Rule of Law Program Asia's commitment to promoting the rule of law underscores the importance of ensuring that legal frameworks governing cyberspace and social media platforms uphold principles of accountability, transparency, and inclusivity.

The KAS Rule of Law Program Asia extends its gratitude to the Centre for Communication Governance (CCG),National Law University Delhi (NLUD), LIRNEasia from Sri Lanka and BRAC University from Bangladesh, for their invaluable work making this research endeavour possible.

We indeed appreciate the guidance and mentorship provided by the NLUD's Vice Chancellor, Prof. (Dr.) G. S. Bajpai, and the dedicated efforts of the Registrar, Prof. (Dr.) Ruhi Paul, Dr. Daniel Mathew, Faculty Director at NLUD's Centre for Communication Governance (CCG) and Jhalak M. Kakkar, Executive Director at CCG. Special thanks to Sachin Dhawan, Archit Lohani and Tavishi, researchers at CCG, for their invaluable drive in taking the lead on this research endeavour, as well as the ever-present Suman Negi and Preeti Bhandari for their unending support.

We also express our gratitude to the LIRNEasia team, namely Helani Galpaya, Ramathi Bandaranayake, Ashwini Natesan and Chiranthi Rajapakse, for their efforts and precious insights about Sri Lanka's landscape on social media platforms regulation.

On the BRAC University side, we are thankful for Md Saimum Reza Talukder and K. Shamsuddin Mahmood's engagement and collaboration in uncovering Bangladesh' trends and legal challenges.

We finally extend our gratitude to Dr. Karthik Nachiappan for generously dedicating his time and expertise to offer valuable feedback, significantly enhancing the overall quality and rigour of the report. Last but not least, we are thankful to Aishwarya Natarajan for initiating this collaborative effort on KAS' side, laying the groundwork for insightful research and meaningful discourse.

We hope that this report serves as a catalyst for meaningful dialogue, policy reform, and collaborative action aimed at strengthening the rule of law in the region and beyond.

Stefan Samse
Director of the KAS Rule of Law Program Asia

Olivia Schlouch
Program Manager, KAS Rule of Law Program Asia

Singapore, May 2024

About the National Law University, Delhi

The National Law University Delhi is one of the leading law universities of India based in the capital city of India. Established in 2008 (by Act. No. 1 of 2009), the University is ranked second in the National Institutional Ranking Framework for the last five years. Dynamic in vision and robust in commitment, the University has shown terrific promise to become a world-class institution in a very short span of time. It follows a mandate to transform and redefine the process of legal education. The primary mission of the University is to create lawyers who will be professionally competent, technically sound and socially relevant, and will not only enter the Bar and the Bench but also be equipped to address the imperatives of the new millennium and uphold constitutional values.

The University aims to evolve and impart comprehensive and interdisciplinary legal education which will promote legal and ethical values, while fostering the rule of law. The University offers a five-year integrated B.A., LL.B (Hons.) and one-year postgraduate masters in law (LL.M), along with professional programs, diploma and certificate courses for both lawyers and non-lawyers. The University has made tremendous contributions to public discourse on law through pedagogy and research.

Over the last decade, the University has established many specialised research centres and this includes the Centre for Communication Governance, the Centre for Innovation, Intellectual Property and Competition, the Centre for Corporate Law and Governance, the Centre for Criminology and Victimology, and Project 39A. The University has made submissions, recommendations, and worked in advisory/consultant capacities with government entities, universities in India and abroad, think tanks, private sector organisations, and international organisations. The University works in collaboration with other international universities on various projects and has established MoU's with several other academic institutions.

About the Centre for Communication Governance

The Centre for Communication Governance at the National Law University Delhi (CCG) was established in 2013 to ensure that Indian legal education establishments engage more meaningfully with information technology law and policy and contribute to improved governance and policy making. CCG is the only academic research centre dedicated to undertaking rigorous academic research on information technology law and policy in India. It has in a short span of time, become a leading institution in Asia. Through its academic and policy research, CCG engages meaningfully with policy-making in India by participating in public consultations, contributing to parliamentary committees and other consultation groups, and holding seminars, courses and workshops for capacity building of different stakeholders in the technology law and policy domain. CCG works across issues such as privacy and data governance, platform governance, and emerging technologies.

CCG has built an extensive network and works with a range of international academic institutions and policy organisations. These include the United Nations Development Programme, Law Commission of India, NITI Aayog, various Indian government ministries and regulators, International Telecommunications Union, UNGA WSIS, Paris Call, Berkman Klein Center for Internet and Society at Harvard University, the Center for Internet and Society at Stanford University, Columbia University's Global Freedom of Expression and Information Jurisprudence Project, the Hans Bredow Institute at the University of Hamburg, the Programme in Comparative Media Law and Policy at the University of Oxford, the Annenberg School for Communication at the University of Pennsylvania, the Singapore Management University's Centre for AI and Data Governance, and the Tech Policy Design Centre at the Australian National University.

The Centre has authored multiple publications over the years, including the Hate Speech Report, a book on Privacy and the Indian Supreme Court, an essay series on Democracy in the Shadow of Big and Emerging Tech, a comprehensive report on Intermediary

Liability in India, an edited volume of essays on Emerging Trends in Data Governance, and most recently a guide for Drafting Data Protection Legislation: A Study of Regional Frameworks in collaboration with the United Nations Development Programme. It has also published reports from the first two phases of the Blockchain Project conducted in collaboration with the Tech Policy Design Centre at the Australian National University, which maps the blockchain ecosystem in India and Australia.

Privacy and data protection have been focus areas for CCG since its inception, and the Centre has shaped discourse in this domain through research and analysis, policy inputs, capacity building, and related efforts. In 2020, the Centre launched the Privacy Law Library, a global database that tracks and summarises privacy jurisprudence emerging in courts across the world, in order to help researchers and other interested stakeholders learn more about privacy regulation and case law. The PLL currently covers 250+ cases from 20+ jurisdictions globally and also contains a High Court Privacy Tracker that tracks emerging High Court privacy jurisprudence in India.

CCG also has an online 'Teaching and Learning Resource' database for sharing research-oriented reading references on information technology law and policy. In recent times, the Centre has also offered Certificate and Diploma Courses on AI Law and Policy, Technology Law and Policy, and First Principles of Cybersecurity. These databases and courses are designed to help students, professionals, and academicians build capacity and ensure their nuanced engagement with the dynamic space of existing and emerging technology and cyberspace, their implications for society, and their regulation. Additionally, CCG organises an annual International Summer School in collaboration with the Hans Bredow Institute and the Faculty of Law at the University of Hamburg in collaboration with the UNESCO Chair on Freedom of Communication at the University of Hamburg, Institute for Technology and Society of Rio de Janeiro (ITS Rio) and the Global Network of Internet and Society Research on contemporary issues of information law and policy.

ccgdelhi.org | privacylibrary.ccgnlud.org | ccg@nludelhi.ac.in | X: @CCGNLUD

About LIRNEasia

LIRNEasia is an independent, regional, digital policy think tank working across the Asia Pacific since 2004. Its mission is *"Catalysing policy change and solutions through research to improve the lives of people in the Asia and Pacific using knowledge, information and technology"*.

LIRNEasia conducts in-depth, policy-relevant research on infrastructure industries, including the digital sector. As such, LIRNEasia's work often extends to areas such as labour, education, agriculture, disability, social welfare and other sectors that can be improved through the information and knowledge that is created and disseminated with the use of digital technology. Given the importance of global digital platforms in facilitating expression and commerce, much of LIRNEasia's work has revolved around the governance of these platforms. This work involves exploring the emerging data governance policy architecture across Asia and proposing models of data sharing and algorithmic transparency and accountability. Platform, data and algorithmic governance focuses on balancing inclusive and sustainable economic growth with the protection of human rights.

LIRNEasia's current work on data governance policy includes studying the data policy ecosystems in South and Southeast Asia, taking into account both formal policy and law as well as informal practice and norms. The research aims to create and mobilise new knowledge about tensions, gaps, and the evolution of the data policy ecosystems in seven selected countries (Sri Lanka, India, Pakistan, Indonesia, Nepal, Thailand and the Philippines). The project also aims to expand the community of practice of Asian Data for Development practitioners and enhance the capacity of actors to participate in policy-making processes and evidence-based policy influence related to data.

Going beyond policy and legal analysis, the LIRNEasia team also develops practical tools that could result in better-governed or used technology. Natural Language Processing (NLP) is used to identify hate speech at scale in resource-poor languages (e.g. Sinhala, Bengali), while tools for fact-checkers help identify how claims in narratives are developed.

LIRNEasia is currently conducting natural experiments and systematically evaluating the effectiveness of different counter-measures, such as fact-checking and digital literacy programs that are aimed at fighting the challenges of dis/misinformation. Qualitative and quantitative methods are also being used to understand the human factors that contribute to the likelihood to believe misinformation among adolescents and adults. This work stems from a previous report ("Meeting the Challenges of the Information in the Global South" authored by LIRNEasia together with researchers from Africa, Latin America and the Middle East) that showed that few fact-checkers and digital literacy program creators understand the impact of their actions.

LIRNEasia recognizes that while platform use is increasing, and the challenges of competition and dis/misinformation are increasing, all this is taking place in a context of low skill and low connectivity in Asia (when compared to the Global North and South America). LIRNEasia's quantitative surveys quantify the level of digital access, use and skill while qualitative research describes the reasons for such relatively low access, use and skill among people of emerging Asia. These 'demand side' data and insights are combined with 'supply side' analysis of the regulatory environment and market conditions to propose solutions that enable meaningful digital access to all in the region.

LIRNEasia engages directly and indirectly with policy actors in taking its research into the public sphere. It provides policy analysis assistance as well as capacity building for policymakers and practitioners (including civil society and private sector solution providers) in the region.

More details of LIRNEasia's research in different areas can be found at lirneasia.net

About BRAC University

Founded in 2004, the **School of Law** at BRAC University is a gateway through which students are prepared for careers in law, administrative services, the judiciary, and the development sector. The four-year undergraduate program at the School of Law culminates in a **Bachelor of Laws (LL.B.)** degree for successful students. Although the program's primary emphasis is on law and the legal profession, given that Law is also intertwined with economics, development, business, technology, philosophy, and sociology, it also prepares students inclined to seek professions in other disciplines.

The faculties of the School of Law are handpicked for their academic excellence and individual expertise. They bring teaching-learning experiences from Universities in the United Kingdom, Australia, Russia, Netherlands, Sweden, the United States of America, and Bangladesh. The faculty has individual expertise in the areas of child rights, criminal law, consumer laws, gender studies, business laws, economics, cyber law, intellectual property rights, international laws, and human rights, all of which are shared with the students in coursework, workshops and lecture programs organized by the school.

As a thriving knowledge-based educational institution, the School of Law believes in global knowledge exchange to create an open, peaceful, and rights-based society. Since 2021, students and faculty members of the School of Law have been engaged in various student and faculty exchange programs and action research supported and facilitated by the **Open Society University Network (OSUN)**.

The School of Law is also noteworthy for its **BRAC University Law Society (BULS)**, where students are constantly preparing for moot court competitions, writing research papers and articles for the **BULS** newsletter '**Acumen**,' regular court visits, conducting seminars and workshops, and social awareness activities including street lawyering and legal awareness campaigns. The mooters of BULS have been successful in several national and international competitions, including the prestigious **Philip C. Jessup International Law Moot Court Competition** and **ICRC Henry Dunant Moot Court Competitions**.

Recognizing BRAC's background and the goals and commitments of BRAC University, the School of Law endeavors to impart legal education to seek legal solutions that respect people's social, cultural, and aesthetic needs. To meet this goal, it strives to impart to its students the tenets of the law and legal philosophy, rights-based issues, and a broader awareness of their society. Graduates from the School of Law are now pursuing careers as lawyers, judges, corporate legal officers, development workers, human rights defenders, and academics.

List of Abbreviations

API	Application Programming Interface
BASL	The Bar Association of Sri Lanka
BCC	Bangladesh Computer Council
BGD e-GOV CIRT	Bangladesh e-Government Computer Incidents Response Team
BSTI	Bangladesh Standards and Testing Institution
BTRC	Bangladesh Telecommunication Regulatory Commission
C&IS	the Cyber and Information Security
CAT	Cyber Appellate Tribunals
CBI	Criminal Bureau of Investigation
CCA	Controller of Certifying Authorities
CERT-In	Computer Emergency Response Team of India
CGS	Centre for Governance Studies
CIA	Central Intelligence Agency
CIA triad	Confidentiality, Integrity, Accessibility
CIB	Coordinated Inauthentic Behaviour
CID	Police and the Criminal Investigation Department
CIIs	Critical Information Infrastructures
CNNI	Critical National Information Infrastructure
COVID-19	Severe Acute Respiratory Syndrome Coronavirus 2
CPJ	Committee to Protect Journalists
CTTC	Counter Terrorism and Transnational Crime
DIG	Deputy Inspector General
DIPA	Digital Infrastructure Protection Agency of Sri Lanka
DoT	Department of Telecom
DPA	Data Protection Authority
E2EE	End-to-end encryption
ERT	Emergency Response Team

FBI	Federal Bureau of Investigation
FIDH	International Federation for Human Rights
FMM	The Free Media Movement of Sri Lanka
FOTN	Freedom on the Net
GAC	Grievance Appellate Committee
HRCSL	The Human Rights Commission of Sri Lanka
I4C	Indian Cyber Crime Coordination Centre
ICNL	International Center for Not-for-Profit Law
ICT	Information Communication and Technology
ICTA	Information and Communication Technology Agency
ICTD	Information and Communication Technology Division
IO	Information Officer
ISEA	Information Security Education & Awareness
ISO	International Organization for Standardization
ISP	Internet Service Provider
LEAs	Law Enforcement Authorities
LGBTQ	Lesbian, Gay, Bisexual, Transgender, and Queer
LICT	Leveraging ICT for Growth, Employment, and Governance
LTTE	Liberation Tigers of Tamil Eelam
MeitY	Ministry of Electronics and Information Technology
MHA	Ministry of Home Affairs
MIB	Ministry of Information and Broadcasting
MLA	Minister of Legislative Assembly
MLATs	Mutual Legal Assistance Treaties
MoU	Memorandum of Understanding
MPs	Members of Parliament
NCB	National Crime Records Bureau
NCIIPC	National Critical Information Infrastructure Protection Centre
NCRF	National Cyber Security Reference Framework
NCSC	National Cyber Security Coordinator

NGO	Non-Governmental Organization
NISPG	National Information Security Policy and Guidelines
OTT	Over-the-top media service
PA	Public Authority
PSU	Public Sector Unit
RTIC	Right to Information Commission
SCO	Shanghai Cooperation Organization
SLCERT	Sri Lanka Computer Emergency Readiness Team
SLPI	Sri Lanka Press Institute
SLPP	Sri Lanka Podujana Peramuna
SMIs	Social Media Intermediaries
SSMIs	Significant Social Media Intermediaries
TID	Terrorism Investigation Division
TRAI	Telecom Regulatory Authority of India
TRCSL	Telecommunications Regulatory Commission of Sri Lanka
UN	United Nations
URL	Uniform Resource Locator
VPN	Virtual Private Network
WHO	World Health Organization

List of Statutes

India	
Blocking Rules	Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009
CERT Rules	Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013
CrPC	Code of Criminal Procedure 1973
DMA	Disaster Management Act 2005
DPDPA	Digital Personal Data Protection Act 2023
FCRA	Foreign Contribution Regulation Act 2010
Interception Rules	Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009
Intermediary Guidelines	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
IPC	Indian Penal Code 1860
IT Act	Information Technology Act 2000
NCII Rules	Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules 2013
NCSP	National Cyber Security Policy 2013
POCSO	Protection of Children from Sexual Offences Act 2012
SPDI Rules	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

Telecom Bill	Indian Telecommunication Bill 2022
Telecom Rules	Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017
Telegraph Act	Indian Telegraph Act 1885
Sri Lanka	
ATA	Anti Terrorism Bill (ATA) 2023
CCA	Computer Crime Act No. 24 of 2007
Cybersecurity Bill	Cyber Security Bill 2023
Emergency Regulations	Emergency (Miscellaneous Provisions and Powers) Regulations, No. 1 of 2022
ETA	The Electronic Transactions Act (2006)
ICCPR Act	International Covenant on Civil and Political Rights Act No. 56 of 2007
MACMA	Mutual Assistance in Criminal Matters Act 2002
OSB	Online Safety Bill 2023
PDPA	Personal Data Protection Act No. 9 of 2022
Penal Code	Penal Code Ordinance No 11 of 1887
Police Ordinance	Police Ordinance No 16 of 1865
PSO 1947	Public Security Ordinance No 25 of 1947
PTA	Prevention of Terrorism Act of 1979
Public Security Ordinance	Public Security Ordinance No. 25 of 1947
RTI Act	Right to Information Act No. 12 of 2016
SLTA	Sri Lanka Telecommunications Act No 25 of 1991
Bangladesh	
ATA	Anti-Terrorism Act 2009
BLI Act	Bengali Language Implementation Act, 1987
Penal Code	Bangladesh Penal Code 1860
BTA	Bangladesh Telecommunications Act 2001
CSA	Cyber Security Act 2023

DPA	Draft Data Protection Act 2022
Draft OTT Policy	Regulation for Digital, Social Media, and OTT Platforms 2021
Draft Cybersecurity Strategy	Draft Cybersecurity Strategy 2021-2025
DSA	Digital Security Act 2018
ICTA	Information and Communication Technology Act 2006
National Cyber Security Strategy	National Cyber Security Strategy 2014
TCD Act	Torture and Custodial Death (Prevention) Act of 2013
Other Jurisdictions	
CDA	US Communication Decency Act 1996
DMA	EU's Digital Markets Act 2022
GDPR	EU's General Data Protection Regulation 2016
NetzDG	Germany's Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) 2017.
Online Safety Act	UK's Online Safety Act 2023
POFMA	Singapore's Protection from Online Falsehoods and Manipulation Act 2019
Removal and Blocking Rules	Pakistan's Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021

List of Cases

India

Tanul Thakur case, W.P.(C) 13037/2019 & CM No. 53165/2019

Anuradha Bhasin case, W.P. (C) No. 1031 of 2019

Shreya Singhal v Union of India 2015 (5) SCC 1 [121]

KS Puttaswamy v Union of India (2017) 10 SCC 1, AIR 2017 SC 4161

Shayara Bano v Union of India, WP (C) 118/2016

Indra Nehru Gandhi V Raj Narayan, (1975 AIR 2299, 1976 (2) SCR 347)

Kesavananda Bharati v State of Kerala (AIR 1973 SC 1461)

Maneka Gandhi v Union of India, 1978 AIR 597

Modern Dental College and Research Centre v State of Madhya Pradesh, (2016) 7 SCC 353

Skand Bajpai v Union of India WP (C) 799 of 2020 (Supreme Court of India, 9 May 2022)

Press Trust of India Limited v Union of India WP (C) 6188 of 2021 (High Court of Delhi)

Foundation for Independent Journalists v Union of India WP (C) 3125 of 2021 (High Court of Delhi)

The Leaflet (Nineteen One Media Pvt Ltd) v Union of India WPL 14172 of 2021 (High Court of Bombay)

Quint Digital Media Ltd v Union of India WP (C) 3659 of 2021 (High Court of Delhi); Pravda Media Foundation v Union of India WP (C) 5973 of 2021 (High Court of Delhi)

News Broadcasters Association v Ministry of Electronics and Information Technology WP (C) 13675 of 2021 (High Court of Kerala)

Truth Pro Foundation of India v Union of India WP (C) 6941 of 2021 (High Court of Karnataka)

Digital News Publishers Association v Union of India WP (C) 13055 of 2021 (High Court of Madras)

Nikhil Wagle v Union of India PIL (L) 14204 of 2021 (High Court of Bombay)

Indian Broadcasting & Digital Foundation v Ministry of Electronics and Information Technology WP 25619 of 2021 (High Court of Madras)

LiveLaw Media Pvt Ltd v Union of India WP (C) 6272 of 2021 (High Court of Kerala)

Sanjay Kumar Singh v Union of India WP (C) 3483 of 2021 (High Court of Delhi)

Uday Bedi v Union of India WP (C) 6844 of 2021 (High Court of Delhi)

Praveen Arimbrathodiyil v Union of India WP (C) 9647 of 2021 (High Court of Kerala)

TM Krishna v Union of India WP (C) 12515 of 2021 (High Court of Madras)

Sayanti Sengupta v Union of India WPA (P) 153 of 2021 (High Court of Calcutta)

Nikhil Wagle v Union of India PIL (L) 14204 of 2021 (High Court of Bombay)

Facebook Inc v Union of India WP (C) 7281 of 2021 (High Court of Delhi)

WhatsApp LLC v Union of India WP (C) 7284 of 2021 (High Court of Delhi)

UTV Software Communications Ltd v 1337x CS (Comm) 724 of 2017 (High Court of Delhi, 10 April 2019)

Kent RO Systems Ltd v Amit Kotak 2017 SCC OnLine Del 7201

Myspace Inc v Super Cassettes Industries Ltd 2016 SCC OnLine Del 6382

Dept of Electronics and Information Technology v Star India Pvt Ltd FAO (OS) 57 of 2015 (High Court of Delhi, 29 July 2016)

Facebook Inc v Union of India TP (C) 1943-46 of 2019 (Supreme Court of India, 24 September 2019)

Srilanka

Kodeeswaran v. Attorney General (1969) 72 NLR 337

Sunila Abeysekera v. Ariya Rubasinghe Competent Authority and Others [2000] SLR 1V3141

Amalini De Sayrah v. Sri Lanka Computer Emergency Readiness Team RTIC Appeal (In-Person)/981/19

Raisa Wickrematunga v. TRCSL RTIC Appeal (In person)/106/2018

Queen v Liyanage and Others (1962) 64 NLR 313

R Sampanthan and Ors v AG and Ors [1965] 68 NLR 265

J S Tissainyagam High Court case No 4425/2008

Bangladesh

Bangladesh v Bangladesh Legal Aid Services Trust (2008) 8 SCOB 1

Mohammed Shamsuddin v. SS Wijesinha, [1967] 3 WLR 1460 (PC)

Corporation of the City of Enfield v Development Assessment Commission (2000) 199 CLR 135, 157

Bangladesh Legal Aid and Services and Trust and Others vs. Bangladesh and Others (Writ Petition No. 3806 of 1998)55 DLR (2003) 363

Executive Summary

This report maps the social media regulatory framework[1] across Sri Lanka, India, and Bangladesh. It focuses on (a) the intermediary liability framework governing social media platforms; (b) the relevant cybersecurity and other information and communication technology (ICT) regulations; and (c) key speech laws (mostly penal) applicable to end-users. In order to understand key trends emerging from the development and implementation of the social media regulatory frameworks, we benchmark social media regulation against the principles of rule of law.

It is observed that social media governance across all three jurisdictions often manifests as regulation of the online information ecosystem. This is operationalised through the following key mechanisms:[2]

- **Internet shutdowns:** Internet shutdowns refer to actions taken by a government to intentionally disrupt access to information and communications systems online, by either blocking or slowing down entire communication networks (or parts of such networks).
- **Blocking content on social media:** Blocking specific pieces of content hosted on social media; this implies a content blocking or removal order by the executive for the purposes of this report.
- **Law enforcement access to user data:** Law enforcement agencies (LEAs) access citizen data stored with the intermediaries for the purposes of investigation of crime; they may also proactively monitor public data across platforms to build intelligence.
- **Criminalisation of online speech:** Various penal laws and online speech offences aim to curtail the misuse of online expression for unlawful purposes.

1 Note that we use the term "regulate" to broadly mean any actions taken to govern or influence the way in which social media platforms are operated as well as, used and accessed. It consists of regulation that is directed at (a) social media platforms as intermediaries; (b) other intermediaries like ISPs; and (c) end users.

2 While internet shutdowns, law enforcement access to user data, and criminalisation of speech are being employed across all three jurisdictions, state blocking of targeted content on social media is absent in Sri Lanka at the time of writing. However, this is set to change if the Online Safety Bill, 2023 is enacted.

The report also examines the frequent mobilisation of such tools and processes with the justification of state security imperatives.[3] While addressing state security concerns is important, it must be done so in balance with constitutional rights and rule of law principles. The pursuit of state security objectives often conflicts with citizens' civil liberties, creating a complex dynamic with far-reaching implications for the democratic rule of law.

Some key observations from the report:

- Bangladesh and India have conditional exemptions of liability for third-party content hosted by intermediaries. However, emerging legislative developments point towards a weakening of safe harbour protection. On the other hand, Sri Lanka does not have an exemption framework for intermediaries at the time of writing and has relied on licensing agreements with ISPs to block social media platforms in emergencies.[4]
- The centralisation of power with the executive is observed in all three countries. The regulatory frameworks lack the necessary and effective judicial and parliamentary oversight over blocking orders, internet suspensions, and user data requests.
- Censorship based on state security imperatives has resulted in the restriction of legally permissible speech in all three countries, highlighting the impact of overbroad and vague language used to codify online and general speech-related offences.
- The centralisation of power with the executive has resulted in a lack of transparency and accountability of government actions. This is often justified on the basis of state security.

To effectively address these concerns and establish a rights-respecting, transparent and accountable framework for regulating social media platforms, we recommend:

- **Precise Definitions and Narrow Scope:** Adopt precise and narrow definitions of online harms and limit national security exceptions to reduce discretion and arbitrariness in enforcement.

3 For the purposes of this report, we do not draw distinctions between internal and external security. Instead, we use the term "state security" to broadly encompass concepts such as "sovereignty and integrity", "security of the state", "defence of the state", "national security" as well as "public order", "public security", "public tranquillity", "public emergency" employed across the three jurisdictions.

4 This is likely to change if the Online Safety Bill 2023 recently introduced in the Sri Lankan Parliament is enacted. The bill lays down Sri Lanka's intermediary liability framework.

- **Safeguards Against Abuse of State Power:** Strengthen safeguards against potential state abuse of power. This can be achieved through mechanisms such as ex-ante judicial authorisation, ex-post judicial review, parliamentary and independent oversight, public disclosure of information, providing fair hearings, and establishing accessible grievance redressal mechanisms for aggrieved parties.

- **Reform for Online Safety and Ensuring Greater Platform Accountability:** Overhaul the social media regulatory framework to prioritise online safety through preventive measures that enforce platform accountability and long-term reform.

- **Multi-Stakeholder Approach:** Embrace a multi-stakeholder approach to policy making, ensuring diverse perspectives are considered. Implement more robust judicial review processes to maintain checks and balances on executive actions, and establish expert committees of members for periodic policy review and assessment, ensuring evidence-based, dynamic policymaking.

- **Capacity Building:** Invest in capacity building for all stakeholders to cultivate technical and subject matter expertise. Additionally, sanction independent research to understand the impact of social media on the region and various communities, especially marginalised groups.

Overall, the report concludes that social media governance in all three countries depends heavily on controlling the flow of online information. In many instances, state security exceptions are misused by these countries to curb the legitimate expression of dissent through direct and collateral censorship and law enforcement access to user data. Current regulatory frameworks and their implementation lack sufficient checks and balances and fall short of established democratic rule of law principles. Therefore, an effective and democratic platform governance model must prioritise the rights of citizens as the central focus when regulating digital public spaces. Its approach should revolve around empowering users and its primary objective should be to address harm to citizens, while balancing security imperatives, rather than exerting control over the flow of information.

1. INTRODUCTION

1.1 Overview

Social media platforms ("platforms") have revolutionised the online information ecosystem and fundamentally altered how we communicate, interact and access information. They empower users to post and share content across networks, enabling a novel "many-to-many" model of communication. This stands in sharp contrast to the traditional "one-to-many" model, which enabled traditional elites to be gatekeepers of information.[1]

This has fostered newer forms of expression, community building, mobilisation and collective action, with the potential to deepen democracy by platforming hitherto marginalised voices. Consequently, social media became celebrated as a tool of democratisation during mass movements like the 2011 Arab Spring protests,[2] Occupy Wall Street[3] and more recently the Black Lives Matter movement.[4]

However, the 2016 US elections proved to be a watershed moment in the global discourse on social media. Online platforms, which were once regarded as harbingers of democracy, are now recognised as a threat to the preservation of the liberal democratic order in the eyes of many critics.[5]

The dangers of online extremism and hate speech shocked the world as gruesome killings such as the Christchurch attack were live-streamed on Facebook.[6] The grave everyday real-life consequences of social media were most apparent during the pandemic when

1 Joshua A Tucker and others, 'From Liberation to Turmoil: Social Media and Democracy' (2017) 28 Journal of Democracy 46 <https://heinonline.org/HOL/P?h=hein.journals/jnlodmcy28&i=609>.

2 Ekaterina Stepanova, 'The Role of Information Communication Technologies in the "Arab Spring"' (2011) PONARS Eurasia Policy Memo No 159.

3 Chenda Ngak, 'Occupy Wall Street Uses Social Media to Spread Nationwide' (*CBS News*, 13 October 2011) <https://www.cbsnews.com/news/occupy-wall-street-uses-social-media-to-spread-nationwide/>.

4 Marcia Mundt, Karen Ross and Charla M Burnett, 'Scaling Social Movements Through Social Media: The Case of Black Lives Matter' (2018) 4(4) Social Media + Society <https://doi.org/10.1177/2056305118807911>.

5 Nathaniel Persily, 'Can Democracy Survive the Internet?' (2017) 28 J. Democracy 63; Nathaniel Persily and Joshua A Tucker, *Social Media and Democracy: The State of the Field, Prospects for Reform* (Cambridge University Press 2020); Michael L Miller and Cristian Vaccari, 'Digital Threats to Democracy: Comparative Lessons and Possible Remedies' (2020) 25 The International Journal of Press/Politics 333 <https://doi.org/10.1177/1940161220922323>.

6 Olivia Solon, 'Six Months after Christchurch Shootings, Videos of Attack Are Still on Facebook' (*NBC News*, 20 September 2019)<https://www.nbcnews.com/tech/tech-news/six-months-after-christchurch-shootings-videos-attack-are-still-facebook-n1056691>.

anti-vaccine misinformation proved to be a challenge to overburdened healthcare systems across the globe.[7]

Meanwhile, countries in the Global Majority have been experiencing the most catastrophic harms associated with social media. Here, social media platforms have often become a tool in the hands of the dominant elite to further marginalise the historically oppressed. In the Philippines, women journalists have become targets of online harassment,[8] while WhatsApp has fuelled mob lynchings against Dalits and Muslims in India.[9] The grave perils of unabated online hatred became tragically clear when misinformation and hate speech on Facebook against minority Rohingya Muslims culminated in genocide in Myanmar.[10]

1.2 Evolution of Social Media Governance

Platforms have come to hold unprecedented power in influencing public discourse.[11] However, there has been very little accountability in terms of how platforms moderate and curate content.[12] As hate speech,[13] violent extremism,[14] disinformation,[15] and computational

7 Evelyn Douek, 'The Year That Changed the Internet' (*The Atlantic* 28 December 2020) <https://www.theatlantic.com/ideas/archive/2020/12/how-2020-forced-facebook-and-twitter-step/617493/>.

8 Edson C Tandoc, Karryl Kim Sagun and Katrina Paola Alvarez, 'The Digitization of Harassment: Women Journalists' Experiences with Online Harassment in the Philippines' (2023) 17 Journalism Practice 1198 <https://doi.org/10.1080/17512786.2021.1981774>.

9 See Bhaskar Chakravorti, 'A Lynching in Digital South' The Indian Express (17 July 2018) <https://indianexpress.com/article/opinion/columns/a-lynching-in-digital-south-whatsapp-rumours-facebook-5262350/>; 'How WhatsApp Helped Turn an Indian Village into a Lynch Mob' (*BBC News*, 18 July 2018) <https://www.bbc.com/news/world-asia-india-44856910>; Rahul Mukherjee, 'Mobile Witnessing on WhatsApp: Vigilante Virality and the Anatomy of Mob Lynching' (2020) 18 South Asian Popular Culture 79 <https://doi.org/10.1080/14746689.2020.1736810>; Shakuntala Banaji and others, 'WhatsApp Vigilantes: An Exploration of Citizen Reception and Circulation of WhatsApp Misinformation Linked to Mob Violence in India'.

10 Paul Mozur, 'A Genocide Incited on Facebook, With Posts From Myanmar's Military' (*The New York Times*, 15 October 2018) <https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html>.

11 See Kate Klonick, 'The New Governors: The people, rules, and processes governing online speech' 131 Harvard Law Review; Evelyn Douek, 'The Internet's Titans Make a Power Grab' (*The Atlantic*, 18 April 2020) <https://www.theatlantic.com/ideas/archive/2020/04/pandemic-facebook-and-twitter-grab-more-power/610213/>.

12 Robert Gorwa and Timothy Garton Ash, 'Democratic Transparency in the Platform Society'.

13 See Mainack Mondal, Leandro Araújo Silva and Fabrício Benevenuto, 'A Measurement Study of Hate Speech in Social Media' (2017).

14 See Daphne Keller, 'Internet Platforms: Observations on Speech, Danger, and Money' [2018] Hoover Institution's Aegis Paper Series.

15 See Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," Science 359, no. 6380 (March 9, 2018): 1146–51, https://doi.org/10.1126/science.aap9559.

propaganda[16] flood online, platforms ability and legitimacy to unilaterally govern online speech has come under scrutiny.[17] There have been multiple instances where platform content moderation decisions have been vigorously contested and publicly criticised.[18]

Over the years, the characterisation of platforms as neutral intermediaries has been brought into question given the profit-driven algorithmic recommendation and moderation systems that govern the visibility and distribution of user content.[19]

Platforms have been criticised for prioritising engagement and profit over user safety.[20] Whistleblower revelations[21] have shown how even when platforms become aware of existing problems internally, they often choose to do nothing. The Facebook Files, for instance, revealed how, despite awareness among internal researchers within Meta about the negative mental health consequences of Instagram on teenage girls, the company failed to make substantial efforts to address them. Moreover, Meta constantly downplayed these concerns in public.[22]

16 See Samuel C Woolley, 'Bots and Computational Propaganda: Automation for Communication and Control' in Joshua A Tucker and Nathaniel Persily (eds), *Social Media and Democracy: The State of the Field, Prospects for Reform* (Cambridge University Press 2020) <https://www.cambridge.org/core/books/social-media-and-democracy/bots-and-computational-propaganda-automation-for-communication-and-control/A15EE25C278B442EF00199AA660BFADD>.

17 See Gilad Abiri and Sebastian Guidi, 'From a Network to a Dilemma: The Legitimacy of Social Media' [2022] SSRN Electronic Journal <https://www.ssrn.com/abstract=4230635>; Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7 Big Data & Society 2053951719897945 <https://doi.org/10.1177/2053951719897945>; Evelyn Douek, 'Content Moderation as Systems Thinking' (10 January 2022) <https://papers.ssrn.com/abstract=4005326>.

18 See Daphne Keller, 'Internet Platforms: Observations on Speech, Danger, and Money' [2018] Hoover Institution's Aegis Paper Series; Billy Perrigo, 'Donald Trump Will Not Be Allowed Back on Facebook Yet—But a Bigger Showdown Is Coming' [2021] Time <https://time.com/6046197/donald-trump-banned-facebook-analysis/>; Alaina Demopoulos, 'Free the Nipple: Facebook and Instagram Told to Overhaul Ban on Bare Breasts' *The Guardian* (18 January 2023) <https://www.theguardian.com/technology/2023/jan/17/free-the-nipple-meta-facebook-instagram>; Usaid Siddiqui, Priyanka Shankar, and Pranav Dixit, '"Significant Censorship" of Palestine on Social Media Sparks Outcry' Al Jazeera (24 October 2023) <https://www.aljazeera.com/features/2023/10/24/shadowbanning-are-social-media-giants-censoring-pro-palestine-voices>;

19 Miriam Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation' (21 June 2021) <https://papers.ssrn.com/abstract=3876328> accessed 25 August 2022.

20 See Ryan Mac and Cecilia Kang, 'Whistle-Blower Says Facebook "Chooses Profits Over Safety"' *The New York Times* (3 October 2021) <https://www.nytimes.com/2021/10/03/technology/whistle-blower-facebook-frances-haugen.html>; Livemint, '"Twitter Prioritizes Profit over Security": Whistleblower Testifies to Congress' Mint (13 September 2022) <https://www.livemint.com/news/world/twitter-is-misleading-public-peter-mudge-zatko-begins-testifying-to-congress-11663079489433.html>.

21 Cristiano Lima, 'A Whistleblower's Power: Key Takeaways from the Facebook Papers' *The Washington Post* (25 October 2021) <https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/>.

22 Georgia Wells, Jeff Horwitz and Deepa Seetharaman, 'Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show' *Wall Street Journal* (14 September 2021) <https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739>.

This has led to a decisive shift in public perception of platforms, fueling demands for greater accountability.[23] This shift in perception is also reflected in the regulatory approach to platforms. Self–governance has been the dominant model of regulation for social media platforms up until now.[24] This model is best exemplified by Section 230 of the U.S. Communication Decency Act[25] which immunised platforms from (i) liability for most of the third-party content they host and (ii) liability for any content they moderate in line with their community guidelines.[26]

However, due to intense criticism directed at platforms regarding their opaque content moderation and curation practices, platforms have been adopting certain voluntary transparency measures.[27] Amid widespread public criticism, Facebook even created an independent oversight authority "like its own Supreme Court" in 2018.[28]

However, regulators across the globe are realising the limitations of the self-regulatory model in bringing about any fundamental changes in platform design or business models. Consequently, there is a shift towards greater state intervention.[29]

State regulation often takes the form of privacy and data protection laws (like the EU's General Data Protection Regulation[30]), revision of intermediary liability laws (like India's Information Technology Rules[31]), competition laws (like the EU's Digital Markets Act[32]),

23 Robert Gorwa and Timothy Garton Ash, 'Democratic Transparency in the Platform Society'.

24 Robert Gorwa, 'What Is Platform Governance?' (2019) 22 Information, communication & society 854.

25 Communications Decency Act 47 U.S.C. s. 230(c) (1996).

26 Daphne Keller, 'Internet Platforms: Observations on Speech, Danger, and Money' (13 June 2018) <https://papers.ssrn.com/abstract=3262936>.

27 These include measures like transparency reporting, publication of community guidelines and creation of public advertisement repositories.

See Robert Gorwa and Timothy Garton Ash, 'Democratic Transparency in the Platform Society'.

28 Kate Klonick, 'The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression' (2019) 129 Yale LJ 2418.

29 Robert Gorwa, 'The Platform Governance Triangle: Conceptualising the Informal Regulation of Online Content' (2019) 8 Internet Policy Review 1 <https://www.econstor.eu/handle/10419/214074>.

30 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

31 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

32 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265.

platform governance laws (like the Digital Services Act[33]) and user safety laws (like the United Kingdom's Online Safety Act[34]).[35]

In fact, states across the globe are contemplating even greater regulation of the digital sphere. According to the Freedom on the Net (FOTN) report of 2021, 48 out of 70 countries analysed, pursued legislative or administrative action to regulate technology companies.[36] This is, in many ways, a sanguine development, inasmuch as it demonstrates that governments are taking the harms caused by social media seriously.

However, these new regulations can cause problems of their own. For instance, the FOTN report also notes that 24 out of these 48 countries introduced regulations targeting online content, which often presents a slippery slope. Take, for instance, the German Network Enforcement Law (NetzDG).[37] It mandates platforms to act on user complaints and takedown "manifestly unlawful" content within 24 hours. While the law aims to counter online hate speech by enforcing the existing 22 statutes that penalise incitement to hatred, terrorist propaganda, etc., it has been criticised for incentivising the over-removal of content and for inspiring similar provisions in authoritarian countries.[38]

While there is a need for rethinking platform regulation, many new regulations emerging across the globe provide states with significant discretionary power that has the potential to infringe on the rights of users.[39] It also raises concerns about increased state surveillance and censorship, especially in countries that have fragile political systems, weaker rule of

33 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277.

34 The Online Safety Act 2023.

35 Robert Gorwa, 'What Is Platform Governance?' (2019) 22 Information, communication & society 854; Robert Gorwa, 'The Platform Governance Triangle: Conceptualising the Informal Regulation of Online Content' (2019) 8 Internet Policy Review 1 <https://www.econstor.eu/handle/10419/214074>.

36 Adrian Shahbaz, Allie Funk, 'The Global Drive to Control Big Tech' (*Freedom House*, 2021) <https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech>.

37 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) 2017.

38 Jacob Mchangama and Natalie Alkiviadou, 'The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship: Act Two' (2020) Copenhagen: Justitia <https://justitia-int.org/wp-content/uploads/2019/11/Analyse_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf>.

39 Adrian Shahbaz and Allie Funk, 'Freedom on the Net 2021' (*Freedom House*, 2021) <https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf>.

law or political violence.[40] Increased instances of internet shutdowns to counter political protests[41] and a decline in freedom of users on the internet have raised concerns about the descent into digital authoritarianism.[42]

Thus, while social media platforms have been used by citizens to organise and communicate their dissent against powerful elites, states are at the same time, through the mechanism of these platforms, engaging in enhanced surveillance and censorship.[43]

To preserve the democratic interests of the citizens from both public censorship and build accountability for corporate privatised standards, public actors must play a crucial role in determining the manner and method of regulating these private transnational corporations. However, this presents several challenges:[44]

Firstly, the nature of the regulation has extraterritorial implications, as information flows seamlessly across borders. *Secondly*, the scale of such services and corporations threatens to overwhelm the government's ability to successfully regulate them. *Thirdly*, state regulation is often not equipped to deal with harms arising out of scalability and virality, much less the newer harms emerging from rapid advances in technology. *Fourthly*, the government has to protect users against online harms while carefully curating regulations for platforms, to avoid infringing on their rights to conduct business. *Fifthly*, the government has to empower users – to exercise their rights to freedom of expression, access to information, and other commercial rights – while balancing them with the competing interests of the state and the rights of other users.

40 See Paul Mozur, Adam Satariano and Aaron Krolik, 'Russia's Online Censorship Has Soared 30-Fold During Ukraine War' *The New York Times* (26 July 2023) <https://www.nytimes.com/2023/07/26/technology/russia-censorship-ukraine-war.html>; Yousef Saba and Nafisa Eltahir, 'Sudan Restricts Social Media Access to Counter Protest Movement' Reuters (3 January 2019) <https://www.reuters.comarticle/idUSKCN1OX08Q-OZATP/>; Rina Chandran and Thomson Reuters Foundation, 'FEATURE-A Year after Myanmar Coup, Growing Surveillance Threatens Lives' Reuters (31 January 2022) <https://www.reuters.comarticle/idUSL8N2TX2KI/>.

41 'The Return of Digital Authoritarianism: Internet Shutdowns in 2021' (*Access Now*, 2022) <https://www.accessnow.org/wp-content/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf>.

42 Tiberiu Dragu and Yonatan Lupu, 'Digital Authoritarianism and the Future of Human Rights' (2021) 75 International Organization 991 <https://www.cambridge.org/core/journals/international-organization/article/abs/digital-authoritarianism-and-the-future-of-human-rights/5027FD3B3C6A3F36A0B26ECBFD9FC061>.

43 Anita R Gohdes, 'Repression Technology: Internet Accessibility and State Violence' (2020) 64 American Journal of Political Science 488 <https://onlinelibrary.wiley.com/doi/abs/10.1111/ajps.12509>.

44 De Gregorio Giovanni, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022).

1.3 Scope of the Study

Different models of social media regulation are evolving across the globe. While the United States, the European Union and China have emerged as major models of regulation.[45] The evolution and impact of social media regulation in many Global Majority countries remains understudied.

The countries face heightened challenges in addressing harmful and illegal speech on platforms as major platforms have limited capacity to govern discourse taking place in diverse languages and socio-political contexts,[46] coupled with limited and differential resource allocation to many regions.[47] Moreover, they share unique power dynamics with major social platforms that shape their regulatory models.[48]

At the same time, it is observed that several governments in Asia are taking regulatory or executive actions that pose grave challenges to the freedoms of end-users. Singapore's fake news law,[49] the Philippines's crackdown on journalistic expression,[50] and censorship in Pakistan[51] all raise concerns about the arbitrary exercise of state power and censoring free speech and expression.

45 Anu Bradford, Digital Empires: The Global Battle to Regulate Technology (Oxford University Press 2023).

46 See Justin Scheck, Newley Purnell and Jeff Horwitz, 'Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show.' *Wall Street Journal* (16 September 2021) <https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953>; Ben Gilbert, 'Facebook Ranks Countries into Tiers of Importance for Content Moderation, with Some Nations Getting Little to No Direct Oversight, Report Says' *Business Insider* (5 October 2021) <https://www.businessinsider.in/tech/news/facebook-ranks-countries-into-tiers-of-importance-for-content-moderation-with-some-nations-getting-little-to-no-direct-oversight-report-says/articleshow/87263447.cms>; Zahra Takhshid, 'Regulating Social Media in the Global South' 24.

47 Ben Gilbert, 'Facebook Ranks Countries into Tiers of Importance for Content Moderation, with Some Nations Getting Little to No Direct Oversight, Report Says' *Business Insider* (5 October 2021) <https://www.businessinsider.in/tech/news/facebook-ranks-countries-into-tiers-of-importance-for-content-moderation-with-some-nations-getting-little-to-no-direct-oversight-report-says/articleshow/87263447.cms>.

48 Zahra Takhshid, 'Regulating Social Media in the Global South' 24.

49 See HRW, 'Singapore: "Fake News" Law Curtails Speech | Human Rights Watch' (Human Rights Watch, 13 January 2021) <https://www.hrw.org/news/2021/01/13/singapore-fake-news-law-curtails-speech> ; Dewey Sim, Kimberly Lim, 'Singapore's online safety bill may be a double-edged sword, analysts say' (*SCMP*, 7 October 2022) <https://www.scmp.com/week-asia/politics/article/3195087/singapores-online-safety-bill-may-be-double-edged-sword-say?module=inline&pgtype=article>.

50 Another attempt to censor online media in Philippines' (*Reporters Without Borders*, 29 June 2022) <https://rsf.org/en/another-attempt-censor-online-media-philippines>.

51 Haroon Janjua, Pakistan moves to stifle social media dissent' (DW, 24 February 2022) <https://www.dw.com/en/pakistan-new-cybercrime-law-threatens-to-to-stifle-social-media-dissent/a-60899561>.

It thus becomes critical to map the emergence of unique regulatory frameworks and models emerging in the Asian region and the impact they have on how online information is created, disseminated and accessed.

1.3.1 Mapping Trends in Social Media Regulation

This report examines the social media regulatory framework in three South Asian countries – Sri Lanka, India and Bangladesh, and maps key trends across these three jurisdictions. It focuses on how cybersecurity and other ICT regulations relevant to the social media landscape, intermediary liability frameworks, as well as, key speech laws (mostly penal) are employed to regulate the flow of online information.

This regulation of the online information ecosystem is a key component of how social media platforms are directly and indirectly "regulated". We use the term "regulate", here to broadly mean any actions taken to govern or influence the way in which social media platforms are operated as well as, used and accessed. It consists of regulation that is directed at (a) social media platforms as intermediaries; (b) other intermediaries like ISPs; and (c) end users.

This regulation of the flow of information is operationalised through the following key mechanisms across the three countries:[52]

- **Internet shutdowns:** Internet shutdowns refer to actions taken by a government to intentionally disrupt access to information and communications systems online, by either blocking or slowing down entire communication networks (or parts of such networks).

52 While internet shutdowns, law enforcement access to user data, and criminalisation of speech are being employed across all three jurisdictions, state blocking of targeted content on social media is absent in Sri Lanka at the time of writing. However, this is set to change if the Online Safety Bill, 2023 is enacted.

- **Blocking content on social media:** Blocking specific pieces of content hosted on social media; this implies a content blocking or removal order by the executive for the purposes of this report.
- **Law enforcement access to user data:** Law enforcement agencies (LEAs) access citizen data stored with the intermediaries for the purposes of investigation of crime; they may also proactively monitor public data across platforms to build intelligence.
- **Criminalisation of online speech:** Various penal laws and online speech offences aim to curtail the misuse of online expression for unlawful purposes.

1.3.2 Social Media Governance and Security Imperatives

The report also examines how governments in Sri Lanka, India, and Bangladesh are increasingly viewing, justifying, and communicating online harms and policy solutions in terms of security imperatives.

This analysis becomes significant as social media platforms are increasingly playing a critical role across several national security and geopolitical fronts.[53] Platforms can be manipulated to spread violent and extremist content[54] as well as organised disinformation by both domestic and foreign actors.[55] This makes platforms vital stakeholders in the state security apparatus.

Since the 2016 U.S. presidential election, disinformation and foreign influence operations have been viewed as significant state security threats.[56] Although these elections brought the role of platforms in state security to the fore,[57] concerns regarding online communication have always existed. Securitisation[58] of different aspects of cyberspace has been a point of contention since the early 2000s(s), when the use of the Internet by terrorist

53 Elena Chachko, 'National Security by Platform' (2021) 25 Stanford Technology Law Review.

54 See Robin Thompson, 'Radicalization and the Use of Social Media' (2011) 4 Journal of Strategic Security 167 <https://www.jstor.org/stable/26463917>; Ariel Victoria Lieberman, 'Terrorism, the Internet, and Propaganda: A Deadly Combination' 9 THE INTERNET; Mark Scott, 'Fringe Social Media Networks Sidestep Online Content Rules' *Politico* (25 January 2022) <https://www.politico.eu/article/fringe-social-media-telegram-extremism-far-right/>.

55 See Arild Bergh, 'Understanding Influence Operations in Social Media' (2020) 19 Journal of Information Warfare 110; Samantha Bradshaw, Hannah Bailey and Philip N Howard, 'Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation' (University of Oxford 2021) <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report-2020-v.2.pdf>.

56 Dennis Broeders, 'The (Im) Possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG: A Mid-Process Assessment' (2021) Journal of Cyber Policy 1,21; Christopher Whyte, 'Cyber Conflict or Democracy 'Hacked'? How Cyber Operations Enhance Information Warfare' (2020) *Journal of Cybersecurity* 6(1); Kathleen Hall Jamieson, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know* (Oxford University Press, 2020).

57 Such alleged threats to the foundations of Western liberal democracy are reflected in the Declaration on Responsible State Behaviour in Cyberspace issued by the G7 that expresses concern about "cyber-enabled interference in democratic political processes".

See G7, *Declaration on Responsible States Behavior in Cyberspace* (G7 Declaration), <https://www.mofa.go.jp/files/000246367.pdf>.

58 Balzacq defines securitisation as "an articulated assemblage of practices whereby heuristic artefacts (metaphors, policy tools, image repertoires, analogies, stereotypes, emotions, etc.) are contextually mobilized by a securitising actor, who works to prompt an audience to build a coherent network of implications (feelings, sensations, thoughts, and intuitions), about the critical vulnerability of a referent object, that concurs with the securitising actor's reasons for choices and actions, by investing the referent subject with such an aura of unprecedented threatening complexion that a customized policy must be undertaken immediately to block its development."

Thierry Balzacq, *A Theory of securitisation: Origins, Core Assumptions, and Variants* (Routledge 2010).

groups for communication, recruitment, broadcasting propaganda and fundraising was under the scanner of Western security agencies and political commentators.[59] State security concerns have been embedded in the architecture of the Internet.[60]

Although social media platforms raise legitimate and significant security concerns for the state, regulating the online information ecosystem on security imperatives introduces potential risks. Since security concerns of the state are associated with an existential threat to the state and society, they often enable the executive to suspend ordinary due process considerations and wield exceptional power.[61] Thus, distinctive or even extraordinary measures suspending due democratic process can be taken by the state to contain the urgent threat at hand.[62] Such extraordinary and unilateral exercise of state power becomes possible when public issues are constructed as security issues.[63] These extraordinary measures often bypass democratic deliberation and consensus building. This comes with the risk of misuse of these provisions, especially in the absence of proper checks and balances.

States can rely on security concerns to curb citizens' rights to free expression and privacy. The dangers of securitisation in the online space have become even more apparent recently manifesting as social media bans justified on national security grounds.[64] Nigeria, for instance, imposed a seven-month ban on Twitter in June 2021, prompted by the platform's removal of a post by the Nigerian President for violating its terms of service amid the

59 A case in point is the USA Patriot Act which gave security personnel increased powers over monitoring online communications post 9/11 attacks.

See Helen Nissenbaum, 'Where Computer Security Meets National Security' (2005) Ethics and Information Technology Volume 7, 59–84 <https://doi.org/10.1007/s10676-005-4582-3>

60 States realise that "points of infrastructural control can serve as proxies to regain (or gain) control or manipulate the flow of money information and the marketplace of ideas in the digital sphere". Russia's proposed laws on the "Autonomous Russian Internet" will result in all traffic being routed through state-approved exchange points leading to complete sovereignty over what has been called a "closed" cyberspace or "information space". By contrast, the European Union has a more "open" conception of cyberspace which nevertheless places the State at the centre of ensuring a degree of technical autonomy and security against foreign surveillance.

See Eva Claessen, 'Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU' (2020) Journal of Cyber Policy 5(1) 140,157 <https://doi.org/10.1080/23738871.2020.1728356>.

61 Thierry Balzacq, *A Theory of securitisation: Origins, Core Assumptions, and Variants* (Routledge 2010).

62 Thierry Balzacq, Sarah Léonard and Jan Ruzicka, '"securitisation" Revisited: Theory and Cases' (2016) 30 International Relations 494 <https://doi.org/10.1177/0047117815596590>.

63 Ibid.

64 'The Return of Digital Authoritarianism: Internet Shutdowns in 2021' (*Access Now*, 2022) <https://www.accessnow.org/wp-content/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf>.

EndSARS protests.[65] In Pakistan, social media platforms and the government are locked in an ongoing conflict over the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules notified in 2021.[66] In Singapore, the Protection from Online Falsehoods and Manipulation Act has armed the state with extraordinary power in light of the securitisation of disinformation.[67]

It thus becomes crucial to investigate how state security concerns play out in social media governance across Sri Lanka, India and Bangladesh. In particular, we examine how tools and processes for regulating the online information ecosystem are deployed on grounds of state security.[68] This has implications for the democratic rule of law.

1.3.3 Social Media Regulation and Rule of Law

Social media platforms have the potential to empower citizens to exercise their fundamental rights, especially civil and political rights. They extend the user's ability to disseminate and access information within online communities at an unprecedented rate.[69]

65 Emmanuel Akinwotu, 'Nigeria Lifts Twitter Ban Seven Months after Site Deleted President's Post' (*The Guardian*, 13 January 2022) <https://www.theguardian.com/world/2022/jan/13/nigeria-lifts-twitter-ban-seven-months-after-site-deleted-presidents-post>.

66 The 2020 version of the rules and the lack of industry consultation during their formulation received intense backlash. Major social media platforms, through the Asia Internet Coalition, threatened to pull out of the country. Data localization requirements, law enforcement access to decrypted data, expansive content blocking powers to the Pakistan Telecommunication Authority, and the 24-hour timeline to remove unlawful content, all sparked concern across industry and civil society. The 2021 Rules increased the content removal timeline to 48 hours, introduced registration of social media companies with the telecommunication authority, and made the timelines for establishing local offices in Pakistan flexible for social media companies. The amended rules were also criticised by industry, as they not only retained several problematic provisions of the earlier version but also further expanded government powers.

See Ramsha Jahangir, 'Tech Giants Threaten to Leave Pakistan If Social Media Rules Stay' (*DAWN.COM*, 20 November 2020) <https://www.dawn.com/news/1591357>;

Manish Singh, 'Google, Facebook and Twitter Threaten to Leave Pakistan over Censorship Law' (TechCrunch, 20 November 2020) <https://techcrunch.com/2020/11/20/google-facebook-and-twitter-threaten-to-leave-pakistan-over-censorship-law/>.

67 Ric Neo, 'The Securitisation of Fake News in Singapore' (2020) 57 International Politics 724 <https://www.researchgate.net/profile/Ric-Neo/publication/336270460_The_securitisation_of_fake_news_in_Singapore/links/5f15544692851c1eff2183bb/The-securitisation-of-fake-news-in-Singapore.pdf>.

68 For the purposes of this report, we do not draw distinctions between internal and external security. Instead, we use the term "state security" to broadly encompass concepts such as "sovereignty and integrity", "security of the state", "defence of the state", "national security" as well as "public order", "public security", "public tranquillity", "public emergency" employed across the three jurisdictions.

69 Brian D Loader and Dan Mercea, 'Networking Democracy?' (2011) 14 Information, Communication & Society 757 <https://doi.org/10.1080/1369118X.2011.592648>.

At the same time, as governments exercise their powers to regulate social media entities and end-users especially while safeguarding security interests, they impose certain restrictions on citizens' fundamental rights and freedoms to balance the security imperative. It is essential that such restrictions respect the substantive and procedural safeguards that enforce rights-protecting legislation. The absence of such safeguards in the platform governance framework results in unchecked executive power and diminished transparency, which undermines the rule of law.

As this report will demonstrate, the security imperative poses a significant challenge to adherence to the safeguards that are the hallmark of the rule of law.

It is also important to note that all three jurisdictions are at different stages in developing platform governance frameworks. Key legislative developments and judicial pronouncements are shaping the way users access platforms and express and share information. These evolving regulatory frameworks are increasingly facing the test of the rule of law, especially in the judicial systems of their countries.

Consequently, the report delves into the impact that such regulation of the flow of online information has on rule of law principles. In this context, our analysis benchmarks social media regulation against the following rule of law parameters:[70]

1) supremacy of law,
2) equality before the law,
3) accountability to the law,
4) fairness in application,
5) separation of powers,
6) participatory decision-making,
7) legal certainty,
8) avoidance of arbitrariness, and
9) procedural plus legal transparency.

70 United Nations Security Council, *The rule of law and transitional justice in conflict and post-conflict societies*, (Report of the Secretary General, S/2004/616), para 6 <https://digitallibrary.un.org/record/527647>.

1.4 Overview of the Report

This report presents a country-wise overview of Sri Lanka's (Chapter 2), India's (Chapter 3)and Bangladesh's (Chapter 4) law and policy landscape as it relates to social media.[71] In particular, this includes an analysis of (a) cybersecurity and other ICT regulations relevant to the social media landscape, (b) intermediary liability framework for social media platforms, (c) mechanisms for regulating the online information ecosystem, (d) the administrative landscape of cybersecurity and social media regulation and (e) the impact of the regulatory framework on rule of law.

Chapter 5 maps trends that are relevant to the regulation of social media platforms and the information ecosystem and further culls out key convergences and divergences that are emerging in the three South Asian countries. It concludes with our findings and key recommendations that will be integral to the maintenance of the rule of law in platform governance frameworks in South Asia.

We conclude that (a) ICT regulation comprising of cybersecurity, data protection, telecommunication regulation; (b) intermediary liability frameworks;[72] (c) key speech laws (mostly penal) are employed to regulate the flow of information. This regulation of the online information ecosystem plays a significant role in how social media platforms and users are governed in all three jurisdictions. It is observed that security imperatives of the state crucially influence the regulation of the online information ecosystem.

A trend of centralisation of power with the executive and a lack of effective checks and balances in the regulation of online information is observed across all three countries. This is magnified by the overbroad and vague language used to codify security exceptions as well as speech-related offences.

In the absence of adequate safeguards, the discretion available to states can be misused to curb the legitimate expression of dissent through direct and collateral censorship and law enforcement access to user data. It is observed across the report that censorship on the basis of state security imperatives has resulted in the restriction of legally permissible speech in all three countries.

Thus, we recommend limiting the scope of security exceptions and expanding procedural and substantive safeguards to balance state security imperatives with the freedom and rights of citizens. More generally, as states across South Asia contemplate major regulatory changes, an effective platform governance model that places the rights of citizens at the centre is needed.

71 The report reflects the social media regulatory framework in the three jurisdictions at the time of writing (November 2023).

72 While India and Bangladesh provide conditional exemption from liability for third-party content hosted by intermediaries, Sri Lanka lacks such an exemption framework at the time of writing. However, this can change with the proposed Online Safety Bill 2023.

2. SRI LANKA'S LANDSCAPE ON SOCIAL MEDIA REGULATION AND IMPACT ON RULE OF LAW

2.1 Overview

As of November 2023, Sri Lanka lacks specific legislation aimed at social media platforms. However, at the time of writing, the Online Safety Bill 2023 (OSB) is under consideration at the Parliament. Should the OSB be enacted, it will establish an intermediary liability framework for social media platforms.[1]

But until a law is passed, Sri Lanka is categorised as a country that does not have a law that can directly regulate social media platforms. Though without a specific law, up to now, several existing statutes have been used to regulate user-generated content. These legislative instruments include the International Covenant on Civil and Political Rights Act (ICCPR Act) No. 56 of 2007,[2] Computer Crime Act (CCA) No. 24 of 2007,[3] the Prevention of Terrorism Act (PTA) of 1979,[4] and Public Security Ordinance No 25 of 1947[5] (in the event of an Emergency being declared).

1 Section 2.6.1 provides a detailed overview of the proposed bill, encompassing its content, context, and the latest developments at the time of writing.

2 International Covenant on Civil and Political Rights Act, Number 56 of 2007.

3 Computer Crime Act, Number 24 of 2007.

4 Prevention of Terrorism (Temporary Provisions) Act, Number 48 of 1978. The PTA was introduced as a temporary wartime prevention measure to prevent unlawful activities but gained the status of a permanent law in 1982. The Act has since been criticised for its misuse through arbitrary application and subsequently amended in 1988 and 2022.

5 Public Security Ordinance No 25 1947< https://www.srilankalaw.lk/p/968-public-security-ordinance.html>.

This chapter begins by examining the laws used to regulate cybersecurity and laws used to regulate social media, as well as laws pertaining to data localisation and data retention.

Second, it considers three case studies in which attempts to control the use and access to social media were deployed extensively – the Easter Sunday Terror Attacks of 2019, the COVID-19 pandemic from 2020 onwards, and the protests related to the economic crisis in Sri Lanka from April 2022 onwards – to assess what kind of real-world actions are taken to "regulate"[6] social media.

The chapter then examines the regulatory frameworks and their application across diverse case studies to identify key mechanisms through which the dissemination of online information in Sri Lanka is governed.

Such actions demonstrate a trend of government's efforts directed at governing individual behaviour, through arrests or blocking access to social media content facilitated by the Internet Service Providers (ISPs), and not the platforms themselves.

We point out that social media regulation is often treated as a security issue, and security is often cited as a reason to implement actions to regulate users' behaviour on social media.[7] We observe from the text of the laws that they were not intended to regulate social media and/or cybersecurity. For example, the Computer Crime Act, which is a law concerning crimes using/affecting computers/computer systems has been used in practice for social media regulation.

Finally, the chapter explores how the principles of the Rule of Law are impacted by social media regulation in Sri Lanka.

6 Note that we use the term "regulate" to broadly mean any actions taken to govern/influence the way in which social media is used and accessed. It does not imply there is a regulator or regulators who have power over regulated entities in the traditional sense (for example, unlike in telecom regulation, where telecom service providers are licence holders that can be regulated by a sectoral regulator in Sri Lanka and many other countries).

7 Aaron Barr, 'Social Media Regulation: The Line Between Privacy and Protection' (*Security Boulevard*, 2021) <https://securityboulevard.com/2021/06/social-media-regulation-the-line-between-privacy-and-protection/>.

2.1.1 Overview of Sri Lanka's Legal System

The legal system of Sri Lanka is influenced by the legal traditions of civil and common law systems.[8] Roman-Dutch law is the residuary law of the country. The laws of Sri Lanka have their origins in English, Roman-Dutch, and many other sources. In the non-statutory areas, case laws are of relevance. Lord Diplock in the case of *Kodeeswaran v. Attorney General* termed case laws as the "indigenous common law of Sri Lanka."[9]

The Constitution of Sri Lanka is an amalgamation of the Westminster model with the French Presidential system. There is an executive President with powers in addition to the Prime Minister.[10] Since gaining independence in 1948, Sri Lanka has had three constitutions.[11] The 1978 Constitution, that is currently in force, provides for an Executive Presidential System of Government with a Prime Minister playing a relatively minor role.[12] In 2015, the 19th Amendment to the Constitution reversed the role of the President in certain respects, for example, the President could not remove the Prime Minister. The powers of the President were also restricted in dissolving the Parliament, and appointments for certain high-level positions could be made by the Constitutional Council.[13] The 20th Amendment has reversed these changes and further consolidated the powers of the President.[14]

8 LJM Cooray, *An introduction to the Legal System of Sri Lanka* (Stamford Lake, 2011), 11.

9 *Kodeeswaran v. Attorney General* (1969) 72 NLR 337.

10 LJM Cooray, *An introduction to the Legal System of Sri Lanka* (Stamford Lake, 2011), 13.

11 LJM Cooray, *Constitutional Government in Sri Lanka 1796- 1977* (Stamford Lake Publication 1984).

12 Danath Jayasuriya, 'Empowering the Executive President Through Sri Lanka's Twentieth Amendment to the Constitution', *Perspectives on Constitutional Reform in Sri Lanka* (ICLS, 2021).

13 Ibid; 19th Amendment to the Constitution of Sri Lanka.

14 See 'A Brief Guide to the 20th Amendment to the Constitution' (*Centre for Policy Alternatives*, 19 July 2021) <https://www.cpalanka.org/a-brief-guide-to-the-20th-amendment-to-the-constitution/>.

2.2 Laws on Cybersecurity and Social Media Regulation[15]

2.2.1 Laws on Cybersecurity

Sri Lanka currently does not yet have a specific cybersecurity law, although a draft legislation, otherwise known as the Cybersecurity Bill, was released in 2019 and went through a process of public consultation.[16] A revised version of the Cyber Security Bill was issued in August 2023, and public comments were again invited for the draft. However, since then there have been no further developments and it has not been formally adopted as a law (discussed further in section 2.6). However, other laws (and strategies) do have cybersecurity provisions:

1. The Computer Crime Act (2007)

Sri Lanka passed the CCA in 2007. This Act was largely modelled on the Budapest Convention (see the section below). The Act covers offences such as "Securing unauthorised access to a computer"; "Causing a computer to perform a function without lawful authority"; and "Offences committed against national security."[17] Specific provisions in the CCA have been used to regulate social media, as we will discuss in subsequent sections of this report.

2. Mutual Assistance in Criminal Matters Act (2002)

Sri Lanka became a state party to the Budapest Convention on Cybercrime in 2015, making it the first South Asian country to do so. The Budapest Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law

15 Please note that the official government published version of the various laws referred to in this section are not always available online to be cited. While we do provide links to online versions that are available via other sources, in order to give the reader a reasonable sense of the laws content, note should be taken that that the official government version is the authoritative source and may differ from online version provided by other sources.

16 Cyber Security Bill 2019 <https://www.cert.gov.lk/documents/Cyber%20Security%20Bill.pdf>.

17 Computer Crime Act No 24 of 2007 <https://www.lawnet.gov.lk/act-no-24-of-2007/>.

powers necessary for the investigation and prosecution of such offences, as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international cooperation.[18]

As party to the Budapest Convention, amendments were made to the Mutual Assistance in Criminal Matters Act (MACMA) in 2018, which covers mutual legal assistance on cybercrime; "the tracing of crimes committed via internet, information communications technology, cloud computing, blockchain technology and other computer networks including the trading of any digital currencies"; "the expedited preservation of stored computer data and expedited disclosure of preserved traffic data and data retention".[19]

In April 2019, the Easter Sunday terrorist attacks resulted in the mass killing of more than two hundred people (see section 2.3 for more information on the attacks). This led to a national emergency in the country, and the Government of Sri Lanka called for international assistance from other State Parties to the Convention, wherein electronic evidence was collected, and joint investigations held.[20] Electronic evidence was obtained through joint investigations, enabled by the amendments to MACMA carried out since becoming a Party to the Budapest Convention. Of the 99 requests received by Facebook, Google/YouTube and Microsoft/Skype, 42 were disclosed by the platforms.[21] These requests were made possible through the international cooperation emanating from the Budapest Convention.

3. The Electronic Transactions Act (2006)

The Act mandates security procedures for the use of electronic data and digital documents, and for carrying out electronic transactions. This Act is used to facilitate e-commerce, enable electronic contracts and electronic evidence. The Act can, therefore, be seen to support the safe/secure use of the Internet and, as such, is listed here for completeness.

18 Convention on Cybercrime 2001; Council of Europe, *Explanatory Report to the Convention on Cybercrime* (European Treaty Series No 185, 2015) < https://rm.coe.int/16800cce5b>.

19 Mutual Assistance in Criminal Matters Act No. 24 of 2018 1 (SL) <https://rm.coe.int/t-cy20-item5-mla-amendment-act-sri-lanka/16808f1f72>.

20 Council of Europe, *The Budapest Convention on Cybercrime: benefits and impact in practice* (T-CY (2020)16) <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>.

21 Council of Europe, *The Budapest Convention on Cybercrime: benefits and impact in practice*' (T-CY (2020)16) <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>.

The Act also provides a definition of "intermediary".[22] However, the definition does not cover intermediaries related to social media platforms and is therefore not relevant to the discussions that follow.

While not a law, for the sake of completeness it is worth mentioning here the Information and Cybersecurity Strategy of Sri Lanka (2019-2023). This strategy, which was released by the Sri Lanka Computer Emergency Readiness Team (SLCERT), highlights a plan of action which will help SLCERT's goal of a secure cybersecurity ecosystem and facilitate growth, mainly focusing on the aim of developing sound cyberspace infrastructure, and the aim of formulating of policies and laws to create a safe regulatory environment. However, the strategy makes no mention of social media, and does not define either cybersecurity or information security.[23]

2.2.2 Laws on Social Media

Sri Lanka does not have specific laws to regulate social media platforms (though, as noted, if the Online Safety Bill becomes law, this situation may change). There is currently no platform conditional intermediary liability exemption or safe harbour protection afforded to social media platforms in Sri Lanka. However, certain laws, which are discussed below, have been used to govern social media. The process by which social media blocks take place is not transparent and is discussed in more detail in section 2.6 of this chapter.

The laws that have been deployed in practice to regulate social media (through certain actions, i.e. arrests of social media users) are discussed below, with the most important section of the laws emphasised in bold text. Examples of the law's usage are given in Box 1 under section 2.3:

22 As per section 26 of the Electronic Transactions Act 2006 an intermediary is defined as, "*a person acting as a service provider on behalf of another person in relation to the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it*."

23 Information and Cyber Security Strategy of Sri Lanka (2019 – 2023) (Sri Lanka CERT 2018) <https://cert.gov.lk/wp-content/uploads/2023/07/Information_and_CyberSecurity_StrategyofSri-Lanka.pdf>.

1. International Covenant on Civil and Political Rights (ICCPR) Act (2007)

The ICCPR Act of 2007 was enacted to protect human rights. The Act criminalises propagation or advocacy related to national, racial or religious hatred as cited below. Section 3 of ICCPR Act criminalises the propagation of war or the advocacy of national, racial, or religious hatred that leads to incitement to discrimination, hostility, or violence.

Section 3: ("No person should propagate war")

> "(1) No person shall **propagate war or advocate national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence**.
>
> (2) Every person who— (a) attempts to commit; (b) aids or abets in the commission of; or (c) threatens to commit an offence referred to in subsection (1) shall be guilty of an offence under this Act."[24]

Section 3 of the ICCPR Act has been routinely deployed to arrest activists, journalists, content creators and comedians for their speech online, ostensibly for online speech perceived as a threat to religious and ethnic harmony (refer to section 2.3 for more details).

2. Computer Crime Act (2007) ("CCA")

CCA deals with crimes using/affecting computers/computer systems. However, in practice, it has been used for "social media regulation" in the sense that it has been used to impact the way people use social media. Section 6 of the CCA pertains to offences committed against national security, national economy and public order. It outlines that any individual who uses a computer to perform a function that endangers national security, the national economy, or public order is deemed guilty of an offence. Upon conviction, the person can face imprisonment for up to five years. The text of section 6 is relevant to demonstrate the vague nature of the provision:

24 As per the ICCPR Act Section 3(3), "a person found guilty of committing an offence under subsection (1) or subsection (2) of this section shall on conviction by the High Court, be punished with rigorous imprisonment for a term not exceeding ten years". Further as per subsection (4), "an offence under this section shall be cognizable and non-bailable, and no person suspected or accused of such an offence shall be enlarged on bail, except by the High Court in exceptional circumstances."

Section 6 (Offences committed against national security):

> "(1) Any person who intentionally **causes a computer to perform any function, knowing or having reason to believe that such function will result in danger or imminent danger to— (a) national security; (b) the national economy; or (c) public order,** shall be guilty of an offence and shall on conviction be punishable with imprisonment of either description for a term not exceeding five years.
>
> (2) In a prosecution for an offence under paragraphs (a) or (c) of subsection (1), a Certificate under the hand of the Secretary to the Ministry of the Minister in charge of the subject of Defence or, in a prosecution for an offence under paragraph (b) of subsection (1), a Certificate under the hand of the Secretary to the Ministry of the Minister in charge of the subject of Finance, stating respectively, that the situation envisaged in subsection (1) did, in fact, exist in relation to national security or public order, or the national economy, as the case may be, shall be admissible in evidence and shall be *prima facie* evidence of the facts stated therein."

This broadly-worded provision has been used to regulate online speech and expression. There have been instances of arrests for social media posts on grounds of spreading fake news or inciting violence and endangering public order (refer to section 2.3 for more detail).

3. Prevention of Terrorism Act (Temporary Provisions) Act No 48 of 1979 ("PTA")[25]

The PTA criminalises acts of terrorism and unlawful activity. It allows the authorities to arrest individuals, groups, or organisations, without a warrant, for these acts of terrorism and unlawful activities. For instance, Section 2(1) (h) of the PTA criminalises any action that causes acts of violence, disharmony, hostility or ill-will between different communities.

Section 2 (1) (h) employs the following broad and vague language to charge any person:

> "who by **words either spoken or intended to be read or by signs or by visible representations or otherwise causes or intends to cause commission of acts of violence or religious, racial or communal disharmony or feelings of ill-will or hostility between different communities or racial or religious groups."**[26]

25 Amendments passed in March 2022 are discussed under the Rule of Law section (see section 2.8).

26 As per Section 2 (2) of the PTA: "Any person guilty of an offence specified in (ii) paragraphs (c), (d), (e), (f). (g). (h). (i) or (j) of subsection (1) shall on conviction be liable to imprisonment of either description for a period not less than five years but not exceeding twenty years."

Furthermore, the PTA lacks judicial oversight in investigations and grants extensive powers to LEAs, to detain and arrest. Misuse of PTA provisions leads to frequent violation of detainees rights and negatively impacts rule of law principles.[27] Notably, the PTA was abused to detain individuals based on their social media posts following the Easter Sunday terror attacks (see Section 2.3 for more details). While the government has attempted to address criticisms by introducing amendments, experts contend that the problem of arbitrary application and potential misuse will persist, as highlighted in the proposed amendments outlined in Section 2.6.3.[28]

4. Penal Code Ordinance No 11 of 1887 (as amended) ("Penal Code")

This sets out the provisions relating to crime and their punishments. Under the Penal Code, Police can make arrests on several grounds. One such section that has been used extensively to regulate content on social media platforms is Section 120, which cracks down on any speech (including online posts) that incites disaffection or hatred towards the State. This section also criminalises other broad taxonomies of harmful conduct that attempts to provoke or create discontent or disaffection among the people of Sri Lanka or promote ill will and hostility between different classes within the population.

Section 120: ("Exciting or attempting to excite disaffection")

> "Whoever by words, either spoken or intended to be read, or by signs, or by visible representations, or otherwise, **excites or attempts to excite feelings of disaffection to the State, or excites or attempts to excite hatred to or contempt of the administration of justice, or excites or attempts to excite the People of Sri Lanka to procure, otherwise than by lawful means, the alteration of any matter by law established, or attempts to raise discontent or disaffection amongst the People of Sri Lanka, or to promote feelings of ill-will and hostility between different classes of such People**."[29]

27 *Centre for Policy Alternatives*, 'A Commentary: Prevention of Terrorism (Amendment) Bill 2022' (January 2022) <https://www.cpalanka.org/wp-content/uploads/2022/01/Final-PTA-Amendment-2022.docx-1-1.pdf>.

28 Ibid.

29 Those held liable shall be punished with simple imprisonment for a term which may extend to two years with a view to the reformation of such alleged error or defects.

Section 2.3 demonstrates how such provisions under the Penal Code are implemented to regulate online speech. For instance, this penal provision has been invoked to criminalise online posts that express criticism of the President or engage in satirical commentary against politicians.

5. Police Ordinance No 16 of 1865 (as amended) ("Police Ordinance")

This legal framework has been established to regulate the LEAs.[30] Within this ordinance, Section 98 relates to false reports that create "panic," without specifying what may constitute false and panic. The threshold of what may be considered alarming false reports and how its impact will be assessed is also unclear. This provision has been interpreted widely to govern user-generated information on social media.

Section 98: ("False reports to alarm people and create a panic")

> "Any person who shall **spread false reports with the view to alarm the inhabitants of any place within Sri Lanka and create a panic** shall be guilty of an offence."[31]

6. Public Security Ordinance, No. 25 of 1947 (as amended) ("Public Security Ordinance")

Emergency regulations are made under the Public Security Ordinance.[32] Where the President declares a state of emergency under the Public Security Ordinance, the President is thereafter empowered to make all such regulations that they deem necessary, expedient or in the interests of public security, preservation of public order, suppression of mutiny, riot or civil commotion or for the maintenance of supplies and services essential to the life of the community.[33] These regulations, when made, override all laws of the country except the Constitution (though some provisions of the Constitution are also derogable). Accordingly, in an instance where the President declares a state of emergency, the President, in their sole discretion may set out any regulation that they deem fit. Such ordinances may include regulation of social media, interception, online speech, disclosure of data, etc.

30 Police Ordinance <https://www.lawnet.gov.lk/police-4/>.

31 The guilty is "liable to a fine not exceeding two hundred rupees, or to imprisonment, with or without hard labour, for any period not exceeding twelve months ; and if he shall be convicted a second time, or shall persist in the offence after warning to desist, he shall be liable to corporal punishment not exceeding twenty lashes."

32 Public Security Ordinance No 25 1947 <https://www.srilankalaw.lk/p/968-public-security-ordinance.html>.

33 Public Security Ordinance No 25 1947, s 5(1).

In May of 2022, the Emergency (Miscellaneous Provisions and Powers) Regulations, No. 1 of 2022 ("Emergency Regulations") were notified in the gazette pursuant to the declaration of an emergency in the country.[34] These Regulations are of relevance since, for the first time, a direct reference was made to content on social/digital media. Paragraph 15 of the Emergency Regulation reads as follows:

> "No person shall, by word of mouth or by any other means whatsoever, **including digital means or social media**, communicate or spread any rumour or false statement or any information or image or message which is likely to cause public alarm, public disorder or racial violence or which is likely to incite the committing of an offence."

A state of emergency was declared in the country in July 2022.[35] The above Emergency Regulations were also re-gazetted[36] and were in force till August 2022.[37]

7. Personal Data Protection Act, No. 9 of 2022 ("PDPA")

The PDPA[38] was passed in the Parliament (and certified by the Speaker of the House on 19 March 2022). The PDPA will be implemented in a phased manner. Part V of the PDPA, which deals with the Data Protection Authority (DPA), has been brought into operation through a Gazette notification on 21 July 2023.[39] Following this, the government appointed the Board of Directors, and the DPA is likely to be functional in early 2024.[40]

---

34 Emergency (Miscellaneous Provisions and Powers) Regulations, No. 1 of 2022, Gazette Extraordinary No. 2278/23.

35 PTI, 'State of emergency declared in Sri Lanka ahead of July 20 presidential election' *The Hindu Business Line* (*Mumbai*, 2022) <https://www.thehindubusinessline.com/news/world/state-of-emergency-declared-in-sri-lanka-ahead-of-july-20-presidential-election/article65653035.ece>;

'Another state of emergency declared in Sri Lanka as acting president takes reins' (*CNBC*, 2018) <https://www.cnbc.com/2022/07/18/another-state-of-emergency-declared-in-sri-lanka-as-acting-president-takes-reins.html>.

36 No. 2289/07 - Monday, July 18, 2022.

37 Waruna Cudah Nimal Karunatilake, 'Sri Lanka Will Not Extend Emergency as Protests Tail Off' Reuters (16 August 2022) <https://www.reuters.com/world/asia-pacific/sri-lankas-state-emergency-wont-be-extended-presidents-office-2022-08-16/>.

38 Personal Data Protection Act No 9 2022 <https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf>.

39 Presidential Secretariat, 'Sri Lanka's Personal Data Protection Authority Progresses with Board of Directors Appointment' (October 2023) <https://www.presidentsoffice.gov.lk/index.php/2023/10/09/sri-lankas-personal-data-protection-authority-progresses-with-board-of-directors-appointment/#:~:text=The%20PDPA%20is%20set%20to,finance%2C%20law%20and%20regulatory%20affairs.>.

40 Hiyal Biyagamage, 'Data Protection Authority to Be Fully Functional by Early 2024: Justice Minister' *Daily FT* (13 October 2023) <https://www.ft.lk/front-page/Data-Protection-Authority-to-be-fully-functional-by-early-2024-Justice-Minister/44-754016>.

The PDPA is the comprehensive data protection legislation in Sri Lanka governing the collection, use, storage, and disclosure of individuals' personal data. The PDPA applies to all data controllers (public and private, including social media platforms) in respect of the personal data of individuals that they collect, use, store, disclose, etc (collectively "processing"). In general, data can only be processed with the consent of the data subject. However, if data is required on grounds of public interest (such as health, control of communicable disease, or for compliance with law), it can be processed without consent of the data subject.

Specifically, under Section 40 of the PDPA, exemptions, restrictions or derogations to the PDPA would be permitted, *inter alia*, for the following reasons:

- the protection of **national security**, defence, public safety, public health, economic and financial systems stability of the Republic of Sri Lanka;
- the impartiality and independence of the judiciary;
- the prevention, investigation, and prosecution of criminal offences; and
- the execution of criminal penalties.

Data controllers may also refuse data subject requests based on data security grounds. The PDPA imposes restrictions on data retention, as indicated in Schedule V, specifying the period for which personal data should be retained.[41]

While the PDPA does not require that data should be stored locally, cross-border data flows (by social media platforms, and others) are limited to an extent. The PDPA allows private entities to engage in cross-border sharing of data with countries where an "adequacy decision" has been made.

It is important to note that the PDPA is not yet in force, and no adequacy decision has been made for any jurisdiction. In the event no adequacy decision is made, the PDPA provides that the controller or processor (Buyer or Supplier who is located in Sri Lanka) of data

41 Kirk Nahra, Tamar Pinto, Ali Jessani, 'Sri Lanka Becomes the First South Asian Country To Pass Comprehensive Privacy Legislation' (*Wilmer Hale*, 2022) <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20220330-sri-lanka-becomes-the-first-south-asian-country-to-pass-comprehensive-privacy-legislation> accessed 31 August 2022>.

must ensure that the country to which data is being shared must satisfy obligations under Part I,[42] Part II,[43] and sections 20, 21, 22, 23, 24 and 25 of Part III[44] of the PDPA. The controller or processor of data should enter into appropriate agreements or instruments with the cross-border entity to ensure compliance with these provisions ("appropriate safeguards"). These appropriate safeguards will be prescribed by the Data Protection Authority. Note that the Authority is yet to be established, and no such safeguards have been prescribed.

8. Sri Lanka Telecommunications Act No 25 of 1991 (as amended) ("SLTA")

The Telecom Act is important in two ways for the regulation of social media – first because of its relevance to lawful interception of communications data, and second because of the powers it gives the regulator to control (including block) access to content.

Even though Sri Lanka does not have specific legislation addressing lawful interception of telecommunication and electronic communication content, several statutes independently provide for such interception or generally permit lawful interception of data transmitted through a telecommunications system or electronic communications in certain circumstances. Some of the laws in relation to interception have been mentioned above – CCA, PTA, and Public Security Ordinance. The PDPA does not per se allow interception/access, but it provides for processing without consent on grounds of public interest.

The SLTA[45] provides for the establishment of the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) and other related matters, including provisions dealing with lawful and unlawful interception or interference with a message, etc. The TRCSL has wide powers in respect of the issuance of telecommunication operator licences, spectrum allocation, etc.

42 Processing of personal data.

43 Rights of data subject.

44 Controllers and Processors; Section 20 – Designation of Data Protection Officer; Section 21 – Additional Obligations of a Controller; Section 22 – Additional Obligations on Processors; Section 23 – Personal Data Breach Notification; Section 24 – Personal Data Impact Assessment; Section 25 – Measures to mitigate risks of harm and the requirement for prior consultation.

45 Sri Lanka Telecommunications Act <https://www.lawnet.gov.lk/sri-lanka-telecommunications-2/>.

Section 54(3) of the SLTA permits the interception of a telecommunications message if such interception is carried out pursuant to a direction issued by the Minister in charge of telecommunications.[46, 47] Furthermore, section 54(3) also permits interception and disclosure of a message or statement of account specifying the person to which the telecommunications services are being[48] provided in connection with the investigation of any criminal offence[49] or for the purposes of any criminal proceedings.

Section 69 of the SLTA provides that due to any public emergency (or in the interest of public safety and tranquillity), the Minister may issue a direction either (i) generally and published in the Gazette or (ii) specifically in writing to any telecommunications service provided in Sri Lanka or to a telecommunications operator (a telecommunication operator licensed in Sri Lanka), an order prohibiting transmission of messages or blocking access to the internet.[50]

9. Right to Information Act, No. 12 of 2016 ("RTI Act")

The RTI Act is relevant since it has been a tool used by journalists and other citizens in accessing information relating to blocking the internet and other related areas.

The right of access to information is guaranteed as a fundamental right by Article 14A of the Constitution of Sri Lanka. The RTI Act[51] provides for the procedure in accessing this information. The RTI Act has an overriding effect over other legislations, wherein in the event of inconsistency between the RTI Act and another law, the former will prevail. The RTI Act empowers citizens to access any information which is in the "possession, custody or control of a public authority".

46 The Telecom Act does not specify that a court order is necessary to legitimise the Minister's direction. It merely provides that interception of a message is not an offence if it is done pursuant to any direction given under the hand of the Minister.

47 See section 5 for a discussion on the implications of frequently having the President as the Minister in charge of the TRCSL.

48 Under the SLTA, "telecommunication service" means a service consisting in the conveyance by means of a telecommunication system of any message, or a service consisting in the installation, maintenance, adjustment, repair, alteration, moving, removal or replacement, of apparatus which is or is to be connected to a telecommunication system.

49 The Telecom Act does not prescribe any threshold as to severity of offence in this context. As such, the powers granted under Section 54(3) of the Telecom Act are available in relation to interception in the context of any criminal investigation or any criminal proceeding.

50 Under the SLTA, "operator" means a person authorised by a licence under section 17 to operate a telecommunication system.

51 Right to Information Act 2016 <https://www.rticommission.lk/web/images/pdf/act/rti-act-en-13122018.pdf>.

The term "public authority" has been widely defined and also includes private organisations as follows:

> "a private entity or organisation which is carrying out a statutory or public function or service, under a contract, a partnership, an agreement or a licence from the government or its agencies or from a local body, but only to the extent of activities covered by that statutory or public function or service".

Under Section 5(1) of the RTI Act, there are various exemptions to information access, including considerations for privacy, defence, territorial sovereignty, national security, and adherence to international obligations. If a public authority, Information Officer, or Designated Officer rejects a request for information, the requester has the option to appeal to the RTI Commission.

2.3 Methods of Regulating Social Media in Sri Lanka

The enforcement authorities have interpreted existing statutes to encompass their concerns over cybersecurity and other ICT regulation, and used them to regulate use of social media. This is possible in part because the language of the provisions of the various laws are wide and can be interpreted to be medium agnostic.

To better illustrate how different laws are used to govern social media information ecosystem, we examine such regulation through three case studies- the 2019 Easter Sunday terror attacks; the COVID-19 pandemic (2020 onwards); and the protests against the Sri Lankan economic crisis (special focus on April 2022 onwards).

Case Study 1: Easter Sunday Terror Attacks. On 21 April 2019, eight bombs went off in Sri Lanka, targeting hotels and churches. These attacks killed over two hundred and injured over four hundred people.[52] Attempts by the government to control the spread of information via social media were seen following the attacks. The Sri Lankan

52 Shereena Qazi, 'Sri Lanka bombing: 'No one can dry our tears today'' (*Aljazeera*, 2019) <https://www.aljazeera.com/news/2019/4/21/sri-lanka-bombing-no-one-can-dry-our-tears-today>.

government blocked social media, stating that it was being used to create panic and spread misinformation.[53] Social media platforms, including Facebook Messenger, WhatsApp, Instagram, YouTube, Snapchat and Viber, were shut down in three instances, all blocks happening within a span of a month (refer to Box 3 for further information).[54]

Additionally, the Sri Lankan government resorted to arresting those who made posts online that were deemed to spread false information or hate speech or were linked to the spreading of content in favour of the attacks. Although there is a lack of transparency around the exact provisions used for each arrest, it is clear that the PTA and the ICCPR Act were mainly used.[55, 56] Some arrests were also made under the Penal Code and the Police Ordinance (refer to Box 1). It was also observed that platforms such as Facebook and YouTube took down content that violated their policies/standards.[57]

Case Study 2: The COVID-19 Pandemic. After the outbreak of the COVID-19 pandemic in early 2020, there was a great deal of focus on the spread of false information related to the pandemic and potential cures for the virus. The World Health Organization (WHO) labelled this phenomenon an "*infodemic*."[58] Given that social media is a key platform through which misinformation spreads, many governments set their sights on taking action against "fake news" spread via social media platforms.[59] However, measures taken have often proved controversial, with critics expressing concern that punishments being meted out were disproportionate, i.e. violating the basic human right principle of proportionality, or that the charge of misinformation or "fake news" was being used to silence dissent and criticism of government's handling of the pandemic.[60]

53 Associated Press, 'Sri Lanka blocks social media after Easter Sunday bombings' (*CNBC*, 2019) <https://www.nbcnews.com/tech/tech-news/sri-lanka-blocks-social-media-after-easter-sunday-bombings-n996886>.

54 Emily Stewart, 'Can Facebook Be Trusted to Combat Misinformation? Sri Lanka's Shutdown Suggests No.' *Vox* (23 April 2019) <https://www.vox.com/2019/4/23/18511640/facebook-sri-lanka-bombing-social-media-attack>.

55 Adam Bemma, 'Is Sri Lanka Using the Easter Attacks to Limit Digital Freedom?' *Al Jazeera* (8 July 2019) <https://www.aljazeera.com/features/2019/7/8/is-sri-lanka-using-the-easter-attacks-to-limit-digital-freedom>.

56 '"In a Legal Black Hole": Sri Lanka's Failure to Reform the Prevention of Terrorism Act' (*Human Rights Watch* 2022) <https://www.hrw.org/report/2022/02/07/legal-black-hole/sri-lankas-failure-reform-prevention-terrorism-act>.

57 'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*, 2021) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>.

58 'Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation' (*World Health Organisation*, 2020) <https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation>.

59 'Covid-19 Triggers Wave of Free Speech Abuse' (*Human Rights Watch*, 2021) <https://www.hrw.org/news/2021/02/11/covid-19-triggers-wave-free-speech-abuse>.

60 Ibid.

In Sri Lanka, actions taken against social media users have primarily been to arrest people for spreading false information. One of the most prominent instruments to make these arrests has been the CCA.[61] Similarly, the Penal Code and the ICCPR Act have been deployed to arrest users spreading false news.[62] It has been observed that the Sri Lankan government did not block social media or social media platforms in the years 2020 and 2021.[63]

Case Study 3: Protest Against 2022 Economic Crisis. The ongoing economic crisis in Sri Lanka, following a default on sovereign debt, led to serious shortages of essentials, including food, medicine, and electricity. This spurred mass protests across the island, calling for the resignation of President Gotabaya Rajapakse and his family members in government.[64] March 31, 2022, witnessed a large protest outside the President's home in Mirihana.[65]

Following this, multiple social media applications were blocked on April 3.[66] The protests continued in various forms after this; while some protests took place across the country, the largest were heavily concentrated in a central location in the city of Colombo, adjacent to several important government and commercial buildings. Supporters of the regime violently clashed with the protestors, the President's house was stormed by the protestors, the President fled the country, and a new President was installed. Subsequently, as President Gotabhaya Rajapakshe returned, many protestors were arrested.[67]

The Official Secrets Act was invoked to "designate public streets and government buildings in central Colombo 'high-security zones', where written permission from the police is required to hold any public gathering".[68] It gave the police wide-ranging authority to

61 Pamodi Waravita, 'No Warrant Needed for "Fake News" Arrests' *The Morning* (8 June 2021) <https://themorning.lk//articles/141524>.

62 Ibid.

63 'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*, 2021) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>.

64 Devana Senanayake, 'Inside Sri Lanka's Unprecedented Mass Protests' (*Foreign Policy*, 2022) <https://foreignpolicy.com/2022/04/26/sri-lanka-protests-rajapaksa-economic-crisis-colombo/>.

65 'Massive protests near President's private residence demanding Sri Lankan President to 'go home'' (*ColomboPage*, 2022) <http://www.colombopage.com/archive_22A/Mar31_1648747227CH.php>.

66 'Social media restricted in Sri Lanka as emergency declared amid protests,' (*NetBlocks*, 2022) <https://netblocks.org/reports/social-media-restricted-in-sri-lanka-as-emergency-declared-amid-protests-JA6ROrAQ>.

67 Agence France-Presse, 'Sri Lanka extends state of emergency as police round-up protestors' (*The Guardian*, 2022) <https://www.theguardian.com/world/2022/jul/28/sri-lanka-extends-state-of-emergency-as-police-round-up-protest-leaders>.

68 Official Secrets Act 2022 <https://www.srilankalaw.lk/Volume-VI/official-secrets-act.html>.

arrest anyone within the high-security zone. The move was criticised due to its sweeping nature to curb freedom of assembly and protest.[69] While the government claimed the high-security zone is required to ensure administration.[70] The order lacked a clear criteria for authorisation of demonstrations and enabled authorities to suppress dissent due to its potential arbitrary enforcement.[71] However, within two weeks, the President issued a new Extraordinary Gazette Notification revoking the previously published Extraordinary Gazette.[72]

Government action in these three instances showcases social media regulation through two main actions: (i) arrests and (ii) blocking of apps. These examples were drawn from what was available in the public domain, and due to this restriction, in some cases, the specific law(s) under which arrests were made is unknown.

In addition, the platforms themselves appear to engage in voluntary content takedowns, based on community guidelines or other internal platform rules. This, too, is a form of regulation, and this chapter presents instances where this happens. However, no evidence has been found of government pressure or government orders being used to force social media platforms to do so.

In the next few subsections, the report outlines these three key modes of regulating information on social media: (Box 1) Authorising arrests of individuals under laws such as the PTA, ICCPR Act and the CCA for posting unlawful content online; (Box 2) Blocking of entire social media applications for law and order concerns during protests, or an emergency like the Easter Attacks; and (Box 3) highlights the role played by platforms in voluntarily takedown of content violative of their terms of service.

69 'Sri Lanka: Revoke Sweeping New Order to Restrict Protest: Misuse of Official Secrets Act Latest Measure to Suppress Dissent', (*Human Rights Watch*, 2022) <https://www.hrw.org/news/2022/09/27/sri-lanka-revoke-sweeping-new-order-restrict-protest>.

70 'Public Security Minister says HSZs required to run administration', (*The Sunday Times*, 2022) <https://www.sundaytimes.lk/220925/news/public-security-ministry-says-hszs-required-to-run-administration-497030.html>.

71 'Sri Lanka: Revoke Sweeping New Order to Restrict Protest: Misuse of Official Secrets Act Latest Measure to Suppress Dissent', (*Human Rights Watch*, 2022) <https://www.hrw.org/news/2022/09/27/sri-lanka-revoke-sweeping-new-order-restrict-protest>.

72 Official Secrets Act 2022 <http://documents.gov.lk/files/egz/2022/10/2299-71_E.pdf>.

Box 1. Social Media Regulation Through 'Arrests'

The below-mentioned examples outline the various components of restrictions imposed on users and their online speech in Sri Lanka.

- A man was arrested for a Facebook post that was perceived as a threat/warning after the Easter Sunday attacks.[73] The concerned user had posted, "*Don't laugh more, 1 day u will cry*," for which the user was detained.
- The Facebook user Dilshan Mohamed was declared an active supporter of ISIS due to his engagement with ISIS-related content on the platform, even though his engagement was critical of their extremist views. In fact, according to journalistic reports, he has been spearheading anti-radicalisation efforts and trying to educate young people about the dangers of their violent ideology. When no incriminating posts were found, he was accused of having deleted them. Dilshan Mohamed received bail after 34 days, after which charges under the ICCPR Act were dropped, but the case continued under the PTA.[74]
- A jewellery shop owner was arrested on May 5, 2019 (during the Easter Sunday aftermath) for content allegedly posted on Facebook and charged with PTA.[75] He was released after he petitioned the Supreme Court for being unlawfully detained since there was no Detention Order.[76]

73 'Sri Lanka Blocks Social Media After Facebook Post Sparks Anti-Muslim Riot' (NDTV, 2019) <https://www.ndtv.com/world-news/sri-lanka-blocks-social-media-after-worst-unrest-since-easter-bombings-2036732>; 'Sri Lanka blocks social media again after attacks on Muslims' (*Al Jazeera*, 2019) <https://www.aljazeera.com/news/2019/5/13/sri-lanka-blocks-social-media-again-after-attacks-on-muslims>.

74 Namini Wijedasa, '"Arrest first, ask later" policy has chilling effect on Muslim community' (*The Sunday Times*, 2019) <https://www.sundaytimes.lk/190609/news/arrest-first-ask-later-policy-has-chilling-effect-on-muslim-community-352955.html>.

75 'Sri Lanka: Muslims Face Threats, Attacks' (*ReliefWeb*, 4 July 2019) <https://reliefweb.int/report/sri-lanka/sri-lanka-muslims-face-threats-attacks>.

76 'SC gives okay for FR case filed by man arrested after Easter Sunday bombings' (*The Sunday Times*, 2019) <https://www.sundaytimes.lk/191006/news/sc-gives-okay-for-fr-case-filed-by-man-arrested-after-easter-sunday-bombings-372022.html>.

- Muslim-owned shops, houses and places of worship were targeted three weeks after the Easter Sunday attack. As a result of this violence, sixty people were arrested and thirty-three were detained for further questioning. In addition to these arrests, action was also taken by detaining those who had spread hatred on social media platforms.[77]

- Kusal Perera, a journalist, was about to be arrested under the ICCPR Act for an article that went by the title "From Islamic terrorism to marauding Sinhala Buddhist violence." The President stepped in and prevented his arrest, claiming that the ICCPR Act was misused in this case.[78]

- The Terrorism Investigations Department (TID) arrested two people in 2021 who had spread media related to the Easter Sunday attacks through a WhatsApp group[79] named 'One Ummah' where extremist views were communicated and charged them with PTA.[80]

- In 2021, a nineteen-year-old boy was arrested for his post on social media: "get ready for another easter attack." This comment was a response to the ban of the burqa which was another action the government took as a safety measure in light of the attacks. He was charged with the ICCPR Act, Penal Code (Section 120) and Police Ordinance (Section 98).[81]

77 'To quench whose thirst?' (*Daily News*, 2019) <http://www.dailynews.lk/2019/05/16/features/185740/quench-whose-thirst>.

78 Colombo Telegraph, 'Friends In High Places Saving Columnist Kusal Perera: Unequal And Arbitrary Application Of ICCPR' (*Colombo Telegraph*, 2019) <https://www.colombotelegraph.com/index.php/friends-in-high-places-saving-columnist-kusal-perera-unequal-and-arbitrary-application-of-iccpr/>.

79 'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*, 2021) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>.

80 'Four including suspect who uploaded Zahran's pledge-taking video arrested' (*Adaderana*, 1 April 2021) <http://www.adaderana.lk/news.php?nid=72728>.

81 'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*, 2021) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>

- In April 2020, the then Acting Inspector General of Police Chandana D. Wickremaratne said he would "arrest those who disseminate false or disparaging statements about government officials combating the spread of the Covid-19 virus." Later that same month, the Human Rights Commission of Sri Lanka (HRCSL) communicated to the police by letter that it would be unconstitutional to carry out arrests simply for criticising policies or public officials.[82]

- A woman was arrested for posting false information on her private Facebook account that President Gotabaya Rajapakse had contracted COVID-19. The Criminal Investigation Department (CID) alleged that this post amounted to an offence committed under the CCA.[83]

- A man was arrested for posting false images on social media, claiming that the image contained the bodies of the deceased (COVID-19 patients) dumped at the Kalubowila Hospital. He was charged under the Quarantine Act, Penal Code, and Computer Crime Act.[84]

- A university student was detained for supposedly spreading a rumour that a VIP quarantine centre had been constructed.[85] Additionally, an individual was arrested for spreading false information about the nature of COVID-19 deaths (in this case about the number of people who had supposedly died of COVID-19 on the road).[86]

82 Law Library of Congress, 'Freedom of Expression During COVID-19,' (*Global Legal Research Directive*, 2020) <https://tile.loc.gov/storage-services/service/ll/llglrd/2020714999/2020714999.pdf>.

83 Manjula Basnayake, 'Directress of a dancing institute remanded for spreading false news about the President' (*Newswire*, 6 April 2020) <https://www.newswire.lk/2020/04/06/directress-of-a-dancing-institute-remanded-for-spreading-false-news-about-the-president/>; Gehan Gunatilleke, 'Covid-19 in Sri Lanka: Is Free Speech the next Victim?', (OxHRH Blog, April 2020), <https://ohrh.law.ox.ac.uk/covid-19-in-sri-lanka-is-free-speech-the-next-victim>.

84 Amani Nilar, 'Police arrests man for posting fake photos of COVID-19 deceased' *News 1st* (Colombo, 24 August 2021) <https://www.newsfirst.lk/2021/08/24/police-arrests-man-for-posting-fake-photos-of-covid-19-deceased/>.

85 'COVID-19 restrictions should not undermine freedom of expression,' (*International Commission of Jurists, Sri Lanka*, 2 September 2021) <https://www.icj.org/sri-lanka-covid-19-restrictions-should-not-undermine-freedom-of-expression/>.

86 Pavani Hapuarachchi, 'Suspect arrested over fake news on COVID-19 deaths: DIG Ajith Rohana' *News 1st* (Colombo, 14 November 2022) <https://www.newsfirst.lk/2020/11/14/suspect-arrested-over-fake-news-on-covid-19-deaths-dig-ajith-rohana/>.

- Ramzy Razeek, a retired government official who often writes posts promoting harmony between Muslims and Buddhists, was arrested for using Facebook to criticise the Sri Lankan government's policy that mandated the cremation of all victims of COVID-19, which is against Islamic practices. He wrote: "Muslims have been surrounded on all sides by racist groups operating in the country ... It is time to prepare for an ideological jihad for the country and all its citizens, using the pen and keyboard as weapons."[87] Upon his arrest, he was accused of promoting hatred which could encourage committing violence, discrimination, or hostility under the ICCPR Act.[88]

- Three social media admins were arrested by the CID following the incidents at protest sites in May 2022. One was of a man who shared posts inciting violence. Another was a 21-year-old whose posts advocated for violence and threatened public safety. The third arrest was of a TV presenter who was charged with aiding and abetting violence via social media. These individuals were charged under the CCA.[89]

- A man who condemned the army on Facebook in July 2022 and was arrested for posting hateful content against the military, which the Police claimed was made to create unrest and public disorder.[90] This arrest was done under the emergency regulations.[91]

87 'Sri Lanka: Due Process Concerns in Arrests of Muslims' (*Human Rights Watch*, 23 April 2020) <https://www.hrw.org/node/341285/printable/print>.

88 Ibid.

89 'Three social media admins including TV presenter arrested over recent unrest' (*Daily Mirror*, 19 May 2022) <https://www.dailymirror.lk/breaking_news/Three-social-media-admins-including-TV-presenter-arrested-over-recent-unrest/108-237338>.

90 'Another arrest over Facebook post – Sri Lankan Police detain man for 'hate-speech' against army' (*Tamil Guardian*, 27 July 2022) <https://www.tamilguardian.com/content/another-arrest-over-facebook-post-sri-lankan-police-detain-man-hate-speech-against-army>.

91 'Youth arrested for spreading hateful content on social media' (*Adaderana*, 26 July 2022) http://www.adaderana.lk/news/83871/youth-arrested-for-spreading-hateful-content-on-social-media>.

- In a prominent case, social media activist Thisara Anuruddha Bandara was arrested for creating a social media page critical of the President. She was arrested under section 120 of the Penal Code.[92] According to an article by Reporters Without Borders:

  > "Thisara Anuruddha Bandara, a young blogger, was taken from his home in Gampola, a town in the centre of the island, by several members of the security forces who arrived at dawn on 1 April. After several journalists sounded the alarm about Bandara's disappearance, a senior police officer in the nearby coastal city Mutwal denied any knowledge of his arrest but he later admitted to the Sri Lankan Human Rights Commission that Bandara was indeed being held at his police station's Crime Division. Bandara was released on bail the next day."[93]

  Bandara has since filed a fundamental rights petition in the Supreme Court regarding his arrest and detention, seeking LKR 100 million in damages.[94] On 21 June 2021, Bandara was released from the case against him via a verdict issued by the Colombo Magistrate's Court, citing insufficient evidence against Bandara to pursue the case.[95]

Box 2. Social Media Regulation through the 'Blocking of Apps'

The two case studies, the Easter Sunday Terror Attacks and the Protest Against 2022 Economic Crisis, have evidenced blocking of apps. This is done with the rationale of quelling panic and the spread of false information, as social media provides easy access to misinformation.

92 'Social media activist Anuruddha Bandara granted bail,' (*Colombo Page*, 3 April 2022) <http://www.colombopage.com/archive_22A/Apr03_1648963819CH.php>.

93 'At least nine journalists injured during Sri Lanka protests' (*Reporters Without Borders*, 7 April 2022) <https://rsf.org/en/least-nine-journalists-injured-during-sri-lanka-protests?>.

94 'Activist Anuruddha Bandara files FR Petition against Police seeking Rs. 100 million in damages,' (*Colombo Page*, 29 April 2022) <http://www.colombopage.com/archive_22A/Apr29_1651255915CH.php>.

95 Amani Nair, 'Social Media activist Anuruddha Bandara released.' (*News 1st*, 21 June 2022) <https://www.newsfirst.lk/2022/06/21/social-media-activist-anuruddha-bandara-released/>.

However, this was not the first time social media was blocked as a means to stop racial/religious violence. In 2018, there were anti-Muslim riots. According to Article One's[96] report "Assessing the Human Rights Impact on the Facebook Platform in Sri Lanka," rumours and hate speech during this time, which were spread via Facebook, could have played a part in offline violence.[97] Facebook, WhatsApp, Instagram, and Viber were blocked under the rationale of preventing the spread of hate speech in the aftermath of anti-Muslim mob violence.[98] It is understood that the government has used the provisions of the SLTA and the applicable licence conditions to implement these blocks through licensed ISPs.[99]

Online censorship during the Easter Sunday Terror Attacks

As a state of emergency was called, the government blocked all social media apps the very next day after the Easter Sunday attacks. The apps which were blocked were Facebook, Messenger, WhatsApp, Instagram, YouTube, Snapchat, Viber and TunnelBear (a VPN).[100]

The Easter Sunday incident had such a big impact that social media was blocked not only once but three times, with all blocking periods happening within a span of a month.

- First block: 22nd – 30th April 2019, implemented the day after the Easter Sunday attacks.

96 Article One is a management consultancy international private organisation working with leading companies around the world, in areas such as human rights, responsible innovation and social impact.

97 'Assessing the Human Rights Impact on the Facebook Platform in Sri Lanka [2018]' (Article One, 2018) <https://about.fb.com/wp-content/uploads/2020/05/Sri-Lanka-HRIA-Executive-Summary-v82.pdf>.

98 Vindu Goel, Hari Kumar and Sheera Frenkel, 'In Sri Lanka, Facebook Contends With Shutdown After Mob Violence' New York Times (Mumbai, 8 March 2018) <https://www.nytimes.com/2018/03/08/technology/sri-lanka-facebook-shutdown.html>.

99 Press Trust of India, 'Sri Lanka Lifts Ban on Facebook after Assurance from Social Media Giant' *Business Standard* (15 March 2018) <https://www.business-standard.com/article/international/sri-lanka-lifts-ban-on-facebook-after-assurance-from-social-media-giant-118031500791_1.html>.

100 *NetBlocks*, (*Twitter*, 22 April 2019) <https://twitter.com/netblocks/status/1120297427871903744>.

- Second block: only for 10 hours on May 5, 2019, which was the result of a brawl in Negombo that got out of hand.[101]
- Third block: for four days, following attacks on mosques and shops owned by Muslims.[102] In addition to the previously stated apps, Twitter was blocked for the first time on May 13, 2019, during the third block.[103]

In each instance, the government turned to blocking these social media apps because they argued that racial tensions were high and, therefore, misinformation and hate speech were spreading rapidly.[104] The government even blocked some Virtual Private Networks (VPNs) to prevent users from accessing these social media platforms.[105]

Crackdown on Protests Against 2022 Economic Crisis

After midnight on Sunday, April 3, 2022, Facebook, WhatsApp, Viber, Twitter, YouTube, Instagram, TikTok, Telegram, Facebook Messenger, Snapchat and IMO were blocked for a period of 16 hours.[106] The ban appeared to have backfired, however, with many users simply resorting to VPNs to access social media. As a result, protest hashtags such as #GoHomeRajapakses and #GoHomeGota ("Gota" is President Gotabaya Rajapakse) were seen trending in other countries.[107]

101 U.S Department of Justice, 'Sri Lanka' <https://www.justice.gov/eoir/page/file/1239311/download>.

102 Ibid.

103 'Sri Lanka blocks social media for third time in a month' (*NetBlocks*, 13 May 2019) <https://netblocks.org/reports/sri-lanka-blocks-social-media-for-third-time-in-one-month-M8JRjg80>.

104 'Sri Lanka bombings: All the latest updates' (*Al Jazeera*, 2 May 2019) <https://www.aljazeera.com/news/2019/5/2/sri-lanka-bombings-all-the-latest-updates>.

105 'VPN services blocked in Sri Lanka as information controls tighten' (*NetBlocks*, 24 april 2019) <https://netblocks.org/reports/vpn-services-blocked-in-sri-lanka-as-information-controls-tighten-RAe2blBg>.

106 'Social media restricted in Sri Lanka as emergency declared amid protests,' (*NetBlocks*, 2 April 2022) <https://netblocks.org/reports/social-media-restricted-in-sri-lanka-as-emergency-declared-amid-protests-JA6ROrAQ>; 'Sri Lanka blocks social media, arrests economic crisis protestors,' (*EconomyNext*, 3 April 2022) <https://economynext.com/sri-lanka-blocks-social-media-arrests-economic-crisis-protestors-92443/>.

107 'Social media ban backfires: Anti Govt slogans trends in other countries,' (*Newswire*, 3 April 2022) <https://www.newswire.lk/2022/04/03/social-media-ban-backfires-anti-govt-solgans-trends-in-other-countrie/>.

After a backlash against the move, the ban was lifted.[108] The ban was imposed by the Telecommunications Regulatory Commission of Sri Lanka (TRCSL), which stated that it was acting on a request from the Ministry of Defence.[109] The Human Rights Commission of Sri Lanka (HRCSL) stated that the TRCSL did not have the power to limit access to social media using the Ministry of Defence's request as a basis to do so.[110] The HRCSL also noted that the general ban on social media was a violation of human rights.[111] The Bar Association of Sri Lanka (BASL) also criticised the ban, stating that "social media is a 'vital aspect' of the freedom of expression and as important as traditional media."[112] On April 4, 2022, the HRCSL stated that it had summoned the Inspector General of Police (IGP), the TRCSL chairman, the Secretary of the Ministry of Defence and the Secretary of the Ministry of Mass Media and Information to the Commission the next day.[113] The Commission was also to inquire into the block on social media as well as alleged assaults on journalists and civilians.[114]

The Sri Lankan civil society group Hashtag Generation also filed a Right to Information Request with the TRCSL, requesting "Certified copies of written directions from Ministry of Defence to the Telecommunications Regulatory Commission requesting for restriction of social media platforms and communications actions in March and April 2022" and "Certified copies of all written communication between Ministry of Defence and Telecommunications Regulatory Commission on the restriction of social media platforms and communications applications in March

108 Meera Srinivasan, 'Sri Lanka crisis: Government restores access to social media following backlash,' (*The Hindu*, 3 April 2022) <https://www.thehindu.com/news/international/sri-lanka-crisis-government-restores-access-to-social-media-following-backlash/article65286448.ece>.

109 Ibid.

110 Ibid.

111 Zulfick Farzan, 'Imposing Social Media Ban a violation of Human Rights – SL Human Rights Chief' (*News 1st*, 3 April 2022) <https://www.newsfirst.lk/2022/04/03/imposing-social-media-ban-a-violation-of-human-rights-sl-human-rights-chief/>.

112 Meera Srinivasan, 'Sri Lanka crisis: Government restores access to social media following backlash' (*The Hindu*, 3 April 2022) <https://www.thehindu.com/news/international/sri-lanka-crisis-government-restores-access-to-social-media-following-backlash/article65286448.ece>.

113 'HRCSL summons key officials over human rights violation,' (DailyFT, 4 April 2022) <https://www.ft.lk/news/HRCSL-summons-key-officialsover-human-rights-violation/56-732971>.

114 Ibid.

and April 2022."[115] The request was rejected on the grounds that "disclosure of such information would undermine the defence of the state or national security," citing Section 5 (1) b (i) of the Right to Information Act.[116] Hashtag Generation has stated their intention to appeal the decision.[117]

Box 3. Social Media Regulation through 'Content Takedowns'

Though this did not involve any government actions, it was observed that platforms such as YouTube and Facebook took down content due to a violation of the respective platform's policies/standards during the Easter Sunday Terror Attacks. However, the government does not have an intermediary liability framework, therefore these voluntary blocks aim to enforce the platform's terms of service.

- Facebook stated that they removed content that violated their standards as they continue to support first responders and LEAs.[118] Zahran Hashim, who was one of the alleged perpetrators of the Easter Sunday attacks, had content in the Tamil language uploaded on Facebook, much of which Facebook has removed in response to complaints that they received.[119]
- Zahran Hashim's content on YouTube was taken down. YouTube stated that it was removing all his videos. The only content to remain relating to him are those which reported on his conduct in the attacks.[120] YouTube took down content if it violated its policies, or when such content was flagged in a request.[121] A case in point would be when SkyNews identified and pointed out videos related to Zahran Hashim on the platform which were then removed.[122]

115 Hashtag Generation, 'Our Right to Information Request to the...' (*Twitter*, 27 April 2022) <https://twitter.com/generation_sl/status/1519272806533693440?cxt=HHwWgIDQ5a2kxZUqAAAA>.

116 Ibid; RTI Act Sri Lanka, <https://www.rti.gov.lk/images/resources/RTI_Act_Sri_Lanka_E.pdf>.

117 Hashtag Generation, 'Our Right to Information Request to the...' (*Twitter*, 27 April 2022) <https://twitter.com/generation_sl/status/1519272806533693440?cxt=HHwWgIDQ5a2kxZUqAAAA>.

118 'Sri Lankan officials shut down Facebook, WhatsApp after bombing' (*CNBC*, 22 April 2019) <https://www.cnbc.com/2019/04/22/sri-lankan-officials-shut-down-facebook-whatsapp-after-bombing.html>.

119 'Sri Lankan Islamist Called for Violence on Facebook Before Easter Attacks' (*The Wall Street Journal*, 30 April 2019) <https://www.wsj.com/articles/sri-lankan-islamist-called-for-violence-on-facebook-before-easter-attacks-11556650954>.

120 'Sri Lanka attacks: Hate preacher Zahran Hashim's videos ,did not violate' YouTube policies' (*SkyNews*, 24 April 2019) <https://news.sky.com/story/sri-lanka-attacks-youtube-defends-hosting-videos-featuring-hate-preacher-zahran-hashim-11702203>.

121 Ibid.

122 Ibid.

2.4 Regulating the Online Information Ecosystem

The case studies in the preceding section show that ICT regulation that is not ostensibly targeted at social media platforms can nonetheless be deployed to regulate the flow of online information. The main mechanisms for the Sri Lankan government to thus regulate the online information ecosystem include: (a) criminalisation of online speech and arresting individuals;[123] (b) limiting internet access by blocking social media apps; and (c) interception of online communication by LEAs.[124]

It is important to note here that there have been no reported instances of the Sri Lankan government issuing orders to block/take down specific pieces of content on social media platforms. Content has been taken down by platforms voluntarily for violating their terms of service.

2.5 Institutional Mapping

This section maps governmental institutions which have an impact on social media regulation are as follows:

Name of Institution	Role of Institution
Telecommunications Regulatory Commission of Sri Lanka (TRCSL)	TRCSL is the government body that regulates the telecommunications industry in Sri Lanka, under the Sri Lanka Telecommunication Act. The provisions of the SLTA and the relevant licence conditions empower the TRCSL to direct licensed ISPs to block content upon the advice of the Minister in Charge. In the recent past, it has been observed that these decisions/ orders on blocking are taken by the Ministry of Mass Media or Ministry of Defence

123 Majority of the arrests were made for posts on Facebook.

124 Sri Lanka Telecommunications Act <https://www.lawnet.gov.lk/sri-lanka-telecommunications-2/>. See section 2.2.2 for more details.

	who in turn direct the TRCSL to communicate these mandates to the relevant ISPs.[125] Note that these ISPs are licensed operators in Sri Lanka.
Information and Communication Technology Agency (ICTA)	ICTA is the main government body tasked with implementing the Government's Policy and Action Plan relating to ICT under the Information and Communication Technology Act No. 27 of 2003, amended by Act No. 33 of 2008. The Inter Ministerial Committee (IMC) under ICTA advises the government on the formation of laws and policies in regard to ICT. Examples of Acts led by ICTA are: the PDPA, the Electronic Transactions Act, CCA and the Draft Cybersecurity Bill.
Police and the Criminal Investigation Department (CID)	The CID is a branch of the Police focused on criminal investigation. As seen in the case studies many of the documented regulatory actions consist of arresting social media users. The police and the CID have been involved in this regard, with the police spokesperson stating in 2021 that the CID had been instructed to deploy teams to monitor cyberspace for "fake news."[126]
Terrorism Investigation Division (TID)	The TID falls as a division under the Police, carrying out actions under the PTA. As seen in the Easter Sunday case study, the TID did make arrests on the basis of messages sent on WhatsApp.[127]
Defence Ministry	The objective of the Ministry of Defence is to ensure national safety. Actions by the Ministry have been taken in this regard. As the third case study reported, the TRCSL received a request from the Defence Ministry to restrict access to social media, which it then acted upon. However, the validity of this request has been questioned by the HRCSL.

125 Telecommunications Regulatory Commission of Sri Lanka, 'Empowering Sri Lanka's Digitization & Eradicating the Digital Divide' (2020) <https://www.parliament.lk/uploads/documents/paperspresented/1662013459028089.pdf>.

126 'CID Teams to Monitor Fake News: DIG Ajith Rohana' *The Morning* (7 June 2021) <https://themorning.lk//articles/141187>.

127 See case study 1 in section 2.3.

Mass Media and Information Ministry	The Ministry of Mass Media & Information carries out policy and strategy actions regarding the establishment of "a people friendly, development-oriented, free and responsible Sri Lankan media culture."[128] As noted previously, the Mass Media Ministry has issued blocking orders/requests on multiple instances.[129]
Sri Lanka Computer Emergency Readiness Team (SLCERT)	SLCERT is mandated with the task of protecting Sri Lanka's cyberspace both by reacting to [cyber] attacks and by proactively strengthening defences against potential attacks. When the 2019 Cyber Security Bill was drafted, it was SLCERT that called for public input on the draft. On its website, SLCERT provides information on cyber issues. One category it tracks and reports is the number of "social media incidents" annually. However, there are no further details available on what this data means. A 2021 Democracy Reporting International report on social media regulation in Sri Lanka elaborates on the role of SLCERT, which is limited to providing technical assistance to resolve social media incidents like hacking of accounts or the creation of fake accounts.[130]

128 Ministry of Mass Media <https://www.media.gov.lk/about-us>.

129 Raisa Wikremetunge, 'Blocked: RTI requests reveal process behind blocking of websites in Sri Lanka' (*Groundviews*, 12 August 2017) <https://groundviews.org/2017/12/08/blocked-rti-requests-reveal-process-behind-blocking-of-websites-in-sri-lanka/>.

130 As per the report, "*With respect to incidents on social media, specifically, SLCERT only provides technical assistance to resolve social media incidents. According to its website, SLCERT does not provide support to trace or take legal action against perpetrators. It also does not remove content on social media platforms or block websites. However, SLCERT can provide support for removing fake accounts, hacked accounts, and reporting content that violates the privacy policy/community standards of social media platforms and other websites. These conditions point to the limited role that SLCERT can play to combat hate speech online. Therefore, SLCERT can only provide support if a social media account is hacked, or if a fake profile is created and used to generate content constituting hate speech.*"

See Regulating Social Media in Sri Lanka: An Analysis of the Legal and Non-Legal Regulatory Frameworks in the Context of Hate Speech and Disinformation' (*Democracy Reporting International*, 2021) <https://democracyreporting.s3.eu-central-1.amazonaws.com/images/3635DRI_Regulating%20Social%20Media%20in%20Sri%20Lanka_Report_Revised%20March%202021.pdf>.

Right to Information Commission (RTIC)	The RTIC is an independent commission established under the RTI Act. The Commission as the appellate body has the powers to hold inquiries, examine persons under oath, inspect information held by public authorities, direct publication of information as held by public authorities, etc. The RTIC has ordered disclosure of information regarding blocking of websites by TRCSL and the procedure thereof. An RTI request revealed some of the government's blocking procedures.[131] This RTI decision has been detailed below.

Besides the existing institutions, there are two other relevant government institutions that are supposed to be set up, under laws that are yet to be enacted. One is the Digital Infrastructure Protection Agency of Sri Lanka (DIPA) and the other is the Data Protection Authority of Sri Lanka. We discuss these further in the Future Trends section.

2.5.1 Other Relevant Non-Governmental Institutions

In addition to the above, there are non-governmental institutions whose actions have or may have an impact in the way social media is governed. The following list is not exhaustive, and we have limited the institutions that were observed during the research of the three case studies, as well as some others which hold major prominence.

131 'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*, 2021) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021> ; discussed in detail in section 2.8 Implications of Rule of Law analysis.

Name of Institution	Role of Institution
Bar Association of Sri Lanka (BASL)	The BASL is a legal union of all lawyers in Sri Lanka. During national issues or crises, the BASL makes certain the law is maintained.[132] As observed in the third case study, the Bar Association acted as a voice condemning the block of social media as it went against the right to freedom of expression.[133]
The Human Rights Commission of Sri Lanka (HRCSL)	HRCSL is an independent commission which ensures that the human rights of all Sri Lankan citizens are protected within the law, policy and practice. It was established in 1997 under the Human Rights Commission Act No. 21 of 1996. The commission aims to protect fundamental rights guaranteed under the Sri Lankan Constitution and ensure adherence to human rights standards under international law.[134] As the third case study reported, the HRCSL stated that TRCSL could not block social media on the Defence Ministry's request and has thus summoned the Inspector General of Police (IGP), the TRCSL chairman, the Secretary of the Ministry of Defence, and the Secretary of the Ministry of Mass Media and Information to the Commission the very next day. The first case study also points in a letter to the police that actions/arrests made must be within the law.
The Free Media Movement of Sri Lanka (FMM)	The FMM is an organisation built of journalists and rights activists who protect Sri Lanka media rights as well as address Freedom of Expression issues.[135]

132 Bar Association of Sri Lanka (BASL)<https://basl.lk/basl/>.

133 See section 2.3, Box 2.

134 The Human Rights Commission Act No. 21 of 1996.

135 Free Media Movement <https://www.fmmsrilanka.lk/who-we-are/>.

	The FMM expressed their concerns when the then police spokesman announced that the CID was instructed to deploy teams to monitor cyberspace for "fake news", as there was no clear definition of the term "fake news".[136]
Sri Lanka Press Institute (SLPI)	SLPI is the leading media institute in Sri Lanka. SLPI has an RTI segment where several RTI details are addressed, including what some RTI requests have revealed. At the end of 2020, SLCERT shared information with SLPI about the number of cyber incidents occurring from March 2020 to November 2020. This came through the RTI Act. It was noted that, within this 8-month window, there were 13,855 "social media incidents".[137]

2.6 Future Trends

There has been some discourse about new laws to regulate cybersecurity and social media. However, there have been few concrete details about the said laws. The proposed Online Safety Bill is one of the key proposed legislations that aims to regulate social media platforms and end-users. However the bill poses multiple challenges, while also drawing criticism for falling short of addressing online safety concerns.

2.6.1 Online Safety Bill 2023

On September 18, 2023, the Ministry of Public Security introduced the Online Safety Bill,[138] and the Bill was subsequently presented to the Parliament on October 3 by the Minister of Security. It was challenged in the Sri Lankan Supreme Court, with 46 petitions filed challenging the Bill.[139]

136 Pamodi Waravita, 'No warrant needed for 'fake news' arrests' (*The Morning*, 9 June 2021) <https://www.themorning.lk/no-warrant-needed-for-fake-news-arrests/>.

137 'Attention Internet Users!' (*Sri Lanka Press Institute*) <http://rtisrilanka.lk/en/attention-internet-users/>.

138 Online Safety Bill 2023 <http://documents.gov.lk/files/bill/2023/10/391-2023_E.pdf>.

139 Lakmal Sooriyagoda, 'SC Concludes Hearing into Online Safety Bill' *The Daily Mirror* (21 October 2023) <https://www.dailymirror.lk/print/front-page/SC-concludes-hearing-into-Online-Safety-Bill/238-269622>.

On 25th October 2023, it was reported[140] that Minister of Security Tiran Alles, who presented the Bill to the Parliament, would be retracting the Bill and reintroducing it with amendments. However, on 28th October, the Minister stated that the Bill had not been officially withdrawn and that the Government was waiting for the Supreme Court determination on the Bill.[141]

The Supreme Court determination on the Bill was released on 7th November 2023. The Supreme Court determined that the Bill can be passed by a simple majority - however for this to happen there should be committee-stage amendments on many of the clauses .[142] The determination stated that Clauses 3, 5, 7, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 36, 37, 42, 45, 53 and 56 require a special majority in Parliament to be enacted into law. However, if the amendments proposed by the Attorney-General (AG), unless otherwise specified by the Court, are introduced to these clauses, the Court determined that the Bill may be enacted with a simple majority in Parliament.

The Supreme Court observed that certain amendments to these clauses can cure their inconsistency with the Constitution, and if that is done at the Committee Stage of Parliament, the Bill can be enacted with a simple majority in Parliament.

In the determination the SC first reproduces all the amendments which were proposed by the Attorney General to the Bill. The determination then comments on some clauses and proposes additional amendments.

The determination also states that certain clauses should be deleted. For example, clause 16: false statements (wounding the religious feelings of any other person) and clause 20 (intentionally insulting by communicating a false statement, and thereby gives provocation to any other person, intending or knowing it to be likely, that such provocation will cause such target person to break the public peace, or to commit any other offence)

140 Sulochana Ramiah Mohan, 'Minister Alles to Amend "Online Safety Bill"' Ceylon Today Daily (24 October 2023) <https://ceylontoday.lk/2023/10/25/minister-alles-to-amend-online-safety-bill/>.

141 Skandha Gunasekara, 'Social Media Regulation: Minister Steadfast on Regulation Even without Online Safety Bill' *The Morning* (28 October 2023) <https://themorning.lk//articles/4Rmxgxo8uwfjchbeo3BP>.

142 'Online Safety Bill: SC Reveals Opinion' *NewsWire* (7 November 2023) <https://www.newswire.lk/2023/11/07/online-safety-bill-sc-reveals-opinion/>.

The Supreme Court determination has been met with varying reactions. Some commentators have pointed out that stipulating that multiple amendments have to be made at the Committee stage means that the Court has not given the Online Safety Bill a green light. Proper compliance the determination will require, time effort, and careful consideration.[143]

Other commentators, however, argue that while the SC determination makes positive changes, it does not go far enough to address problematic issues with the Bill, and that some of the amendments may even have a negative effect.[144]

The provisions of the Bill are discussed in more detail below. The Bill, if implemented, will result in a comprehensive overhaul of Sri Lanka's social media regulatory framework.

The Bill establishes the Online Safety Commission, defines the roles and responsibilities of intermediaries and introduces content-based offences aimed at regulating the online information ecosystem.

The current preamble of the Bill reads as "An Act to establish the Online Safety Commission; to make provisions to prohibit online communication of certain statements of fact in Sri Lanka..." As per the Supreme Court determination, this will be changed through Committee stage amendments to "... An Act to establish the Online Safety Commission to provide safety from prohibited statements made online ..."

Section 3 of the Bill sets out its objectives, including protecting persons from false statements that may be "threatening, alarming or distressing". These words will be replaced, as it is now an objective of the Bill to "protect persons against damage caused by the communication of prohibited statements".

Lack of clarity in defining offences

The Bill was criticised for laying down broad and vague offences. The Bill centres on prohibition of "communication of false statements". It defines false statements ambiguously as "a statement that is known or believed by its maker to be incorrect or untrue and is

143 Maneesha Dullewe, 'Online Safety Bill: Not out of the Woods?' *The Morning* (11 November 2023) <https://themorning.lk//articles/PhpqK2qdolpRefZMjhmf>.

144 'Committee-Stage Amendments to Sri Lanka's "Online Safety Bill": CPA Concerned' (*EconomyNext*, 2 November 2023) <https://economynext.com/committee-stage-amendments-to-sri-lankas-online-safety-bill-cpa-concerned-13869>.

made especially with intent to deceive or mislead but does not include a caution, an opinion or imputation made in good faith."[145] A statement is defined as "any word including abbreviation and initial, number, image (moving or otherwise), sound, symbol or other representation, or a combination of any of these".[146]

The offences laid down in the Bill included the following; prohibition of false statement of fact which is "a threat to national security, public health or public order or promotes feelings of ill-will and hostility between different classes of people, by communicating a false statement",[147] "wantonly giving provocation by false statement to cause riot",[148] "Disturbing a religious assembly by a false statement,"[149] false statement with the intent to wound religious feelings of a person or class of persons,[150] false statement with the intent to provoke a breach of peace,[151] and other offences.

Online Safety Commission and procedures

The Bill provides for the establishment of an Online Safety Commission to perform the powers and functions to achieve the objectives set out in the Bill (Section 4). The Bill currently states that the Commission would consist of five members to be appointed directly by the President. According to the Supreme Court Determination, this will be amended at the Committee stage, so that the Commission shall consist of five members appointed by the President, subject to the approval of the Constitutional Council.

The Committee stage amendments will also amend the provisions for removal of a commission member – "A member of the Commission may be removed from his office by the President, subject to the approval of the Constitutional Council" (Previously, the Bill simply stated that "The President may, for reasons assigned, remove a member of the Commission from his office.")

145 Online Safety Bill 2023, s 56.
146 Online Safety Bill 2023, s 56.
147 Online Safety Bill 2023, s 12(a).
148 Online Safety Bill 2023, s 14.
149 Online Safety Bill 2023, s 15.
150 Online Safety Bill 2023, s 16 and 17.
151 Online Safety Bill 2023, s 20.

The Commission will wield extensive powers, including the authority to issue content blocking and internet suspension orders.

The Bill provides the Online Safety Commission with the powers to determine what constitutes a false statement. A person "aggrieved by the communication of a prohibited statement", could orally, in writing or through electronic form submit a complaint to the Commission.[152] Where possible, the complainant should also serve a copy of the complaint to the person or persons making or communicating the prohibited statement and any internet access service provider or internet intermediary. If the Commission decided that "sufficient material exists that a prohibited statement has been communicated", the Commission would have to carry out investigations and could issue notice on the person to take measures to prevent circulation of the statement.[153] The person would have to comply with the notice within 24 hours.

The Bill, in its current form, has no provision for the affected person to appeal against the notice issued by the Commission, which is very problematic and a violation of the principles of natural justice. There was also no indication of how checks and balances would be imposed on the powers of the Commission (the power of appointing commission members lay solely with the President).

If the person did not comply with the notice within 24 hours, "the Commission had the power to issue a notice to the internet access service provider or internet intermediary on whose online location the prohibited statement had been communicated to (a) to disable access by the end users in Sri Lanka to such prohibited statement; or (b) to remove such prohibited statement from such online location".[154]

This procedure will now be slightly amended through the Committee stage amendments.

A Committee Stage Amendment will be made to confer power on the Commission to hear the person who is alleged to have communicated the prohibited statement, during the course of an investigation carried out by the Commission.

152 Online Safety Bill 2023, s 26(1).

153 Online Safety Bill 2023, s 26(5), 26(6).

154 Online Safety Bill 2023, s 26(7).

Further, the Committee Stage Amendment would be moved, requiring the Commission to apply to the Magistrate's Court where there has been non-compliance with its notice in terms of Clauses 26(6b) and 26(8) of the Bill.

The Bill also lays down an alternative procedure for any person affected by the communication "of any prohibited statement" to apply directly to the Magistrates Court to obtain an order to prevent the circulation of such information.[155]

Furthermore, the Commission is equipped to issue directives to persons, service providers or intermediaries who have "*published or communicated or whose service has been used to communicate any prohibited statement*" to provide an opportunity to those aggrieved by such a statement to respond to it.[156]

Further, the Bill makes provisions to identify and declare online locations used for prohibited purposes in Sri Lanka. It further empowers the Commission to "make recommendations to disable access to the information disseminated through such online location".[157]

The Bill also lays down the framework for Sri Lanka's intermediary liability framework. Any service provider[158] is exempted from liability for the communication of prohibited statements unless it "(a) has initiated the communication; (b) has selected the end user of the communication; (c) has selected or modified the content of the communication; or (d) has not complied with the provisions of this Act and any regulation or rule made thereunder, in providing the service".[159]

The Bill overhauls Sri Lanka's social media regulatory framework. If the Bill is implemented it will mark a stark change for social media regulation in Sri Lanka, as currently there is no law empowering the state to block specific pieces of content on social media via notices.

155 Online Safety Bill 2023, s 27.

156 Online Safety Bill 2023, s 11(a).

157 Online Safety Bill 2023, s 11(h).

158 Including (a) an internet intermediary service; (b) a telecommunication service; (c) a service of giving public access to the internet; or (d) a computer resource service.

159 Online Safety Bill 2023, s 31(2).

OSB has been criticised by various international organisations, including the International Commission of Jurists. ICJ contended that the wide range of powers granted to the Commission, the lack of checks and balances, disproportionate punishments and the vague overbroad definition of offences raise severe human rights concerns.[160]

Codes of practice and registration of 'websites providing social media platforms'

The Bill stipulates that the Commission on Online Safety has the power to "... issue codes of practice" (specifying the security practices and procedures to be followed) by service providers and internet intermediaries who provide internet-based communication services to the end users in Sri Lanka, and to register, "...in such manner as may be specified by rules made under this Act, the websites providing social media platforms to the end users in Sri Lanka". It was not clear what purpose is served by requiring registration in this manner.

The process for this is set out in Section 53. The commission is required to hold public consultations for two weeks prior to issuing the codes of practice. (There was no such stipulation for public consultation regarding registration of websites)

Offences against children and other specific forms of harassment

The Bill also introduces new offences aimed at protecting persons from disclosure of private information resulting in harassment. For instance, section 22(1) states that, 'any person, whether in or outside Sri Lanka who wilfully makes or communicates a statement of fact, with the intention to cause harassment to another person (in this section referred to as the "target person"), by publishing any "private information" of the target person or a related person of the target person, and as a result causes the target person or any other person harassment, commits an offence.'.

While the introduction of these provisions filled a needed gap, it did not counteract the effects of the rest of the Bill.

160 *International Commission of Jurists, Sri Lanka* (29.09.2023) Proposed Online Safety Bill would be an assault on freedom of expression, opinion, and information. <https://www.icj.org/sri-lanka-proposed-online-safety-bill-would-be-an-assault-on-freedom-of-expression-opinion-and-information/>.

Current status and criticisms against the Bill

At the time of writing (8th November 2023), the Supreme Court determination had just been issued stating that the bill can be passed in parliament by a simple majority subject to amendments made at the Committee stage to 31 of its provisions.[161]

The Bill has been met with significant opposition from opposition political parties,[162] civil society,[163] and platforms.[164] It has been widely criticised for violating freedom of expression. The provisions related to the setting up and functioning of the Online Safety Commission and the vague and overbroad wording of conduct designated as punishable offences have come in for particular censure.[165]

The Bar Association of Sri Lanka has called for both the Online Safety Bill and the Anti-Terrorism Bill to be withdrawn, stating that these will have "... a serious impact on democracy and the rule of law in the country', and noting that both Bills were introduced without due consultation with the stakeholders including the BAS".[166]

The Human Rights Commission of Sri Lanka issued a detailed set of recommendations regarding the Bill, including a recommendation that the powers and functions of the Commission be confined to raising awareness and educating the public on online safety, and making recommendations to a relevant court of law, and that any restriction (i.e., directives and notices to persons, internet access service providers, and internet intermediaries) on statements or online locations be imposed only pursuant to an order of a competent court of law.[167]

161 'Committee-Stage Amendments to Sri Lanka's "Online Safety Bill": CPA Concerned' (*EconomyNext*, 2 November 2023) <https://economynext.com/committee-stage-amendments-to-sri-lankas-online-safety-bill-cpa-concerned-138692>.

162 Opposition Files Petition against Online Safety Bill' (*NewsWire*, 4 October 2023) <https://www.newswire.lk/2023/10/04/opposition-files-petition-against-online-safety-bill/>.

163 After Protests, Sri Lanka Minister Agrees to Consult Controversial Online Safety Bill' (*EconomyNext* ,8 October 2023) <https://economynext.com/after-protests-sri-lanka-minister-agrees-to-consult-controversial-online-safety-bill-134292>.

164 Niresh Eliatamby, 'World's Social Media and Tech Giants Slam Sri Lanka's Online Safety Bill as a "Draconian System to Stifle Dissent"' (*Newsfirst*, 2 October 2023)

165 *International Commission of Jurists, Sri Lanka* (29.09.2023) Proposed Online Safety Bill would be an assault on freedom of expression, opinion, and information. <https://www.icj.org/sri-lanka-proposed-online-safety-bill-would-be-an-assault-on-freedom-of-expression-opinion-and-information/>.

166 Niresh Eliatamby, 'BASL Demands Withdrawal of Anti-Terrorism and Online Safety Bills' (23 September 2023) <https://english.newsfirst.lk/2023/9/23/basl-demands-withdrawal-of-anti-terrorism-and-online-safety-bills>.

167 Human Rights Commission of Sri Lanka (02.10.2023) <https://www.hrcsl.lk/press-notice-no-hrc-p-i-e-02-10-23/>.

The Supreme Court determination has been met with varying reactions. Some commentators have pointed out that stipulating that multiple amendments have to be made at the Committee stage means that the Court has not given the Online Safety Bill a green light. Proper compliance the determination will require time, effort, and careful consideration.

Other commentators, however, argue that while the SC determination makes positive changes, it does not go far enough to address problematic issues with the Bill, and that some of the amendments may even have a negative effect. The proposed amendment to Section 11(i) of the Bill[168] would have the effect of enhancing the role of the Online Safety Commission from a regulator of 'prohibited statements' to an autonomous investigative agency.[169] Another amendment is proposed to Clause 37(1) of the Bill. The gazetted Bill authorised the Minister to appoint private individuals as "experts" to assist in the investigation of the commission of an offence subject to the courts deeming such appointment "necessary". However, the amendment now allows the Minister to appoint "experts" without prior approval by the courts.

The Supreme Court determination noted that "...regulation of the internet has become an urgent need of the world. Therefore, several countries such as the United States of America, France, Germany, Australia, South Korea, Singapore and China have enacted legislation to regulate the internet." (Page 34).

The determination goes on to say that "...the protection of freedom of expression has highlighted that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the internet. In particular, they recommend the development of tailored approaches for responding to illegal content online, as well as pointing out that specific restrictions for material disseminated over the internet are necessary." (Page 36).

168 The current clause 11(i) of the Bill reads,"*to carry out such investigations and provide such services upon being directed by any court". The proposed amendment reads as, "to carry out such investigations and provide such services as may be necessary to exercise and perform the powers and functions of the Commission*".

169 'Committee-Stage Amendments to Sri Lanka's "Online Safety Bill": CPA Concerned' (*EconomyNext*, 2 November 2023) <https://economynext.com/committee-stage-amendments-to-sri-lankas-online-safety-bill-cpa-concerned-138692>.

With regard to freedom of expression, the determination states, "... the Bill does not prohibit the freedom of speech and expression, including publication, but only regulate matters such as protecting persons against harm caused by communication of prohibited statements, protection from communication of statements in contempt of court or prejudicial to maintaining the authority and impartiality, of the judiciary. Further, it introduces measures to detect, prevent and safeguard against the misuse of online accounts and bots to commit offences specified in the Bill, and to prevent financing, promotion and other support of online locations, which communicate prohibited statements in Sri Lanka." (Page 38).

2.6.2 New Law(s) on Cybersecurity

In 2019, Sri Lanka released a Cybersecurity Bill. An analysis of this draft legislation did not reveal anything related to social media or social media regulation. The bill outlines cybersecurity and cybercrime provisions to strengthen the Sri Lankan digital economy. However, the bill has been criticised for being vague as it does not disclose what constitutes as minimum baseline for a cybersecurity offence or cybercrime.[170] Additionally, the bill allows for the designation of infrastructure as Critical Information Infrastructure (CII) but does not specify the sectors which the CII covers. It also gives the government bodies the powers to designate new CIIs. As such it is unclear if any part of the social media platforms would be included in the definition.

In August 2023, an amended version of the Cyber Security Bill was issued, and comments on the Bill were invited by the Ministry of Technology.[171]

There were some significant differences between the 2019 and 2023 versions of the Bill. The 2019 Bill referred to three separate institutions: the Cyber Security Agency of Sri Lanka (CSASL), the National Cyber Security Operations Center (NCSOC), and the existing Sri Lanka Computer Emergency Readiness Team (SLCERT).

In the Bill issued in 2023, the institutional arrangements have been simplified to avoid confusion; the Bill provides for the establishment of one authority - the Cyber Security Regulatory Authority of Sri Lanka (the 'Authority'), which will be the apex executive

170 LGC Vithakshana, 'A qualitative analysis on strengths and weaknesses of Cyber Security Bill 2019 in Sri Lanka' (2020) International Conference on Applied and Pure Sciences <http://repository.kln.ac.lk/handle/123456789/21868>.

171 https://cert.gov.lk/wp-content/uploads/2023/08/Cyber-Security-Bill-13-07-2023.pdf

body for the implementation of all matters relating to civilian aspects of cyber security (Section 3). Once the Bill becomes an Act, the SLCERT will be wound up and the powers and functions exercised by the SLCERT will be exercised by the Authority. (Section 18)

As in the previous version, the Bill provides for the identification of a computer, computer program, computer system or related device as a "Critical National Information Infrastructure" (CNNI). The definition of CNII given in Section 38 (interpretation) reads as follows:

> "the computer, computer program, computer system, or related device identified by the Authority as a Critical National Information Infrastructure under this Act, which is located wholly or partly in Sri Lanka, and its disruption or destruction would create a serious impact on the national security, public safety, public health and economic wellbeing of citizens, delivery of essential services or effective functioning of the government or the economy of Sri Lanka."

There are still no clear and transparent criteria given on how CNNIs will be identified. However the Authority must inform the owner regarding the classification. Furthermore, Section 20 (3) specifies that the Authority may "... if it considers appropriate, obtain the views of the owner of such Critical National Information Infrastructure relating to such a Critical National Information Infrastructure and publish such Critical National Information Infrastructure in the Gazette."

At the time of writing, there has still been no information on whether a further revised version of the Bill would be released, or when it would be presented to Parliament.

2.6.3 Revised Anti-Terrorism Bill (ATA) September 2023

The revised 'Anti-Terrorism Bill' (ATA) was published in the Gazette of 15th September 2023.[172] This Bill seeks to replace the widely criticised Prevention of Terrorism Act (PTA). The publication of the present version of ATA follows a former version of the ATA, which was published on the 22nd of March 2023. A similar Bill, referred to as the Counter Terrorism Bill, was also put forward in 2018.[173]

172 Anti Terrorism Bill 2023<http://documents.gov.lk/files/bill/2023/9/383-2023_E.pdf>.

173 Commentary comparing the proposed Anti Terrorism Bill to the Prevention of Terrorism Act (CPA, October 2023) https://www.cpalanka.org/wp-content/uploads/2023/10/ATA-Table-Complete-v1.2.pdf

This chapter will discuss only the section of the September 2023 ATA Bill which is relevant for social media regulation. Sections 10 (Encouragement of Terrorism) and Section 11 (Dissemination of terrorist publications) could have implications for the regulation of online social media content.

Section 10 states that an offence is committed by any person who:

> "publishes or causes to be published a statement, or speaks any word or words, or makes signs or visible representations which is likely to be understood by some or all of the members of the public as a direct or indirect encouragement or inducement for them to commit, prepare or instigate the offence of terrorism and such person – (i) intends directly or indirectly to encourage or induce the public to commit, prepare or instigate the offence of terrorism; or (ii) is reckless as to whether the public is directly or indirectly encouraged or induced by such statement to commit, prepare or instigate the offence of terrorism, commits an offence under this Act".

Further, as per section 10(3), a "statement" includes every statement –

> "(a) which glorifies the commission of the offence of terrorism or preparation for the offence of terrorism; and
>
> (b) from which the public may reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances, but does not include an opinion, legitimate criticism, satire, parody, caution or imputation made in good faith."

The provision applies to publishing a statement using print media, the internet or electronic media and could, therefore, potentially be used against social media content. The explanation of what amounts to publications that "directly or indirectly encourage members of the public to acts of terrorism" is vague. Commentators argue that this provision poses a serious threat to freedom of expression and the work of media organisations and human rights activists.[174]

Section 11 stipulates a similar offence for disseminating terrorist publications through print media, electronic media and the Internet.

174 Ibid.

The offence of terrorism itself is very widely defined[175] under the ATA Bill, another reason for the Bill being criticised as this broad definition gives the executive wide leeway in deciding who can be accused of terrorism and does not meet internationally recommended standards in defining the term 'terrorism'.[176]

2.6.4 Calls for Regulating Social Media

There have been several calls to regulate social media in Sri Lanka over the past few years, often on the basis of regulating misinformation / "fake news" and hate speech. A "fake news" law was advocated for in the aftermath of the Easter Sunday attacks.[177] Prominent legal actions were taken against "fake news" in 2021. In June 2021, the then police spokesman, Deputy Inspector General (DIG) Ajith Rohana, announced that the CID was instructed to deploy teams to monitor cyberspace due to a rise in fake news.[178] In a media statement, the Police stated that those sharing fake news can be arrested without a warrant.[179]

There has also been advocacy of social media regulation by politicians in government in 2020-21. In late 2020, the then media minister Keheliya Rambukwella stated that the government was planning to register social media users, but later claimed that the government intended to register only "foreign digital operators"[180] without addressing what a "foreign digital operator" precisely is. Thus far, there has been no move to officially register social media companies as businesses in Sri Lanka. However, this may change once the Online Safety Bill is passed into law.

175 Under Section 3, terrorism is defined in the following manner, "*Offence of terrorism (1) Any person, who commits any act or illegal omission specified in subsection (2), with the intention of– (a) Intimidating the public or a section of the public; (b) wrongfully or unlawfully compelling the Government of Sri Lanka, or any other Government, or an international organisation, to do or to abstain from doing any act; (c) Propagating war or, violating territorial integrity or infringement of sovereignty of Sri Lanka or any other sovereign country*".

176 UN experts say Sri Lanka's counter-terrorism bill fails to heed their recommendations, status quo fundamentally unchanged (18.10.2023) https://www.ohchr.org/en/press-releases/2023/10/un-experts-say-sri-lankas-counter-terrorism-bill-fails-heed-their; Anti-Terrorism Bill Version 2.0: Still Worse Than the PTA, *Groundviews* (23.09.2023) https://groundviews.org/2023/09/23/anti-terrorism-bill-version-2-0-still-worse-than-the-pta/

177 'Sri Lanka proposes new law on fake news after Easter attacks' *France24* (Colombo, 5 June 2019) <https://www.france24.com/en/20190605-sri-lanka-proposes-new-law-fake-news-after-easter-attacks>.

178 Aazam Ameen, 'CID teams to monitor fake news: DIG Ajith Rohana' (*The Morning*, 7 June 2021) <https://www.themorning.lk/cid-teams-to-monitor-fake-news-dig-ajith-rohana/>.

179 Pamodi Waravita, 'No warrant needed for 'fake news' arrests' (*The Morning* ,9 June 2021) <https://www.themorning.lk/no-warrant-needed-for-fake-news-arrests/>.

180 Hassaan Shazuli, 'Rambukwella does a U-turn on registering social media users' (*News 1st*, 21 December 2020) <https://www.newsfirst.lk/2020/12/21/rambukwella-does-a-u-turn-on-registering-social-media-users/>.

Since mid-2019, the government has intended to criminalise 'fake news'. In April 2021, the Cabinet Office stated that the Cabinet had approved a proposal to draft legislation that would deal with false and misleading online statements. Singapore's POFMA was reported to serve as a model for the new laws.[181] Subsequently, the Bill on Online Safety was released. While the Bill shared certain similarities with the POFMA, in certain aspects, it even went beyond it.[182]

In August 2021, Labour Minister Nimal Sirispala de Silva stated that social media should be banned or regulated, blaming social media for child abuse.[183] In October 2021, Sagara Kariyawasam, an MP and the general secretary of the Sri Lanka Podujana Peramuna (SLPP), the ruling party in Sri Lanka, expressed the need for the regulation of content on social media. He emphasised the spread of "wrong and hateful views" on these platforms and highlighted the absence of a legal framework to address such issues. Kariyawasam also suggested that individuals posing a threat to the country and contributing to its destabilisation may be taking advantage of the current situation.[184]

An opposition MP, Thalatha Athukorala, also spoke in favour of regulation, saying, "We too would like if there were some laws and regulations, [turning to Justice Minister Ali Sabry] Hon Minister of Justice, that were robustly implemented. We would like that very much, because we all know how it was used for just one side before November 16, 2019 [the date of the 2019 presidential election in Sri Lanka], and how it is being used now."[185] However, none of these pronouncements have resulted in any concrete proposals to regulate social media under a separate law.

181 Shreetesh Angwalkar, 'Sri Lanka Implements Singapore Style Law to Control Fake News' (*Spherex*, 23 April 2021) <https://www.spherex.com/regulation/sri-lanka-implements-singapore-style-law-to-control-fake-news>.

182 Sri Lanka's new Bill on Online Safety:comparison with Singapore (LIRNEasia, 22nd September 2023) https://lirneasia.net/2023/09/sri-lanka-online-safety-bill

183 'Ban or regulate social media in Sri Lanka, top minister tells parliament' (*Economy Next*, 5 August 2021) <https://economynext.com/ban-or-regulate-social-media-in-sri-lanka-top-minister-tells-parliament-84604/>.

184 'Another Sri Lanka govt MP calls for social media regulation amid online backlash' (*Economy Next*, 21 October 2021) <https://economynext.com/another-sri-lanka-govt-mp-calls-for-social-media-regulation-amid-online-backlash-87218/>.

185 Ibid.

2.6.5 Self-Regulation by Platforms

Perhaps in response to the threat of regulation by the government, the platforms themselves appear to be keen to develop Codes of Practice regarding content. The most prominent such code is Aotearoa New Zealand Code of Practice for Online Safety and Harms,[186] that was championed by NetSafe (a not-for-profit online safety organisation in New Zealand) and NZtech (an industry association). It is seen as an attempt by the platforms to work towards reducing harms of online content. Meta (Facebook), Google (and Youtube), TikTok, Twitch and Twitter have already signed up to the code at the time of writing.[187]

The Code has come under criticism from InternetNZ (New Zealand's top-level domain name registry, which also helps inform and foster key internet policy conversations and decisions), among others.[188] One criticism is the lack of legitimacy due to limited community consultations that were done prior to the finalisation of the Code. Another is that this is an effort to prevent government regulation. A strong concern appears to be that the Administrator (who will monitor platform performance against the code and track violations) is funded by the platforms it monitors, creating a conflict of interest.

In Sri Lanka too, a similar initiative has been started by Factum, a think tank funded (at least in part) by the Asia Internet Coalition (a regional industry association of the global platforms and large technology companies).[189] While Factum has not published its draft code, it is likely that similar challenges and concerns could be expressed by critics.

186 'Aotearoa New Zealand Code of Practice for Online Safety and Harms' (*NZ Tech Alliance*) <https://netsafe.org.nz/aotearoa-new-zealand-code-of-practice-for-online-safety-and-harms-draft/>.

187 Curtis Barnes, Tom Barraclough and Allyn Robins, ,Platforms Are Testing Self-Regulation in New Zealand. It Needs a Lot of Work.' (Lawfare, September 2022) <https://www.lawfaremedia.org/article/platforms-are-testing-self-regulation-new-zealand-it-needs-lot-work>.

188 'Code of Practice for Online Safety and Harms' (*InternetNZ*) <https://internetnz.nz/assets/Archives/InternetNZ-submission-on-NetSafe-Code.pdf>.

189 'SafeWebLK: New Initiative with Global Tech Companies on a Code of Practice for Online Safety' *NewsWire* (15 March 2022) <https://www.newswire.lk/2022/03/15/eb-users-to-collaborate-with-global-tech-companies-on-a-code-of-practice-for-online-safety/>.

2.7 Process, Trends and Impacts of Security Concerns on Social Media in Sri Lanka

Social Media Governance as a Security Issue: In Sri Lanka, we see there are no laws that enable the government to directly regulate or control platform behaviour. However, the government does exercise control over its licensed ISPs, and it has used these powers to order ISPs to block access to social media for users, as seen in the multiple examples given. In addition, it also uses multiple laws and institutions to arrest, charge or detain users of social media. As such, there is "regulation" of social media.

Importantly, security exceptions like those under section 6 of the CCA, PTA, section 120 of the penal code, public security ordinance, section 69 of the SLTA are often used to govern the information ecosystem and content on social media as seen in the case studies. Clauses in existing laws that refer to national security are often used to arrest or charge people with various offences. This is also clear from the types of institutions that are involved in regulatory activity. The police, TID and CID have all played roles in carrying out arrests. The Ministry of Defense has been involved in the issuing of social media blocking orders.

Incidents that are threats to national security, such as the Easter Sunday Attacks, have provided an impetus for regulatory activities. Even other incidents have been dealt with in a securitized manner. Social media users were arrested for their posts during the COVID-19 pandemic. The Ministry of Defense requested the TRCSL to block social media during protests against the economic crisis.

The Online Safety Bill that is currently before Parliament also lays down offences relating to national security. For example, Section 12 specifies that anyone who '... poses a threat to national security, public health or public order or promotes feelings of ill-will and hostility between different classes of people, by communicating a false statement' commits an offence. Sections 21 makes it an offence for any person who '... communicates any false statement, with intent to cause any officer, sailor, soldier, or airman in the navy, army or air force of Sri Lanka to mutiny, or with intent to cause fear or alarm to the public, induces any other person to commit an offence against the State or against the public tranquillity ...'

Executive discretion and lack of independence of institutions: A significant amount of executive discretion in the system aids the actions of the government. This extends to control over institutions that are meant to operate independently.

As we point out above, the order to block access to social media has been issued by the TRCSL, the regulator of the telecom sector. While TRCSL was set up as an independent regulator, its lack of independence from the executive/President has been commented upon by several publications .[190] Often, the TRCSL has been gazetted under the President (instead of a separate subject Minister, such as that of Media, Science and Technology or Digital Infrastructure or Information Technology), and TRCSL's Chairman has been the President's own Secretary.

The Director General of the TRCSL has at times been a close ally of the President.[191] Civil society organisations accused the then President of using his powers over TRCSL to send messages that could unfairly advantage him in an upcoming election.[192] Others have pointed to the appointment of retired military officers (who served under another President) being appointed as the Chair of the TRCSL as a sign of lack of independence.[193] A former Chair and Director General of TRCSL were convicted of misappropriating TRCSL funds to fund an election campaign, but were later acquitted on appeal .[194] More recently, the TRCSL has been directly under the Ministry of Defense, which itself came under the President.[195]

190 Malathy Knight-John, Shantha Jayasinghe and Andrew Perumal, 'Regulatory Impact Assessment in Sri Lanka: The Bridges That Have To Be Crossed' (2004) *Institute of Policy Studies* <https://assets.publishing.service.gov.uk/media/57a08ccce5274a27b200142f/CRCwp74.pdf>;

'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*, 2021) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>.

191 'Sri Lanka: Freedom on the Net 2023 Country Report'(*Freedom House*, 2023)<https://freedomhouse.org/country/sri-lanka/freedom-net/2023>

192 Asanga Welikala, 'The Shocking Behaviour of the Telecommunications regulatory Commission of Sri Lanka' (*Groundviews*, 1 September 2010) <https://groundviews.org/2010/01/09/the-shocking-behaviour-of-the-telecommunications-regulatory-commission-of-sri-lanka/>.

193 Harindrini Corea, 'In Sri Lanka, state-sponsored disinformation and suppression of dissent taint COVID-19 response' (*Association for Progressive Communications*, 10 August 2022) <https://www.apc.org/en/news/sri-lanka-state-sponsored-disinformation-and-suppression-dissent-taint-covid-19-response>.

194 'Lalith Weeratunga and Anusha Palpita acquitted in Sil Coth case' (*NewsFirst*) <https://www.newsfirst.lk/2020/11/19/lalith-weeratunga-and-anusha-palpita-acquitted-in-sil-cloth-case/>.

195 Chandani Kirinde, 'Gotabaya to take over Defence, Tech Ministries' (DailyFT, 23 November 2020) <https://www.ft.lk/front-page/Gotabaya-to-take-over-Defence-Tech-Ministries/44-709277>.

In short, TRCSL, Ministry of Defense, and other ministries that have exerted varying levels of control over social media accessibility or social media users have been under the control of the President for significant amounts of time, thus enabling a significant amount of discretion in the actions that can be taken by the executive.

TRCSL's actions around content blocking have been criticised by various parties. For instance, "Freedom on the Net (2021)- Sri Lanka" Report noted:

> "There is a lack of transparency around restrictions of online content, but a 2017 right to information (RTI) request revealed some of the government's blocking procedures. The government's response revealed that blocking orders can originate from the Mass Media Ministry and the Presidential Secretariat for a number of reasons, including "publishing false information" and "damaging the president's reputation." Orders are then sent to the TRCSL, which instructs ISPs to block the content. The TRCSL denied part of the RTI request on national security grounds, and an appeal of the case was heard before the RTI Commission in the spring of 2018."[196] (Please note that, subsequently, information in this regard was released by the RTI Commission on appeal, and the said order has been discussed below.)

Furthermore:

> "There is no independent body regulating content, which leaves limited avenues for appeal. Content providers have filed fundamental rights applications with the Supreme Court to challenge blocking orders...."[197]

Case study 3 in section 2.3 also noted that the social media blocking request in April 2022 came to TRCSL from the Ministry of Defence, although the validity of this request has been questioned, as noted previously.

Institutional Capacity: Lack of independence is not the only challenge faced in Sri Lanka. We observe that the regulatory capacity too appears to be low.

The SLCERT is mandated with the task of protecting Sri Lanka's cyberspace both by reacting to [cyber] attacks and by proactively strengthening defences against potential attacks. On its website, SLCERT provides information on cyber issues. One category it

196 'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*, 2021) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>.

197 Ibid.

tracks and reports is the number of "social media incidents" annually. However, there are no further details available on what this data means as noted previously.[198]

An RTI application was filed seeking information from SLCERT on names of individuals in charge of operating SLCERT's social media account, guidelines for posts made from that social media accounts, and a list of blocked accounts and reasons for blocking certain accounts (in this case, SL-CERT's Twitter account @SLCERT had blocked a few separate twitter accounts/users from accessing @SLCERT's page).

The Information Officer (IO) at SLCERT responded stating that the Twitter account @ SLCERT volunteers to offer free services on cybersecurity related matters, and that the Twitter account is governed by the US Law. It further stated that, therefore, any information requested in relation to this particular account should comply with the US Freedom of Information Act. The response by the IO (as indicated in the RTI Commission Order) leads to confusion, as it did not clearly spell out that the account @SLCERT was not the official handle and was in fact run by an impersonator. It gives the impression that the account was in fact run by SLCERT, but they are unaware of Twitter's workings.

On appeal to the Designated Officer, it was stated that the SLCERT account was a private account and hence such information was not in possession, custody, or control of the public authority under Section 3(1) of the RTI Act and that there were no guidelines for social media accounts, as such. Subsequently, an appeal was made to the RTI Commission. At the appeal hearing (*Amalini De Sayrah v. Sri Lanka Computer Emergency Readiness Team*[199]), SLCERT's submission stated that the alleged @SLCERT Twitter account was administered by an impersonator and that SLCERT has taken all necessary measures to close down the account. It can be observed that there is lack of capacity at SLCERT and there is room for strengthening the mechanisms/processes adopted, including in the managing of social media incidents.

198 'Regulating Social Media in Sri Lanka: An Analysis of the Legal and Non-Legal Regulatory Frameworks in the Context of Hate Speech and Disinformation' (*Democracy Reporting International*, 2021) <https://democracyreporting.s3.eu-central-1.amazonaws.com/images/3635DRI_Regulating%20Social%20Media%20in%20Sri%20Lanka_Report_Revised%20March%202021.pdf>.

199 RTIC Appeal (In-Person)/981/19.

Desire to control social media: The government not only uses the grounds of national security as a justification to selectively target content and users on social media, but has expressed its desire to monitor social media more closely. In the past, this quest has been supported by China. For instance, several years ago the then President requested social media surveillance technology from China citing "ideologically based terrorism" as a reason for the need to track fake profiles and encrypted content.[200] Other reports indicate that China granted this request and that the Chinese firm ZTE deployed censorship and safe site technology to Sri Lanka.[201]

As we will see, there have been various attempts to craft regulation to enable governance of social media and we see the government continues to work towards this objective. However, various such attempts and policies have been deemed too restrictive. For instance, the government issued a circular regulating "Expression of opinion on social media by public officials".[202] This circular imposes a comprehensive set of restrictions on the statements public officials make on social media. The restrictions outlined in section 6 highlight this issue, explicitly stating that public officials are prohibited from providing information, even factual statements, if their publication may potentially embarrass the Government, any Government Institution, or officer.[203]

The introduction of the aforementioned Online Safety Bill and the Anti Terrorism Bill can also be seen as attempts to control the flow of information on social media. As discussed in Section 2.6.4 terrorism is defined very broadly in the Anti Terrorism Bill, and gives the executive wide leeway in deciding who can be accused of terrorism.

200 'China to share social media surveillance technology with Sri Lanka' (*Sunday Observer*, 29 October 2023) <https://www.sundayobserver.lk/2019/05/26/news-features/china-share-social-media-surveillance-technology-sri-lanka>.

201 Valentin Weber, 'The Worldwide Web of Chinese and Russian Information Controls' (2019) Centre for Technology and Global Affairs <https://www.ctga.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf>.

202 'Expresison of opinions on Social Media by public officials' (*News.lk*, 27 September 2022) <https://www.news.lk/news/political-current-affairs/item/34489-expression-of-opinions-on-social-media-by-public-officers>.

203 Ministry of Public Administration, Home Affairs, Provincial Councils and Local Government, 'Establishments Code' <https://www.pubad.gov.lk/web/index.php?option=com_content&view=article&id=45&Itemid=192&lang=en>.

2.8 Implications for the Rule of Law

In this section, we situate the above findings and dwell on the impact they have on the democratic rule of law within Sri Lanka's social media environment. There are several indicators to assess rule of law, some of those indicators have been analysed below.[204]

(a) Supremacy of Law

The Sri Lanka Constitution (1972) curtailed the powers of the judiciary, wherein judicial review of laws (post-enactment) was not permitted. Subsequently, the 1978 Constitution (the one currently in force) continued such a trend and established an exclusive system of presidential governance, placing the President as the Head of the State with wide powers and immunity.[205] The 20th Constitutional Amendment accorded more discretion, expansive powers and greater immunity to the President.[206] In light of these constitutional provisions it can be argued that the law provides for concentration of power in the hands of the President and undermines the principle of supremacy of law.

The Public Security Ordinance provides wide law-making powers to the President, wherein laws already enacted by the Parliament, regulations, by-laws, and provincial regulations can be overridden. Section 2 (1) of the Public Security Ordinance outlines the circumstances under which the emergency regulations need to be in place in the country. The President may issue a Proclamation of a State of Emergency where, "the President is of the opinion that it is expedient to do so, in the interests of public security and the preservation of public order or for the maintenance of supplies and services essential to the life of the community."

204 United Nations, *Rule of Law Indicators: Implementation Guide and Project Tools* (1st edn, United Nations, 2011) <https://peacekeeping.un.org/sites/default/files/un_rule_of_law_indicators.pdf>.

205 'The rule of law' (DailyFT, 3 September 2021) <https://www.ft.lk/columns/The-rule-of-law/4-722553>.

206 Meera Srinivasan, 'Sri Lanka: Controversial 20th Amendment passed' (*The Hindu*, 22 October 2022) <https://www.thehindu.com/news/international/sri-lanka-controversial-20th-amendment-passed/article32921800.ece>.

The Public Security Ordinance enumerates various purposes for which Emergency Regulations may be made. These include provision for the detention of persons, commandeering and acquisition of private property, entry and search, and hearings, appeals and compensation for those affected by the regulations.[207] Other than the power to make Emergency Regulations, the PSO also sets down the special powers of the President during a state of emergency, including calling out the armed forces in aid of the civil power, the procedure for arrest, detention and executive review of detention, and the suspension of certain safeguards for the liberty of the individual in the Code of Criminal Procedure. However, the fundamental and due process rights of citizens must only be restricted in compliance with established rule of law principles like proportionality and necessity.

In the case of *Sunila Abeysekera v. Ariya Rubasinghe Competent Authority and Others*,[208] emergency regulations were challenged on grounds of it being violative of Articles 10, 12, and 14(1)(a) of the Constitution. The petitioner alleged that the impugned regulation was to prohibit the publication of information that was embarrassing to the Government, rather than to protect national security. While the court held that the regulation did not infringe the Petitioner's fundamental right, it was reasoned that impugned regulations were framed in reasonably precise terms and confined in their application to defined circumstances. This illustrates that emergency regulations can not only be challenged in Court but that such regulations must be framed within reasonably precise terms and applied within defined circumstances.

The Public Security Ordinance provides wide and, to some extent, unfettered powers to the President to pass laws on several areas, including regulating social media. It has been observed time and again that "national security" / emergency imposition has preceded blocks on social media. The Emergency Regulations gazetted in July 2022 particularly provided for regulating content including on social media. Paragraph 15 states that no person must "communicate or spread any rumour or false statement or any information or image or message which is likely to cause *public alarm, public disorder or racial violence or which is likely to incite the committing of an offence*."

207 'Understanding a State of Emergency: March 2018' (*Centre for Policy Alternatives*, 16 March 2018) <https://www.cpalanka.org/understanding-a-state-of-emergency-march-2018/>.

208 *Sunila Abeysekera v. Ariya Rubasinghe Competent Authority and Others* [2000] SLR 1V3141.

The terms such as "public alarm" and "public disorder" are broad and cannot be precisely defined. At the time of writing, it is unclear as to how many complaints have been registered under the said Regulation. It is pertinent to note that the imposition of emergency provides sweeping powers to the Executive / President to pass laws on any subject matter. While they can be put to test under a fundamental rights petition and several such petitions have been filed,[209] the current Emergency Regulations remain valid.

It is also observed that in the blocking of social media platforms in April 2022, the TRCSL acted upon a request from the Ministry of Defence, which the HRCSL noted it could not do.[210] The relevant provision i.e. Section 69 of the Sri Lanka Telecommunications Act (detailed in Section 2.2) does not provide for the TRCSL to act under the direction of the Defence Ministry.

Further, an RTI request also revealed the process for blocking websites, where the TRCSL acted on the order from the Ministry of Mass Media.[211] It should be highlighted that in case of some of the blocked websites, the Presidential Secretariat has sent a letter flagging the news articles to the Ministry of Mass Media, who in turn have ordered for the blocking of such sites by the TRCSL.

The Supreme Court of Sri Lanka observed in *Sunila Abeysekera v. Ariya Rubasinghe*, that the right to free speech includes the right to use "whatever medium is deemed appropriate to impart ideas and to have them reach as wide an audience as possible."[212] The Constitution of Sri Lanka guarantees several fundamental rights including freedom of speech. However, in the recent past, several persons have been prosecuted (see section 2.3) under the various provisions of the existing laws, including the Penal Code and ICCPR Act, without following the necessary legal processes/transparency and in violation of their rights to free speech. Therefore, the implementation of rights restrictive provisions must be carefully situated in the legal basis provided under the law and adhere to existing jurisprudence on proportionality and necessity.

209 'SC permits examination of FRs against Emergency, Curfew, & SM Ban' *NewsFirst* (Colombo) <https://www.newsfirst.lk/2022/04/07/sc-permits-examination-of-frs-against-emergency-curfew-sm-ban/>.

210 Shamindra Ferdinando, 'State of Emergency: HRCSL criticises govt. decision' (*The Island*, 4 April 2022) <https://island.lk/state-of-emergency-hrcsl-criticises-govt-decision/>.

211 Raisa Wikremetunge, 'Blocked: RTI requests reveal process behind blocking of websites in Sri Lanka' (*Groundviews*, 12 August 2017) <https://groundviews.org/2017/12/08/blocked-rti-requests-reveal-process-behind-blocking-of-websites-in-sri-lanka/>.

212 S.C. Application No. 994/99 (Supreme Court of Sri Lanka 1999).

The definitions of many of the offences are very vague and can be broadly interpreted. This creates more scope for abuse, and citizens run the risk of dilution of their digital rights and protection against arbitrariness.[213] Therefore, arbitrary enforcement infringes on the freedom of expression, assembly, privacy, and procedural rights.

Importantly, Articles 15(2) and 15(7) of the Constitution outline a more extensive list of restrictions on freedom of expression. Articles 15(2) and 15(7) establish that freedom of expression shall be subject to such restrictions as may be prescribed by law in the interests of "racial and religious harmony or in relation to parliamentary privilege, contempt of court, defamation or incitement to an offence", and "national security, public order and the protection of public health or morality, or for the purpose of securing due recognition and respect for the rights and freedoms of others, or of meeting the just requirements of the general welfare of a democratic society", respectively.[214]

While Article 19 (3) of the ICCPR requires the restrictions placed on freedom of expression to be "by law" and "necessary", the only procedural safeguard provided for by the Sri Lankan Constitution in Article 15 for the imposition of restrictions on fundamental rights is that they are required to be "prescribed by law".[215] As the Constitution does not include a requirement that the restrictions need to be reasonable or necessary, the government has considerable leeway in the imposition of restrictions on rights.[216]

The right to privacy, though not guaranteed as a fundamental right, is said to be protected in other statutes. In 2008, the Sri Lankan Supreme Court, in *Advisory Opinion, SC Reference No. 1 of 2008*, recognised that the right to privacy was protected under various provisions of common and statutory law, though not under the Constitution, and contended that Sri Lanka's legal framework adequately protects the right to privacy established under Article 17 of the ICCPR.[217]

213 Gehan Gunatilleke, 'Covid-19 in Sri Lanka: Is Free Speech the Next Victim?' (*Oxford Human Rights Hub*, 16 April 2020) <https://ohrh.law.ox.ac.uk/covid-19-in-sri-lanka-is-free-speech-the-next-victim/>.

214 Constitution of Sri Lanka, art 15.

215 *Confronting Accountability for Hate Speech in Sri Lanka* (*Centre for Policy Alternatives* 2018) <https://www.cpalanka.org/wp-content/uploads/2018/09/Confronting-Accountability-for-Hate-Speech-in-Sri-Lanka-2018.pdf>.

216 Rohan Edrisinha and Asanga Welikala, 'GSP Plus and the ICCPR: A Critical Appraisal of the Official Position of Sri Lanka in respect of Compliance Requirements' in 'GSP+ and Sri Lanka: Economic, Labour and Human Rights Issues' CPA and Friedrich Ebert Stiftung, October 2008, pp 93-140.

217 Supreme Court Advisory Opinion, SC Reference No 1 of 2008; The Supreme Court relied on Post Office Ordinance, No 11 of 1908: Sections 71, 75; Computer Crimes Act, No 24 of 2007: Sections 3, 8, 10 and the Common law delictual right to sue for damages loss of reputation.

However, in the aforementioned case, it was pointed out that piecemeal protection in various statues was insufficient to guarantee the right to privacy.[218] Though the PDPA seeks to fill this void and protect citizen's data and elaborate on the right to privacy. Although, it remains to be seen whether the broad exemptions and grounds of national security will affect the protections.

It is also pointed out that public consultations are not uniformly held during the drafting of all laws in Sri Lanka.[219] Participative decision-making, including consultative processes for law-making, are essential prongs of the rule of law. While several recent legislations such as the RTI Act, PDPA, and the proposed Cybersecurity Bill included public/stakeholder consultations, there have also been several important legislative changes passed without necessary consultative steps.

(b) Procedural and Legal Transparency

The SLTA, as mentioned above, provides for the Minister to issue a gazette notification to restrict or prohibit transmission of telecommunication on grounds of public emergency or in the interest of public safety and tranquillity (Section 69). The telecommunication licence conditions, that are publicly available also reveal that the telecommunication operators are required to block access or comply with Directions of the TRCSL.

It is clear that the TRCSL is the institution that orders ISPs to block social media websites. However, who can give orders to the TRCSL is much less clear due to lack of transparency of the process. As observed previously, in practice, blocking orders have originated in the Mass Media Ministry and the Presidential Secretariat, as well as the Defence Ministry.

In 2011, the Supreme Court dismissed a petition filed by four websites that had been blocked on grounds of failing to register.[220] The argument that no specific provision under law/ regulation required such registration was dismissed by the Apex Court. The Court

218 R Edrisinha and A Welikala, 'Civil and Political Rights in the Sri Lankan Constitution and Law: Making the New Constitution in compliance with the ICCPR' (2016), *Centre for Policy Alternatives* <http://constitutionalreforms.org/wp-content/uploads/2016/06/Working-Paper-8.pdf>.

219 'Global Indicators of Regulatory Governance' (*World Bank*) <https://rulemaking.worldbank.org/en/data/comparedata/consultation>.

220 Bob Dietz, 'Sri Lanka Supreme Court slams door on websites' (*Committee to Protect Journalists*, 17 May 2012) <https://cpj.org/2012/05/sri-lanka-supreme-court-slams-door-on-websites/>.

favourably considered the submissions of the State that freedom of expression was not an absolute right and could be restricted on grounds specified in the Constitution of Sri Lanka. The State further pointed out that none of the websites that had complied with the registration rule had suffered any form of restraint or impediment.[221]

From the situation in 2011, it has to be conceded that there has been much improvement by the constitutional amendment, where the right of access to information was guaranteed as a fundamental right under Article 14A of the Constitution of Sri Lanka. The RTI Act lays down the statutory procedure in exercising the Fundamental Right of "Access to Information".

An RTI request in 2017 to the TRCSL relating to the blocking of a particular news site and requesting to know the authority who ordered the blocking of the site, etc., was rejected by the public authority ("PA") on grounds of national security. On appeal to the RTI Commission, this information was ordered to be released (*Raisa Wickrematunga v. TRCSL*[222]), wherein it was revealed that a written complaint was sent by the Office of the President.

Although the RTI Act has resulted in fostering a culture of transparency and increased focus on accountability, the relevant PA (s) continue to reject information requests, in relation to social media blocks, on grounds of "national security" under Section 5(1)(b)(i) of the RTI Act. The denial of RTI requests in relation to the social media blocking of April 2022, on the grounds of national security by the Pas[223] shows that the processes are still opaque. The RTI requests show that while some information on the orders for blocking of social media are available, which Ministries can direct TRCSL to block social media is not clear.

Thus, the lack of transparency in the procedure behind social media blocks and the ambiguity surrounding the authorities that may issue blocking orders undermines accountability to citizens. Although the RTI Act has instituted a mechanism enabling

221 'IFJ Disappointed by Sri Lanka's Supreme Court Decision on Internet Restrictions' (*International Federation of Journalists*) <https://www.ifj.org/media-centre/news/detail/category/africa/article/ifj-disappointed-by-sri-lankas-supreme-court-decision-on-internet-restrictions>.

222 RTIC Appeal (In person)/106/2018.

223 Yudhanjaya Wijeratne (*Twitter*, 27 April 2022) <https://twitter.com/yudhanjaya/status/1519288044490211328?s=21&t=fs06t7SkF0hlclxqhQgZgg>.

citizens to request information held by public authorities, the "national security" exceptions are often used by the government to deny such requests and maintain a cloak of secrecy on how social media applications are blocked in Sri Lanka.

(c) Equality before law

Equality before law is the foundational principle of legal frameworks that safeguards against the arbitrary and discriminatory application of law. In Sri Lanka, the criminalisation of online speech under the PTA and the ICCPR Act has raised concerns of equality before law.

The PTA has been used extensively in Sri Lanka, and the arbitrary use of this law has been criticised by many, both nationally and internationally.[224] Recently, the US Ambassador to Sri Lanka, Julie Chung, questioned the use of the PTA as it is not compliant with international human rights standards.[225]

As noted earlier, the PTA can be used against those spreading false/fake information via social media. Criticism arose on the issue of how one would judge the 'fakeness' of the social media content and that the CID's intervention would cause more harm than good.[226]

The PTA has also been used to target political dissidents and ethnic minorities.[227] It has been observed that the PTA is used mainly against those belonging to Tamils and Muslims ethnic and religious backgrounds.[228] Several people had been arrested under the PTA for social media posts. Some of these posts were commemorating the Tamils who lost their lives during the war, while other arrests were for posts sending birthday wishes to the late

224 'In a Legal Black Hole' (*Human Rights Watch*, 7 February 2022) <https://www.hrw.org/report/2022/02/07/legal-black-hole/sri-lankas-failure-reform-prevention-terrorism-act>;

'Sri Lanka: UN experts call for swift suspension of Prevention of Terrorism Act and reform of counter-terrorism law' (*OHCHR*, 2 March 2022) <https://www.ohchr.org/en/press-releases/2022/03/sri-lanka-un-experts-call-swift-suspension-prevention-terrorism-act-and>.

225 'US ambassador says using laws like PTA erodes democracy in Sri Lanka' (*Adaderana*, 22 August 2022) <http://www.adaderana.lk/news/84464/us-ambassador-says-using-laws-like-pta-erodes-democracy-in-sri-lanka>.

226 'Sri Lankans posting information deemed 'fake' on social media face arrest without warrant' (*EconomyNext*, 8 June 2021) <https://economynext.com/sri-lankans-posting-information-deemed-false-on-social-media-face-arrest-without-warrant-82783/>.

227 'Sri Lanka: UN experts call for swift suspension of Prevention of Terrorism Act and reform of counter-terrorism law' *Relief Web* (Geneva, 2 March 2022) <https://reliefweb.int/report/sri-lanka/sri-lanka-un-experts-call-swift-suspension-prevention-terrorism-act-and-reform#:~:text=The%20PTA%20has%20been%20used,the%20commission%20of%20enforced%20disappearances>.

228 '"In a Legal Black Hole" : Sri Lanka's Failure to Reform the Prevention of Terrorism Act' (*Human Rights Watch* 2022) <https://www.hrw.org/report/2022/02/07/legal-black-hole/sri-lankas-failure-reform-prevention-terrorism-act>.

LTTE leader Velupillai Prabhakaran, who was killed back in 2009.[229] Human rights activists claimed, "They are using PTA to create fear among activists. When we talk to the families of the disappeared, they say they can be arrested at any time. Police are arresting people for posting pictures on Facebook. They can arrest you for anything."[230]

The Tissainayagam Case[231] has been quoted as a focal point in highlighting the PTA's arbitrary and repressive nature and its ready availability for abuse by the State.[232] The judgement in the said case does not go into detailed discussion or definition on numerous key aspects of the relied-on PTA provisions. It has been criticised as being "riddled with baseless inferences".[233] The lack of jurisprudential discussion of phrases "intention to cause 'ill will' or 'communal disharmony' or 'hostility' amongst 'different communities'" by the High Court leaves their interpretation entirely open-ended.[234]

In February 2022, the HRCSL took a stance in support of the view that the PTA should be abolished in Sri Lanka. The Commission is working towards taking action which prevents the suspects arrested under the PTA from being abused.[235]

Following demands,[236] in 2022, there were amendments made to the PTA. Most minority parties in the Parliament have argued that the recent amendments do not address the fundamental issues with the PTA, such as accepting evidence given during detention. Human Rights Watch has pointed out that these changes still leave room for the PTA to be exploited and would not entirely follow Sri Lanka's international human rights

229 'In a Legal Black Hole' (*Human Rights Watch*, 7 February 2022) <https://www.hrw.org/report/2022/02/07/legal-black-hole/sri-lankas-failure-reform-prevention-terrorism-act>.

230 Ibid.

231 *J S Tissainyagam* High Court case No 4425/2008.

232 *Confronting Accountability for Hate Speech in Sri Lanka* (*Centre for Policy Alternatives* 2018) <https://www.cpalanka.org/wp-content/uploads/2018/09/Confronting-Accountability-for-Hate-Speech-in-Sri-Lanka-2018.pdf>.

233 Ibid.

234 Ibid.

235 'Sri Lanka's Human Rights Commission supports PTA abolishment' (*NewsFirst*, 16 February 2022) <https://www.newsfirst.lk/2022/02/16/sri-lankas-human-rights-commission-supports-pta-abolishment/>.

236 'Sri Lanka. UN experts call for swift suspension of Prevention of Terrorism Act and reform counter-terrorism law' (*United Nations Human Rights Office of the Human Rights Commissioner*, 2 March 2022) <https://www.ohchr.org/en/press-releases/2022/03/sri-lanka-un-experts-call-swift-suspension-prevention-terrorism-act-and>.

obligations.[237, 238] Amendments to the PTA were one of the demands of the European Union in return for the trade concessions worth over USD 500 million.[239, 240]

Furthermore, it has also been argued that the ICCPR Act has been used against members of religious minorities, while in contrast Buddhist clergy have not been targeted by the law, despite speech by certain members of the clergy inciting violence against Muslims.[241] (Buddhism is the majority religion in Sri Lanka).

(d) Separation of Powers

The Sri Lankan Constitution provides for a theoretically clear separation of powers between the Executive, the Legislature, and the Judiciary. Executive power is vested in the President, and legislative power with the Parliament.[242] The Supreme Court is empowered to hear cases of violations of fundamental rights (which must be filed within one month of the violation).[243]

However, the powers of the President were considerably widened with the 20th Amendment to the Constitution.[244] The 20th Amendment sought to roll back several changes brought in by the 19th Amendment and also provide wide powers to the President. It is important to reproduce the criticism of the International Commission of Jurists when the amendment was proposed: "*The proposed 20th Amendment, which bestows an already powerful executive president with additional powers with no effective checks on him, essentially placing him above the law.*"[245]

237 'In a Legal Black Hole' (*Human Rights Watch*) <https://www.hrw.org/report/2022/02/07/legal-black-hole/sri-lankas-failure-reform-prevention-terrorism-act>.

238 'A commentary: Prevention of Terrorism (Amendment) Bill 2022' (*Center for Policy Alternatives*, 2022) <https://www.cpalanka.org/wp-content/uploads/2022/01/Final-PTA-Amendment-2022.docx-1-1.pdf>.

239 Shihar Aneez, 'Sri Lanka agrees to further changes to terror law to save GSP plus ahead of UNHRC' (*EconomyNext*, 12 February 2022) <https://economynext.com/sri-lanka-agrees-to-further-changes-to-terror-law-to-save-gsp-plus-ahead-of-unhrc-90448/>.

240 'Sri Lanka agrees to reform terror law to keep EU trade deal' *France24* (Colombo, 5 October 2021) <https://www.france24.com/en/live-news/20211005-sri-lanka-agrees-to-reform-terror-law-to-keep-eu-trade-deal>.

241 Rehab Mahamoor, 'The Problem With Sri Lanka's New 'False News' Law' (*The Diplomat*, 7 August 2019) <https://thediplomat.com/2019/08/the-problem-with-sri-lankas-new-false-news-law/>.

242 Kishali Pinto- Jayawardana, *Rule of law in Decline: Study on Prevalence, Determinants and Causes of Torture and Other Forms of Cruel, Inhuman or Degrading Treatment or Punishment in Sri Lanka* (Rehabilitation Center 2009) <http://www.humanrights.asia/wp-content/uploads/2018/07/THE-RULE-OF-LAW-OF-DECLINE.pdf>.

243 Ibid.

244 'A brief guide to the 20th Amendment to the Constitution' (*Centre for Policy Alternatives*, 19 July 2021) <https://www.cpalanka.org/a-brief-guide-to-the-20th-amendment-to-the-constitution/>.

245 Statement of the International Commission of Jurists on the proposed 20th Amendment.

The Supreme Court in its special determination on the 20th Amendment ruled that Bill could be enacted with a mere two-thirds majority (special majority).[246] Although some clauses were found to be inconsistent with the provisions of the Constitution, it was agreed that they could be remedied with amendments in the Committee stage.[247]

The key changes brought in by the 20th Amendment include:

- Changes to the Executive Presidency (repeal of duties such as "ensure Constitution is respected and upheld"; bolstered immunity, etc.);
- Abolishing the Constitutional Council (The Constitutional Council overseeing appointments to key public service institutions, both at individual and institutional levels, was replaced by the Parliamentary Council, which comprised only of Members of Parliament. The Parliamentary Council was also limited in its influence in that it could only make observations to the President, who is not bound by them);
- Changes to the legislature and law-making process (imposing additional conditions on the dissolution of the Parliament power to pass urgent bills); and
- Changes to the judiciary and judicial services commission (The President could appoint the Chief Justice, the other judges of the Supreme Court, the President of the Court of Appeal and the other judges of the Court of Appeal at his/her discretion).[248]

These amendments have certainly obliterated the existence of Separation of Powers. It is pertinent to note that eliminating the Executive Presidency was one of the major demands of the people who were protesting the Economic Crisis we have cited in Case Study 3. Various proposals were put forth by candidates who were vying for the position left vacant when the then-President resigned. However, no formal proposals that would lessen the powers of the President have been made as of yet.[249]

246 C. SD No. 01/2020 - 39/2020, <https://supremecourt.lk/images/documents/sc_sd_01_39_2020.pdf>.

247 'SC Gives Green Light To Passage Of 20A: Clauses 3, 5 & 14 Can Be Passed Without Referendum But Subject To Amendment – Determination' (*Colombo Telegraph*, 10 October 2020) <https://www.colombotelegraph.com/index.php/sc-gives-green-light-to-passage-of-20a-clauses-3-5-14-can-be-passed-without-referendum-but-subject-to-amendment-determination/>.

248 'A brief guide to the 20th Amendment to the Constitution' (*Centre for Policy Alternatives*, 19 July 2021) <https://www.cpalanka.org/a-brief-guide-to-the-20th-amendment-to-the-constitution/>.

249 Muqaddasa Wahid 'Questions Persist in Sri Lanka over abolition of Executive Presidency after election' (The Hindu *Frontline*, 24 July 2022) <https://frontline.thehindu.com/world-affairs/testing-times-questions-persist-in-sri-lanka-over-abolishing-executive-presidency-after-election-of-ranil-wickremesinghe-as-president/article65670514.ece>.

The powers of the President are thus wide-reaching in the country, and the constitutional safeguards for challenging laws passed are also limited in comparison with other jurisdictions where powers of judicial review are wider. It is thus relevant to mention the role of the judiciary in the review of legislative enactments.

Historically, the Soulbury Constitution[250] recognized judicial review, and there were many instances in which the people resorted to the judiciary when a conflict arose between various forms of legislation and their entrenched rights.[251] It was this position that was changed by the 1972 Constitution. It is to be noted that the reasoning provided was that judicial review would interfere with the law-making powers of the Parliament.[252] The 1978 Constitution relocated the power of the judiciary to look into the constitutionality of laws only at the Bill stage before the law was enacted.[253]

The principle of judicial review provides opportunity for any citizen to challenge a law at any stage, if it could be proved in court that the law as passed violates the principle of legality that is enshrined within a democratic constitution.[254] The availability of pre- and post-enactment judicial review enables the courts to exercise effective oversight, which would in turn, guarantee the existence of checks and balances.

Sri Lanka has no post-enactment review of legislation. In Sri Lanka, the Constitution by virtue of article 124, only allows the judiciary to review bills pre-enactment. It specifically states that the validity of bills and the legislation process shall not be questioned except in the manner provided for in the Constitution as under articles 120, 121 and 122, which limit judicial review of legislation to that of reviewing Bills. Article 80 (3) categorically prohibits post-enactment review.

250 Sri Lanka gained independence under the Soulbury Constitution in 1948. It was replaced by the Republican Constitution of 1972 when Sri Lanka gave up the British Dominion Status and became an independent republic. See KM de Silva, 'Sri Lanka's First Decade of Independence: Phase II in the Transfer of Power' (1975) 8 Verfassung und Recht in Übersee / Law and Politics in Africa, Asia and Latin America 331 <https://www.jstor.org/stable/43108473>.

251 Basil Fernando, ,The Need to Restore Judicial Review' (*Ground Views*, 5 May 2022) <https://groundviews.org/2022/05/05/the-need-to-restore-judicial-review/>.

252 Ibid.

253 Ibid.

254 Ibid.

Article 80 (3)[255] reads as follows:

> (3) Where a Bill becomes law upon the certificate of the President or the Speaker, as the case may be being endorsed thereon, no court or tribunal shall inquire into, pronounce upon or in any manner call in question, the validity of such Act on any ground whatsoever.

Furthermore, the ability of a party to challenge a Bill is restricted by the time duration within which a petition challenging the Bill has to be brought in front of the Supreme Court in order for it to be considered a valid challenge. These can be seen as some vital considerations jeopardising the independence of the judiciary and an affront to the rule of law, constitutionalism and democracy.

Queen v Liyanage and Others[256] also highlights the importance of judicial independence. In this case, it was pointed out that the appointments of judges which are made by executive officials, could amount to an encroachment on the judicial territory. It was further stated that 'the nomination of the judges by the Minister was a violation of the Constitution and ultra vires the Constitution. These considerations notwithstanding, it is incorrect to state that the judiciary has not passed judgements of far-reaching consequences.

A Presidential Order was passed in October 2018 to dissolve the Parliament. The Full Bench decision of the Supreme Court in *R. Sampanthan and Ors vs. AG and Ors*[257] where this order was challenged, is of great relevance. The Court categorically stated that the 19th Amendment was an initiative that clarified that the President was required to act within the powers and responsibilities given to him by the Constitution.[258]

The Court rejected the argument that there were some "residual plenary executive powers" rather like a "royal prerogative" not subject to restrictions. The Full Bench decision reiterates that the President cannot exercise plenary powers outside the specific provisions of the Constitution.[259] In a departure from this position, the Supreme Court, in a subsequent decision,[260] referred to the President as the "repository" of Executive Power.

255 Constitution of Sri Lanka.

256 *Queen v Liyanage and Others* (1962) 64 NLR 313.

257 *R Sampanthan and Ors v AG and Ors* [1965] 68 NLR 265.

258 Danushka Sewwandi Medawatte 'Separation of Powers: A Fairytale of Utopia' (2014) SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2519929>.

259 Rehab Mahamoor, 'The Problem With Sri Lanka's New 'False News' Law' (*The Diplomat*, 7 August 2019) <https://thediplomat.com/2019/08/the-problem-with-sri-lankas-new-false-news-law/>.

260 Gehan Gunatilleke, 'Covid-19 in Sri Lanka: Is Free Speech the Next Victim?' (*Oxford Human Rights Hub*, 16 April 2020) <https://ohrh.law.ox.ac.uk/covid-19-in-sri-lanka-is-free-speech-the-next-victim/>.

(e) Legal Certainty

The review of the laws and case studies point out that several legislation and provisions have been used in the regulation of social media.

The police have also stated that those who are arrested for sharing fake news can be charged under the following: Penal Code Sections 120, 286,[261] 286 A,[262] 291 A,[263] 291 B,[264] 345,[265] *365C ,[266] 402,[267] 403,[268] and 486,[269] ICCPR Act Section 3, CCA Section 6, PTA Sections 2[270] and 3,[271] and provisions under the Obscene Publications Ordinance.[272] [273] This had led to criticism, including from the main opposition party.[274] The Free Media Movement has also expressed concerns about what the term "fake news" constituted.[275]

The executive committee of the Bar Association of Sri Lanka (BASL) also observed in a statement that: "*Given that the very prospect of being arrested for expressing harsh criticism or dissent can itself have a chilling effect that would erode the citizens' freedom to openly share critical views or freely comment on important matters as members/stakeholders of society, utmost care and restraint should be exercised in causing the arrest of any person for an offence pertaining to alleged 'fake news' prior to a full investigation of any complaint.*"[276]

261 "Having in possession obscene books, &c., for sale or exhibition."

262 "Obscene publication, exhibition & c. relating to children."

263 "Uttering words &c., with deliberate intent to wound religious feelings."

264 "Deliberate and malicious acts intended to outrage religious feelings of any class, by insulting its religion or religious beliefs."

265 "Sexual harassment."

266 "Publication of matter relating to certain offences" (wrongly cited as 365D in the article).

267 "Punishment for cheating by personation."

268 "Cheating and dishonestly inducing a delivery of property."

269 "Punishment for criminal intimidation."

270 "Offences under this Act and penalties."

271 "Penalty for abetment conspiracy, or incitement to commit offence."

272 Obscene Publications Ordinance <https://www.lawnet.gov.lk/obscene-publications-4/>.

273 Pamodi Waravita, 'No warrant needed for 'fake news' arrests' (*The Morning*, 9 June 2021) <https://www.themorning.lk/no-warrant-needed-for-fake-news-arrests/>.

274 Ibid.

275 Ibid.

276 Executive Committee of the Bar Association of Sri Lanka, 'Statement By The Executive Committee Of The Bar Association Of Sri Lanka On The Police Media Release On Circulation Of Fake News, Photographs, Videos Causing Disunity, Hate And Obstructing The Covid-19 Programme' (BASL, 11 June 2021) <https://basl.lk/statement-by-the-executive-committee-of-the-bar-association-of-sri-lanka-on-the-police-media-release-on-circulation-of-fake-news-photographs-videos-causing-disunity-hate-and-obstructing-the-covid-1/>.

In May 2021, a government official (an Assistant Land Settlement Commissioner in Kotmale) was arrested for Facebook posts made about deforestation. The police alleged that the posts were fake news and an offence under Section 120 of the Penal Code. The Facebook posts were analysed by the CID's computer crimes unit.[277]

In June 2021, a man was arrested under the CCA for releasing a statement saying that several government websites had been hacked. According to the police, the claims were incorrect, which misled the public and stopped them from getting information from the sites, as well as leading the public to think that the websites contained false information.[278] Further controversy ensued when, despite a magistrate's order to release the man on bail, prison authorities refused to do so, saying that the man had to conduct a PCR test and the results needed to be received.

It was pointed out by the suspect's lawyers that the man could not be charged under the sections of the CCA even if the claims of hacking government websites were incorrect. The police reported that government information had not leaked despite the claims, but the CID did not know whether the man in question had aided or abetted the act. The CID had no basis for his arrest and requested that the man be held in remand until they could charge him under a different law. The request was denied, and the man was released under bail of Rs 100,000. The Chief Magistrate advised the accused "to exercise his right to expression responsibly, without causing social disruption".[279]

In January 2022, the man filed a Fundamental Rights petition in the Supreme Court of Sri Lanka against his arrest and detention, with respondents including the Inspector General of Police, the Director of the CID, the CID Digital and Forensic Unit Officer-in-Charge, the CID Social Media Unit Officer-in-Charge, the Director General of Health Services, the Pitakotte Medical Officer of Health, and the Attorney General. He stated that the CID officials who arrested him were dressed in civilian attire, did not inform him why he had been arrested, and failed to produce him before a magistrate without undue delay.[280]

277 'Sri Lanka police arrest govt official over alleged fake news on deforestation,' (*Economy Next*, 22 May 2021) <https://economynext.com/sri-lanka-police-arrest-govt-official-over-alleged-fake-news-on-deforestation-82285/>.

278 'Head of the ITSSL arrested over misleading news on cyber attack,' (*Colombo Gazette*, 8 June 2021) <https://colombogazette.com/2021/06/08/head-of-the-itssl-arrested-over-misleading-news-on-cyber-attack/>.

279 'Prisons Dept Defies Magistrate's Bail Order As Gota's Social Media Crackdown Intensifies' (*Colombo Telegraph*, 10 June 2021) <https://www.colombotelegraph.com/index.php/prisons-dept-defies-magistrates-bail-order-as-gotas-social-media-crackdown-intensifies/>.

280 'ITSSL Chairman files FR over detention' (*The Morning*, 12 January 2022) <https://www.themorning.lk/itssl-chairman-files-fr-over-detention/>.

These examples reflect that in terms of legal certainty for regulation of content on social media, the approach of the State/enforcement authorities has not been consistent. The existing laws (including the Penal Code) have been applied, but the provisions under which crimes have been prosecuted have not been uniform despite some similarity in facts and circumstances.

2.9 Conclusion

It can be seen that Sri Lanka does not have a specific law on regulating social media platforms at the time of writing (though this may change if the proposed/modified Online Safety Bill becomes law). But several existing laws have been used to perform actions that effectively regulate social media. One example is the CCA. The recently passed Emergency Regulations also provide for regulation of content on social media.

Furthermore, in practice, social media regulation often has a security component to it. This was especially visible in the actions taken to regulate social media in the aftermath of the Easter Sunday Attacks, and the use of laws such as the PTA and the Emergency Regulations. These point towards a lack of legal certainty as to the laws, wherein the application of laws for the regulation of social media remains wide-ranging from the penal code to the ICCPR Act.

It is also worth noting that the application of the laws discussed above has come in for criticism. For instance, critics argue that the ICCPR act has been applied selectively and arbitrarily,[281] while others have warned of the adverse effects that arrests could have on the freedom of speech.[282]

According to our desk research around three key national-level incidents in the country, arrests of social media users appeared to be more publicly reported than any other form of action by the government. Social media blocks have also taken place. However, this

281 Rehab Mahamoor, 'The Problem With Sri Lanka's New 'False News' Law' (*The Diplomat*, 7 August 2019) <https://thediplomat.com/2019/08/the-problem-with-sri-lankas-new-false-news-law/>.

282 Gehan Gunatilleke, 'Covid-19 in Sri Lanka: Is Free Speech the Next Victim?' (*Oxford Human Rights Hub*, 16 April 2020) <https://ohrh.law.ox.ac.uk/covid-19-in-sri-lanka-is-free-speech-the-next-victim/>.

could change with the new Online Safety Bill 2023 laid down before the Parliament, which provides the Online Safety Commission wide-ranging powers to issue notices to block content on social media platforms.

Thus, the position in Sri Lanka can be summarised as follows:

- Social media "regulation" is through policing of individuals/users and blocking access to social media platforms (until the time the proposed Online Safety Bill comes into law. If it does, there will be direct regulation of social media platforms in the form of content takedowns).
- Taking these "regulatory" actions on grounds of "national security" or larger public interest without justification or evidence is prevalent, even more so during times of unrest.
- At the time of writing, social media intermediary/platform liability (for social media) has not been defined or imposed by law. However, this will change once the Online Safety Bill 2023 is enacted.
- There is keen interest among politicians and the government to bring in a law to regulate content on social media *vis-à-vis* fake news. This is also demonstrated in the introduction of the Online Safety Bill 2023 in the Parliament.
- The self-regulation efforts are still at an early stage, and it is hard to judge the impact.
- The rule of law as examined through various indicators reflect that there can be more concerted efforts in bringing about greater supremacy, transparency and certainty in law.

3. INDIA'S LANDSCAPE ON SOCIAL MEDIA REGULATION AND IMPACT ON RULE OF LAW

3.1 Overview

Presently, the Information Technology Act, 2000 ("IT Act")[1] is the primary legislation governing Information Communication and Technology (ICT) in India. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Guidelines)[2] is the primary subordinate legislation governing intermediaries, including social media platforms.

In addition, the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("Blocking Rules")[3] governs blocking access to information. The Indian Penal Code 1860 (IPC)[4] and other laws like the Protection of Children from Sexual Offences Act, 2012 (POSCO)[5] and Disaster Management Act, 2005 (DMA)[6] have also been used to govern speech on social media platforms.

1 The Information Technology Act, 2000 <https://www.indiacode.nic.in/handle/123456789/1999>.

2 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code)Rules, 2021 <https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=information_technology_(intermediary_guidelines_and_digital_media_ethics_code)_rules,_2021_(updated_06.04.2023)-.pdf>.

3 The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 <https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=blocking_for_access_of_information_rule_2009.pdf>.

4 The Indian Penal Code, 1860 <https://www.indiacode.nic.in/handle/123456789/2263?sam_handle=123456789/1362>.

5 The Protection of Children from Sexual Offences Act, 2012 <https://www.indiacode.nic.in/handle/123456789/2079?sam_handle=123456789/1362>.

6 The Disaster Management Act, 2005 <https://www.indiacode.nic.in/bitstream/123456789/2045/1/AAA2005___53.pdf>.

The Indian Telegraph Act 1885,[7] the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 ("Telecom Rules")[8] and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("Interception Rules")[9] govern internet shutdowns and monitoring and interception by the State.

The National Cyber Security Policy (NCSP) 2013[10] is the overarching framework that governs the prevention of, response to and mitigation of cyber incidents. The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 ("CERT Rules")[11] constitute the cyber incident response framework and the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules 2013[12] demarcate the functions and responsibilities of the National Critical Information Infrastructure Protection Centre.

It is important to note that ICT regulation in India is undergoing a major overhaul. Since 2021, multiple delegated legislations under India's IT Act have been promulgated. These changes update the country's intermediary liability and digital media governance frameworks and, in effect, serve as a forerunner to the country's forthcoming technology law reform. They impose greater regulatory obligations on social media platforms — and they could help reasonably forecast the direction of Indian social media regulation moving forward.

7 The Indian Telegraph Act,1885 <https://www.indiacode.nic.in/bitstream/123456789/13115/1/indiantelegraphact_1885.pdf>.

8 The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 <https://dot.gov.in/sites/default/files/Suspension%20Rules.pdf>.

9 The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 <https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf>.

10 The National Cyber Security Policy, 2013 <https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf>.

11 The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 <https://www.meity.gov.in/writereaddata/files/G_S_R%2020%20(E)2_0.pdf>.

12 The Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 <https://www.meity.gov.in/writereaddata/files/GSR_19%28E%29_0.pdf>.

The next phase of India's technology law reform will include: (a) a legal framework for personal data protection, which has been ratified by the President in August 2023 and is likely to come into force soon,[13] (b) a newly drafted 'Digital India Act' which is expected to replace India's nodal IT Act,[14] (c) an updated cybersecurity policy,[15] and (d) potentially a new legal framework governing the country's telecommunication landscape.[16]

This chapter maps (a) cybersecurity and other ICT regulations which are relevant to social media; (b) the intermediary liability regime applicable to social media platforms; and (c) the relevant administrative institutions which oversee India's social media ecosystem.

In this way, it identifies the key mechanisms deployed by the state to regulate and impact the flow of online information. These include (a) criminalisation of online speech; (b) law enforcement access to citizen information; (c) internet suspension; (d) blocking public access to online content; and (e) informal channels of communication between state and social media platforms. Apart from these, a new mechanism to regulate the online information ecosystem through statutory fact-checking bodies is emerging.

It is important to note that the state wields significant influence on platforms and, hence the online information ecosystem through a broad range of due diligence obligations.

The chapter then examines recent trends in social media governance wherein state security concerns have been invoked to regulate the online information ecosystem. Finally, it analyses India's social media regulatory landscape against established rule of law principles. It concludes that India's social media regulatory framework is not in complete alignment with these rule of law principles.

13 The Digital Personal Data Protection Act, 2023 <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>.

14 Govind Choudhary, 'Government Holds First Consultation on Digital India Act to Replace IT Act 2000' (*Mint*, 10 March 2023) <https://www.livemint.com/news/government-holds-first-consultation-on-digital-india-act-to-replace-it-act-2000-11678440033837.html>.

15 Shouvik Das, 'Govt Prepares New Cyber Security Policy to Beat Malware Attacks' (*Mint*, 14 June 2023) <https://www.livemint.com/technology/govt-prepares-new-cyber-security-policy-to-beat-malware-attacks-11686717816691.html>.

16 Gulveen Aulakh, 'Telecom Bill May Not Make It to Monsoon Session as Talks Continue' (*Mint*, 16 July 2023) <https://www.livemint.com/news/india/new-telecom-bill-unlikely-to-be-tabled-in-monsoon-session-cabinet-approval-awaited-11689527695000.html>; Gulveen Aulakh, 'Govt May Not Table Telecom Bill This Year' *Mint* (5 November 2023) <https://www.livemint.com/industry/telecom/govt-may-not-table-telecom-bill-this-year-11699202938801.html>.

3.2 Cybersecurity and ICT Regulation Applicable to Social Media

Social media regulation in India has direct and indirect interlinkages with cybersecurity law and policy, as well as other ICT domains like telecommunication regulation and data protection. These manifest in the form of (a) cyber incident reporting obligations; (b) data security through civil and criminal liability; (c) critical information infrastructure (CII) and cyberterrorism; (d) data retention requirements; (e) data protection frameworks to safeguard personal data; (f) licensing requirements for telecommunication services; (g) interception, monitoring and decryption of online information and (h) internet shutdowns.[17]

India's IT Act defines "cybersecurity" as "protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction."[18] The NCSP 2013 is the guiding framework to safeguard cyberspace and protect information and information infrastructure. However, its ability to curb cybersecurity risks has been limited due to its inconsistent implementation.[19] Further, the NCSP came into effect in 2013 and has failed to evolve while cyber threats have increased at a fast pace.

Since 2019, India has been in the process of developing a new National Cybersecurity Strategy.[20] Press reports in early 2021[21] indicated that the new strategy could address information security by focusing on the abuse of social media for "narrative warfare".

17 For detailed analysis of (g) and (h) refer to section 3.5, "Regulating the online information ecosystem". See 3.5.2 for detailed analysis of internet shutdowns and 3.5.5 for Law enforcement access to information.

18 Information Technology Act 2000, s 2(1)(nb).

19 As per IBM's X-Force Threat Intelligence team, in 2021, India ranked third in Asia for server access and ransomware attacks.

Cyber incidents continue to wreak havoc on the Indian economy, the average cost of a data breach has increased twenty-five percent from 14 crore in 2020 to 17.6 crore in 2022

See Col. Sanjeev Relia (Retd.), 'India's Tryst with a New National Cyber Security Policy: Here's What We Need' *The Financial Express* (4 August 2021) <https://www.financialexpress.com/business/defence-indias-tryst-with-a-new-national-cyber-security-policy-heres-what-we-need-2304053/>.

20 IANS, 'India in Final Stages of Clearing National Cybersecurity Strategy' Business Standard India (27 October 2021) <https://www.business-standard.com/article/current-affairs/india-in-final-stages-of-clearing-national-cybersecurity-strategy-121102700663_1.html>.

21 Ibid.

These suggest that "... fake news, manipulation, fraud, misinformation and disinformation" are likely to be included in the Strategy.[22]

If the upcoming cybersecurity policy does indeed take this direction, it could possibly impact how content on social media platforms is regulated. In June 2023, India's national cyber security coordinator announced that the National Cyber Security Reference Framework (NCRF) 2023, which will provide strategic guidance to organisations to address cyber security threats, will be published soon.[23]

3.2.1 Data Security and Social Media | Limited Accountability

Data security is prima facie an important facet of social media regulation. This is because in order to execute their monetisation models social media platforms undertake very extensive collection, storage, sharing and processing of personal and non-personal data. It thus becomes imperative to maintain the confidentiality, integrity and availability of such data and protect it from unauthorised access, corruption or theft.

In India, the IT Act governs data security. It contains multiple provisions which assign civil liability to address data security risks to computer resources,[24] systems,[25] and networks[26] — terms which are defined broadly and thus may be interpreted to include social media platforms. The IT Act prescribes penalties for unauthorised persons in cases of:[27]

- accessing computer resources, systems and networks e.g. hacking and/or cracking;
- downloading, copying, or extracting information;

22 Sunetra Choudhury, 'Cyber Policy to Factor in Threat from State Actors' *Hindustan Times* (New Delhi, 5 March 2021) <https://www.hindustantimes.com/india-news/cyber-policy-to-factor-in-threat-from-state-actors-101614897658901.html >.

23 Shouvik Das, 'Govt Prepares New Cyber Security Policy to Beat Malware Attacks' (*mint*, 14 June 2023) <https://www.livemint.com/technology/govt-prepares-new-cyber-security-policy-to-beat-malware-attacks-11686717816691.html>.

24 IT Act 2000, s 2(1)(k).

25 IT Act 2000, s 2(1)(l).

26 IT Act 2000, s (1)(j).

27 IT Act 2000, s 43.

- damaging computer resources, information or software through viruses, contaminants and other means; and
- providing assistance or services to others in accessing computer resources, systems /networks in an unauthorised manner.

The IT Act further provides that such activities will attract criminal penalties should evidence establish mens rea i.e. that the prohibited actions have been committed with "dishonest" and "fraudulent" intent.[28] The IT Act also criminalises the intentional tampering of computer source documents,[29] cheating by impersonation[30] and identity theft.[31]

Additionally, the IT Act assigns civil liability against private entities which fail to implement reasonable security practices and procedures in protecting sensitive personal data or information.[32] To this end, the Indian Government has passed regulations which seek data and information security compliance by private entities, including social media platforms.[33]

However, the efficacy of India's data security provisions under the IT law is dubious. The Cambridge Analytica data breach exemplifies this. The incident, which became publicly known in 2018, involved a political consulting firm using Facebook APIs to compromise data security for information manipulation purposes. It is estimated that over 560,000 Indian Facebook users might have been impacted.[34]

Despite the incident coming to light in 2018, India's legal system has (as of writing) yielded very limited accountability. No criminal or civil action has been taken against Facebook and India's Criminal Bureau of Investigation ("CBI") only filed an FIR against the political

28 IT Act 2000, s 66.

29 IT Act 2000, s 65.

30 IT Act 2000, s 66D.

31 IT Act 2000, s 66C.

32 IT Act 2000, s 43A.

33 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

34 ET Bureau, 'CBI Files Case against Cambridge Analytica for Illegal Harvesting of Facebook Users Data in India' *The Economic Times* (22 January 2021) <https://economictimes.indiatimes.com/news/politics-and-nation/cbi-files-case-against-cambridge-analytica-for-illegal-harvesting-of-facebook-users-data-in-india/articleshow/80400033.cms>.

consulting firm and its affiliates after an extensive investigation which stretched across a prolonged period of time.[35]

The length of that preliminary investigation can partly be attributed to the incompleteness of India's information law and policy framework, which necessitated a close referral to legacy criminal laws under the country's IPC and CrPC.

3.2.2 Cyber Incident Response and Reporting Obligations

The cyber incident response and reporting frameworks are administered by the Computer Emergency Response Team of India ("CERT-In"). India's IT (Amendment) Act 2008, inserted Section 70B to establish CERT-In as the country's nodal agency for cyber incident response. CERT-In is assigned with both reactive and proactive mandates.[36] CERT-In's reactive mandate is most relevant for this study.

The reactive mandate requires CERT-In to perform emergency measures for handling cyber security[37] and coordinating cyber incident response activities.[38] The CERT Rules 2013, which prescribe CERT-In's overall operational framework makes it mandatory for ISPs, intermediaries, data centres, bodies corporate or persons to report certain categories of cybersecurity incidents to CERT-In in a timely manner.[39] Failure to comply with the reporting mandate can mean that defaulting parties are subject to penalties in the form of imprisonment and/or fines.[40]

35 See ET Bureau, 'CBI Files Case against Cambridge Analytica for Illegal Harvesting of Facebook Users Data in India' *The Economic Times* (22 January 2021) <https://economictimes.indiatimes.com/news/politics-and-nation/cbi-files-case-against-cambridge-analytica-for-illegal-harvesting-of-facebook-users-data-in-india/articleshow/80400033.cms>; Scroll Staff, 'CBI Files Case against Cambridge Analytica in Data Breach Scandal: Reports' (*Scroll.in*, 22 January 2021) <https://scroll.in/latest/984787/cbi-files-case-against-cambridge-analytica-in-data-breach-scandal-reports>; HT Correspondent, 'CBI Files Case against Cambridge Analytica, Global Science: Key Points' (*Hindustan Times*, 22 January 2021) <https://www.hindustantimes.com/india-news/cbi-files-case-against-cambridge-analytica-uk-s-global-science-research-ltd-101611292060859.html>.

36 For more about CERT-In's proactive mandate read: Udbhav Tiwari, Cyber Security and CERT-In: A Report on the Indian Computer Emergency Response Team's Proactive Mandate on the Cyber Security Ecosystem, The Centre for Internet and Society (November 2016) <https://cis-india.org/internet-governance/blog/cert-ins-proactive-mandate-a-report-on-indian-computer-emergency-response-teams-proactive-mandate-in-indian-cyber-security-ecosystem#:~:text=CERT-%2DIN's%20proactive%20mandate%20is,itself%2C%20which%20has%20been%20operational>.

37 IT Act 2000, s 70B (4)(c).

38 IT Act 2000, s 70B (4)(d).

39 Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, Rule 12(1)(a) read with the Annexure.

40 IT Act, s 70B (7).

Since it applies to intermediaries, the aforementioned cyber incident response framework and accompanying obligations are applicable to social media platforms. This was explicitly codified as a mandatory requirement when intermediaries were required to report cybersecurity incidents to CERT-In under the Intermediary Guidelines, 2021.[41]

Subsequently, in April 2022, CERT-In issued directions under the IT Act which imposed stricter cyber incidents reporting obligations within six hours of knowledge of specified cyber incidents.[42] Among others, that list included "unauthorised access to social media accounts".[43] Another key provision in these directions is that covered entities must maintain logs of all their ICT systems and maintain them for a period of 180 days.

Even before April 2022 directions India's cyber incident response framework have applied to social media. When deposing before the Joint Parliamentary Committee on Data Protection, India's Minister of Electronics and Information Technology highlighted that social media platforms were legally mandated to report all cybersecurity incidents affecting their platforms to CERT-In.[44] Additionally, in light of the Cambridge Analytica breach which compromised the personal information of over 560,000 Indian Facebook users, CERT-In issued an advisory which advocated internet users adopt social media security best practices.[45]

This section demonstrates that over time the government has been imposing more specific (and stringent) cyber incident response conditions (and the penalties which accompany its non-compliance) over social media platforms. This trend is important to trace as India continues to reform its digital governance landscape.

41 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(1)(l).

42 No. 20(3)/2022-CERT-In, April 28, 2022, <https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf>.

43 Ibid. Annexure 1, Item (xvii).

44 Joint Committee on the Personal Data Protection Bill 2019, *Report of the Joint Committee on the Personal Data Protection Bill 2019* (Lok Sabha 2021) para 1.15-12.5.

45 Pranab Dhal Samanta, Tell us who all in India have used your services: Modi government issues notice to Cambridge Analytica, *The Economic Times* (May 2018) <https://economictimes.indiatimes.com/news/politics-and-nation/tell-us-who-all-in-india-have-used-your-services-modi-government-issues-notice-to-cambridge-analytica/articleshow/63432675.cms?from=mdr>.

3.2.3 Critical Information Infrastructure Protection

Another strand of cybersecurity regulation which is incidental and may become relevant for social media in the future relates to the protection of critical information infrastructures ("CIIs"). The IT Act defines "critical information infrastructure" broadly as computer resources which if incapacitated or destroyed will have a debilitating impact on national security, economy, public health, or public safety.[46] Any computer resource that directly or indirectly impacts CII may be designated as a protected system by central or state government authorities.

The designation of any computer resource as a protected system under section 70 of the IT Act results in heightened scrutiny and punishment in the event of an incident or breach. Currently, the government has identified six critical sectors.[47] These are (a) Transport; (b) Power and energy; (c) Telecom; (d) Government; (e) Banking, Finance and Insurance; and (f) Strategic and Public Enterprises. Any unauthorised person who attempts to or secures access to protected systems is liable to imprisonment for up to ten years.[48] It is essential to convey that "critical sectors" are vaguely defined under Indian law as sectors which are "... critical to the nation and whose incapacitation or destruction will have a debilitating impact on national security, economy, public health or safety ..."[49]

3.2.4 Cyber Terrorism

The IT Act was amended in January 2009 and introduced the offence of cyber terrorism.[50] Here, it is important to keep in mind that this amendment was introduced in the aftermath of a major terrorist attack in Mumbai in November 2008.[51] This national security context behind the amendment is important to keep in mind as we study the actual legal contours

46 IT Act 2000, s 70(1).

47 National Critical Information Infrastructure Protection Centre <https://www.nciipc.gov.in/?p=sector>.

48 IT Act 2000, s 70(3).

49 Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules 2013, Rule 2(1)(e).

50 IT Act 2000, s 66F.

51 Debarati Halder, 'Information Technology Act and Cyber Terrorism: A Critical Review' (1 August 2011) <https://papers.ssrn.com/abstract=1964261>.

of the offence and how it is implemented. Section 66 F of the IT Act defines cyber terrorism as an offence in three distinct forms:[52]

Form 1 addresses (a) denial of access to authorised persons; (b) unauthorised access; and (c) the introduction of contaminants (e.g. malicious software). When these activities concerning computer systems and networks lead to death, injuries, property damage, disruption, or denial of essential services, or adversely impact "critical information infrastructure" – then they constitute an offence of cyber terrorism.

Form 2 addresses activities which knowingly or intentionally penetrate "computer resources" without appropriate authorisation to access information, data or databases, that have been restricted for reasons relating to State security.

Form 3 is similar to Form 2 and is applicable when accessing restricted information where the concerned party has "reasons to believe" that unauthorised access to information/ data can cause injury to not only India's State security but also harm public order, decency, morality, or lead to contempt of court or any criminal offence.

Form 3 has a broad ambit, with the potential for discretionary implementation by LEAs. This potential for discretion has manifested in authorities using the provision in the context of online speech over social media—an area which is not explicitly mentioned or even conceived when the provision was enacted. For example, a journalist was arrested for cyber terrorism for social media posts in Haryana.[53] Similarly, students in Kashmir have been arrested for cyber terrorism for social media posts celebrating the victories of Pakistan's cricket team.[54]

This demonstrates evidence of a mismatch between the overarching purpose of this provision and its actual implementation, which has been used by LEAs as a mechanism for controlling speech over social media.

52 Vakul Sharma, Information Technology Law and Practice (Universal Law Publishing 2011), pp. 279.

53 PTI, 'Haryana: Journalist Booked For "Cyber-Terrorism" Over Social Media Post' (*The Wire*) <https://thewire.in/media/haryana-journalist-booked-for-cyber-terrorism-over-social-media-post>.

54 Safwat Zargar, 'Kashmiri Students Charged with Cyberterrorism, Sedition for Allegedly Cheering Pakistan Cricket Team' (*Scroll*, 29 Jan 2022) 2022 <https://amp.scroll.in/article/1016166/illegal-custody-says-lawyer-of-three-kashmiri-students-held-in-an-agra-jail-for-three-months>.

3.2.5 Data Protection and Social Media

As data-driven algorithms became more sophisticated and integral to the operation of online services, including social media intermediaries, it became clear that protecting citizens' rights is not limited to ensuring data security. It became critical to protect citizens' privacy and ensure that personal data is processed in a fair and legal manner.

Section 43A of the IT Act governs the collection and processing of personal data. Currently, it provides compensation for failure to protect sensitive personal data by a body corporate. It also provides a remedy to users in case of negligence in maintaining "reasonable security practices and procedures", causing wrongful harm or wrongful gain to any person.

Pursuant to this, the central government notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") to provide detailed guidelines on handling sensitive personal data or information.[55] All private entities that fail to implement reasonable security practices and procedures in protecting sensitive personal data or information can be implicated under the SPDI Rules.[56]

However, the remedy under Section 43A has proven to be inadequate due to its limited scope.[57] This provision lacks an adequate framework to ensure the accountability of platforms, without a regulatory authority that enforces the SPDI Rules. To successfully claim compensation, the affected party must prove that the body corporate failed to adopt 'reasonable security practices' causing 'wrongful loss'. The scope of sensitive personal data is also limited to passwords, health data, financial data, or biometrics.[58] Besides the

55 The body corporate needs to take the consent of the data subject for collection of SPDI for a particular purpose and also notify them regarding the same and provide the option to withdraw such consent. The body corporate can collect SPDI only if its necessary for a lawful purpose and is used only for the said purpose. Disclosure or transfer of SPDI information to third parties will require the consent of the data subject unless it has been agreed to in a lawful contract or is mandated by any law .The rules also mandate that while transferring data it must also be ensured that the same level of data protection is accorded by the recipient.

56 IT Act 2000, s 43A read with SPDI Rules 2011.

57 Surabhi Agarwal, 'IT Act allows govt to pull up platforms for data misuse', *The Economic Times*(April 3, 2018) <www.economictimes.indiatimes.com/tech/internet/it-act-allows-govt-to-pull-up-platforms-for-data-misuse/articleshow/63588414.cms>.

58 Siddharth Sonkar 'Privacy Delayed Is Privacy Denied' (*The Wire*, 24 May 2021) <https://thewire.in/tech/data-protection-law-india-right-to-privacy>.

narrow definition of sensitive personal data, this provision is restricted to cases with demonstrable financial loss.[59]

Aside from substantive limitations, the framework's full potential in terms of implementation is hindered, because there is limited enforcement due to limited institutional capacity and resource allocation.[60] As a result, most digital platforms, including social media platforms, are left with limited incentives to comply wholly. Instead, they tend to show superficial compliance, by only publishing a privacy policy which reflects the language outlined under India's SPDI Rules.[61]

However, there has been a shift in approach to data protection. In 2017, India's Supreme Court reaffirmed the right to privacy as a fundamental constitutional right.[62] Since the Supreme Court's decision, the Indian government has worked on a comprehensive data protection law to replace existing frameworks under the IT Act.

The prolonged journey has included one independent expert committee,[63] one joint parliamentary committee,[64] one consultation by the Telecom Regulatory Authority of India ("TRAI"),[65] and multiple public consultations by ministries of the Indian government. In that period, there has been one committee white paper (2017),[66] an expert committee

59 Ibid.

60 White Paper of the Committee of Experts on a data protection framework for India, Ministry of Electronics and Information (2017) Technology <https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf>,p 17.

61 The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 <https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf>

62 Justice K.S. Puttaswamy vs. Union of India (2017) 10 SCC 1.

63 'Justice Krishna to head expert group on Data Protection Framework for India, PIB, Ministry of Electronics & IT' (Press Information Bureau, 2019) <https://pib.gov.in/newsite/PrintRelease.aspx?relid=169420>.

64 Joint Committee on the Personal Data Protection Bill 2019, *Report of the Joint Committee on the Personal Data Protection Bill 2019* (Lok Sabha 2021).

65 Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector,Telecom Regulatory Authority of India (2017) <https://trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf>.

66 White Paper of the Committee of Experts on a data protection framework for India, (Ministry of Electronics and Information Technology, 2017) <https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf.

report (2018),[67] a joint parliamentary committee report (2021),[68] a draft legislation in 2018,[69] a 2019 legislation[70] which was introduced in the Indian Parliament, and a draft 2021 legislation[71] which was submitted by the aforementioned joint parliamentary committee to the Indian Parliament.

The Indian government ultimately withdrew the draft 2021 legislation from the Parliament in August 2022.[72] In November 2022, India's Ministry of Electronics and Information Technology ("MeitY") released a fresh draft of a proposed legislation for public consultation.[73] This latest draft was entitled The Digital Personal Data Protection Bill, 2022.[74] Finally, the Digital Personal Data Protection Act, 2023 (DPDPA) was passed in August 2023. It is likely to come into force in the coming months as the central government notifies various provisions of the law.[75]

Several of its provisions attempt to introduce greater accountability for data collection and processing activities of digital companies, especially social media platforms.

Firstly, user consent is a prerequisite to the data collection and processing activities of all private entities (including social media platforms).[76] Secondly, digital entities ("data fiduciaries") like social media companies are required to provide users with notice about

67 Committee of Experts under Chairmanship of Justice B.N Srikrishna Submitted to Ministry of Electronics and Information Technology, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians (2018)<https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf>.

68 Anushka Jain and others, 'Key Takeaways: The JPC Report and the Data Protection Bill, 2021 #SaveOurPrivacy' (*Internet Freedom Foundation*, 16 December 2021) <https://internetfreedom.in/key-takeaways-the-jpc-report-and-the-data-protection-bill-2021-saveourprivacy-2/>.

69 The Personal Data Protection Bill, 2018.

70 The Personal Data Protection Bill, 2019.

71 Joint Committee on the Personal Data Protection Bill 2019, *Report of the Joint Committee on the Personal Data Protection Bill 2019* (Lok Sabha 2021) <https://drive.google.com/file/d/1emcAB8HjE2oCC_DI6zR5YPnPQ5iwwwCT/view>.

72 Soumyarendra Barik, 'Govt Withdraws Data Protection Bill to Bring Revamped, Refreshed Regulation' *The Indian Express* (New Delhi, 3 August 2022) <https://indianexpress.com/article/india/government-withdraws-data-protection-bill-8068257/>.

73 The Digital Personal Data Protection Bill 2022, *PIB* (2022) <https://pib.gov.in/PressReleasePage.aspx?PRID=1881402>

74 The Digital Personal Data Protection Bill, 2022.

75 Soumyarendra Barik, 'Your Personal Data Online: Five Key Questions Answered' *The Indian Express* (4 September 2023) <https://indianexpress.com/article/explained/explained-economics/personal-data-act-key-questions-8923846/>.

76 The Digital Personal Data Protection Act 2023, s 4(1).

(a) the types/categories of personal data that they collect/process, (b) the purpose for which this collection/processing takes place, and (c) information on grievance redressal for Data Principals.[77]

Thirdly, the DPDPA contemplates graded regulation, with heightened compliance obligations for large digital enterprises, which would very likely include some social media platforms. It creates a special category of digital entities known as "significant data fiduciaries", which are imposed with special institutional compliance requirements like (a) appointing a designated data protection officer, (b) carrying out regular data protection impact assessments, and (c) periodic data audits.[78]

The government can notify any digital entity or a class of digital entities ("data fiduciaries") as significant data fiduciaries. Its determination is proposed to be based on criteria such as:[79]

- the volume and sensitivity of personal data processed,
- risks to the rights of the data principal,
- the impact a platform's activities can have on the sovereignty and integrity of India,
- the platform's perceived risk to "electoral democracy",
- security of the state,
- and public order.

Given these criteria, it is likely that major social media platforms will be classified as "significant data fiduciaries" under the above proposal.

Fourthly, another relevant feature of the DPDPA concerning social media platforms pertains to data retention. Data fiduciaries must erase personal data when (a) the data principal withdraws their consent or (b) the specified purpose of processing is no longer being served. However, this is not applicable when data retention is "necessary for compliance with any law for the time being in force".[80]

77 DPDPA 2023, s 5(1).
78 DPDPA 2023, s 10(2).
79 DPDPA 2023, s 10(1).
80 DPDPA 2023, s 7.

This leaves room for the government to require social media platforms (as would be the case with most digital entities) by law to retain people's personal data (i.e. personally identifiable information) for extended periods. Since this can be for legal purposes, it is clear that social media platforms could be directed under India's data protection framework to retain personal data for extended periods to support law enforcement objectives.

Finally, the DPDPA confers powers on the central government to direct any agency or intermediary to block public access to "any information generated, transmitted, received, stored, or hosted, in any computer resource that enables such data fiduciary to carry on any activity relating to the offering of goods or services to data principals within the territory of India" in the "interests of the general public".[81]

The Data Protection Board can advise blocking of data fiduciaries to the central government after it has issued monetary penalties twice or more to the entity.[82] Before issuing such a blocking order, a hearing has to be provided to the concerned data fiduciary.[83] However, the unprecedented blocking powers and the overbroad and vague grounds of "public interest" have been criticised.[84] Concerns about potential censorship become even more prominent if such blocking is directed at content and extends beyond blocking services of non-compliant businesses.[85] It is also important to note that this provision did not exist in any of the previous draft proposals.

81 DPDPA 2023, s 37(1)(b).

82 DPDPA 2023, s 37(1)(a).

83 DPDPA 2023, s 37(1)(b).

84 Aarathi Ganesan, 'Censorship Concerns with New Blocking Powers under India's Data Protection Bill' (*MediaNama*, 7 August 2023) <https://www.medianama.com/2023/08/223-censorship-concerns-blocking-powers-data-protection-bill/>; Shruti Shreya, 'What's a Content Blocking Provision Doing in a Data Protection Legislation?' *Moneycontrol* (8 August 2023) <https://www.moneycontrol.com/news/opinion/whats-a-content-blocking-provision-doing-in-a-data-protection-legislation-11119181.html>.

85 See Jhalak M Kakkar and Shashank Mohan, 'Data Protection Bill: In Process and Practice, a Step Back' *The Indian Express* (19 August 2023) <https://indianexpress.com/article/opinion/columns/data-protection-bill-in-process-and-practice-a-step-back-8899924/>.

3.2.6 Proposed Telecom Reform

The Indian Government's draft Indian Telecommunication Bill, 2022 (Telecom Bill) – released for public consultation[86] – proposed updating the legal regime for telecom and ISPs. The Telecom Bill, *inter alia*, proposed an expansive definition of "telecommunication services"— a class of services which are to be governed under a dedicated licensing framework.[87]

As a result, it essentially proposed bringing most digital services within the scope of this licensing framework. The broad definition of "telecommunication services" means that any reasonable interpretation of the term would bring social media platforms within the scope of the envisioned licensing framework.

The Telecom Bill contains a dedicated chapter on national security, public emergency, and public safety. Notably, it attempts to provide a framework which ensures that internet and digital service providers (including social media platforms) cooperate with the Indian government across these various security-laden objectives (and provisions) in cyberspace.[88]

Thus, the Indian government's recent proposals to reform the country's legal regime for telecommunications reflects a push towards measures to achieve the state's security objectives.[89] It provides the government with wide powers in matters relating to internet suspension, content blocking, and interception and monitoring in times of public emergency or public safety.[90] For instance, clause 24(2) of the Bill empowers the central and state government during a public emergency or in the interest of public safety to "intercept or detain or disclose" any communication "to or from any person or class of persons or

86 Draft Indian Telecommunication Bill 2022 <https://dot.gov.in/sites/default/files/Draft%20Indian%20Telecommunication%20Bill%2C%202022.pdf>.

87 'Global Technology Products, U.S. Security Policy, and Spectrums of Risk' (Default). <https://www.lawfaremedia.org/article/global-technology-products-u.s.-security-policy-and-spectrums-of-risk>.

88 CCG, 'Comments to the Department of Telecommunications on the Draft Indian Telecommunication Bill, 2022' (Centre for Communication Governance, 9 Nov 2022) <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccgnlud-telecom-bill-comments-326.pdf>.

89 Anunay Kulshrestha and Gurshabad Grover, 'Comment on the Indian Telecommunication Bill 2022' (November 2022). <https://gurshabad.github.io/writing/Anunay_Kulshrestha-Gurshabad_Grover-Comments_Telecommunication_Bill_2022.pdf>.

90 Draft Indian Telecommunication Bill 2022, clause 24(2).

relating to any particular subject" in the interest of "sovereignty, integrity or security of India, friendly relations with foreign states, public order, or preventing incitement to an offence". This provision has garnered criticism for its potential implications on End to end encryption (E2EE) and user privacy.[91] Clause 25 goes further and grants exceptional powers to the central government, including "taking over the control and management of any or all telecommunications services" in the interest of "national security, friendly relations with foreign states, or in the event of war". The Draft Telecommunications Bill was heavily criticised by civil society and prominent platforms.[92]

3.3 India's Approach to Regulating Social Media Platforms

This section analyses regulations which oversee the day-to-day operations of social media platforms. Social media platforms are regulated primarily under India's intermediary liability regime contained in the IT Act. Intermediaries are defined broadly; they include "telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online marketplaces and cyber cafes".[93] Social media platforms also fall within the ambit of this broad definition.

Section 79 of the IT Act holds that intermediaries are not liable for the third-party content they host, provided they meet certain conditions. They must for instance fulfil "due diligence" obligations, prescribed by the government via delegated legislation. India's current due diligence framework for internet intermediaries was promulgated in February 2021.

91 'India's Draft Telecommunication Bill Must Be Revamped to Protect Human Rights' (*Access Now*, 22 September 2022) <https://www.accessnow.org/press-release/telecommunication-bill-india/>.

92 See Chetan Thathoo, 'Proposed Telecom Law Undermines Free Speech, Burdens OTT Apps: Internet Body' *Inc42 Media* (6 November 2022) <https://inc42.com/buzz/proposed-telecom-law-undermines-free-speech-burdens-ott-apps-internet-body/>; Aihik Sur, 'Draft Telecom Bill an Attack on End-to-End Encryption, Say Digital Rights Groups' *Moneycontrol* (23 September 2022) <https://www.moneycontrol.com/news/business/draft-telecom-bill-an-attack-on-end-to-end-encryption-say-digital-rights-groups-9221811.html>.

93 IT Act 2000, s 2(1)(w).

The process began in December 2018 MeitY released the draft Information Technology [Intermediary Guidelines (Amendment) Rules] (Intermediary Guidelines 2018) for public consultation.[94] The Intermediary Guidelines 2018 were slated to replace the then-existing Information Technology (Intermediaries Guidelines) Rules 2011 (Intermediary Guidelines 2011).

However, the Intermediary Guidelines 2018 never became law. They were widely criticised during the public consultation process for exceeding the permissible lawful scope of delegated legislation under the IT Act.[95] Critics also highlighted the fact that the Intermediary Guidelines 2018 undermined the right to freedom of speech and the right to privacy.[96]

Despite this barrage of criticism, the government promulgated the Intermediary Guidelines, 2021 by building on the main provisions of the Intermediary Guidelines 2018.

3.3.1 Safe Harbour Protection

As discussed above, the safe harbour protection afforded to intermediaries is conditional upon compliance with due diligence requirements.[97] Also, section 79(2) of the IT Act lays down that intermediaries must act as mere conduits for information dissemination and not modify the information/content they host — if they want to qualify for safe harbour protection.

The Intermediary Guidelines 2021 clarify that this restriction does not constrain intermediaries from engaging in voluntary content moderation.[98] It will be interesting to see whether intermediaries will receive similar treatment in the upcoming Digital India Act.

94 The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018. <https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf> accessed 30 March 2022.

95 'Intermediary Liability 2.0: A Shifting Paradigm' (2019). <https://sflc.in/wp-content/uploads/2019/03/Intermediary_Liability_2_0_-_A_Shifting_Paradigm.pdf>.

96 See Apar Gupta, 'India Must Resist the Lure of the Chinese Model of Online Surveillance and Censorship #IntermediaryRules #RightToMeme #SaveOurPrivacy' (*Internet Freedom Foundation*, 24 December 2018) <https://internetfreedom.in/india-must-resist-the-lure-of-the-chinese-model-of-surveillance-and-censorship-intermediaryrules-righttomeme-saveourprivacy/>; Abhijit Ahaskar, 'What the Government's Draft IT Intermediary Guidelines Say' Mint (12 February 2019) <https://www.livemint.com/technology/tech-news/what-the-government-s-draft-it-intermediary-guidelines-say-1549959448471.html>.

97 IT Act 2000, s 79.

98 Vasudev Devadasan, 'Report on Intermediary Liability in India (December 2022)' [2023] Centre for Communication Governance.

Section 79 of the IT Act, read with the Intermediary Guidelines 2021, requires intermediaries to expeditiously remove or disable public access to unlawful information upon receiving "actual knowledge".[99] The Supreme Court's landmark judgement in *Shreya Singhal v. Union of India* clarified an intermediary obtains actual knowledge once it receives a takedown order either from a court or an appropriate government authority.[100] Section 69A of the IT Act is a major statutory mechanism through which the executive can issue content-blocking orders to intermediaries.[101]

Rules 3, 4 and 5 of the Intermediary Guidelines, 2021 constitute some of the major due diligence requirements for intermediaries. Rule 4 applies to a class of intermediaries known as "significant social media intermediaries" (SSMIs). Rule 5 comprises additional due diligence obligations for intermediaries in the context of news and current affairs content. They are analysed below.

3.3.2 Institutional Compliance for Safe Harbour Protection

As indicated above, the Intermediary Guidelines 2021 created new classes of intermediaries – known as Social Media Intermediaries (SMIs) and Significant Social Media Intermediaries (SSMIs). The government has specified, via notification, that any SMI with more than five million registered users in India constitutes an SSMI.[102]

SSMIs are required to comply with additional due diligence obligations under Rule 4 of the Intermediary Guidelines, 2021.[103] These additional obligations are designed to minimise the impact of online harms from social media platforms with greater user bases, virality and reach.[104]

More generally the Intermediary Guidelines 2021 have increased the due diligence obligations for intermediaries. The Intermediary Guidelines, 2021 have expanded the requirement for intermediaries to institute a redressal mechanism, appoint local officers

99 IT Act 2000, S. 79(3)(b).

100 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [121].

101 See section 3.4.3 for detailed analysis.

102 MeitY, Notification S.O. 942(E) dated 25 February 2021 <https://www.meity.gov.in/writereaddata/files/Gazette%20Significant%20social%20media%20threshold.pdf>.

103 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Rule 4.

104 Ministry of Electronics & Information Technology, Open, Safe & Trusted And Accountable Internet: Frequently Asked Questions (FAQs) on Part II of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (MeitY 2021) <https://www.meity.gov.in/writereaddata/files/FAQ_Intermediary_Rules_2021.pdf?ref=static.internetfreedom.in>[FAQ 12].

and comply with technical requirements such as requiring private messaging platforms to identify the first originator of information for monitoring communications.

The institutional requirements require SSMIs, which are predominantly headquartered outside India, to appoint dedicated local officials for (a) compliance,[105] (b) grievance redressal ,[106] and (c) dynamic contact and coordination with LEAs.[107]

Additionally, the Intermediary Guidelines 2021 introduced softer compliance measures to address accountability and oversight of platform operations. This includes periodic transparency/compliance reports for content takedowns and voluntary verification of users.[108] Since then, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 (Intermediary Guidelines, 2022) has built on these accountability and oversight mechanisms by providing for the creation of Grievance Appellate Committees (GACs). The GACs are analysed in section 3.3.5 of this chapter.

Thus, major due diligence requirements under the intermediary liability framework include: publishing monthly compliance reports,[109] traceability of the "first originator" of unlawful content,[110] best efforts deployment of automated tools for filtering content,[111] and establishing a redressal mechanism for voluntary takedowns.[112]

Non-compliance with these provisions will disqualify intermediaries from receiving safe harbour protection; consequently, they will be held liable for the unlawful third-party content[113] that they host. This will open intermediaries to civil and criminal lawsuits as a publisher of content. The Intermediary Guidelines 2021, illustrate a worldwide trend wherein governments are departing from the foundations of global intermediary liability laws, which are premised on robust safe harbour protections.

105 Intermediary Guidelines 2021, Rule 4(1)(a).
106 Intermediary Guidelines 2021, Rule 4(1)(c).
107 Intermediary Guidelines 2021, Rule 4(1)(b).
108 Intermediary Guidelines 2021, Rule 4(1)(d) and Rule 18(3).
109 Intermediary Guidelines 2021, Rule 4(1)(d).
110 Intermediary Guidelines 2021, Rule 4(2).
111 Intermediary Guidelines 2021, Rule 4(4).
112 Intermediary Guidelines 2021, Rule 4(8).
113 MeitY (n 104). [FAQ 27].

3.3.3 Regulation of Digital Media

Disinformation and news aggregation are regulated partially under Part II and primarily under Part III of the Intermediary Guidelines 2021. Rule 5 of Part II prescribes additional due diligence requirements concerning news and current affairs content to intermediaries. It requires intermediaries (including social media intermediaries) to ensure that news and current affairs publishers share all relevant information relating to their user profiles/ accounts.[114] Once such information is furnished, social media platforms are subsequently permitted to provide such publishers with a public and visible mark of verification (e.g. a blue tick).[115]

The government, specifically the Ministry of Information and Broadcasting (MIB), also has the power to issue emergency directions for issues of expediency which conform to standards provided under Section 69A of the IT Act.[116] Therefore, the emergency directions for expedient content removal provide the government with tremendous leeway. Specifically, the powers under the emergency directions provision can be exercised by the government on numerous grounds, such as national security, public order, and even prevention of the commission of any cognisable offence relating to the above.[117] The confidentiality clause in the Blocking Rules[118] also means that there is a lack of publicly available information on blocking orders, making it difficult to distinguish blocking orders that have been issued under emergency directions from those issued under standard blocking procedure (see section 3.5.3 for more detail).

This empowers the government to utilise its powers under this provision with wide discretion by citing "national security, India's foreign relations, and public order" concerns. There is evidence of Part III blocking and content modification powers being exercised over social media platforms like YouTube, Twitter (now X) and Meta.[119]

114 Intermediary Guidelines 2021, Rule 5 r/w Rule 18.

115 Intermediary Guidelines 2021, Rule 5 Proviso.

116 Intermediary Guidelines 2021, Rule 16(1).

117 Ibid "... in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above...".

118 Blocking Rules 2009, Rule 16.

119 Sarvesh Mathi, "Ministry Of Information And Broadcasting Blocks 22 YouTube Channels For Spreading Fake News And Disinformation," (April 6, 2022) <https://www.medianama.com/2022/04/223-mib-blocks-youtube-channels/>.

Indeed, a growing body of evidence indicates that the MIB's emergency blocking power is subject to arbitrary use.[120] This raises serious questions about its constitutionality.[121] Various challenges have been instituted at the High Courts, resulting in interim orders that suspend the enforceability of some provisions of the Intermediary Guidelines (See Section 3.2.9).[122]

Finally, Part III also requires publishers of news and current affairs content to submit monthly compliance reports to the MIB.[123]

3.3.4 Traceability and End-to-End Encryption

The broad definition of SMIs includes private messaging and communication services like WhatsApp and Signal, which consequently brings them within the ambit of India's social media regulatory framework. WhatsApp, for instance, is an extremely popular peer-to-peer internet service in India.[124] A massive volume of communication takes place over such services - they have thus become a digital enabler of both legitimate and illegal activities/interactions.[125]

These prominent digital messaging services secure their users' communications through end-to-end encryption. This protection of user data creates complications for legal authorities who are entrusted with preventing, investigating, and/or prosecuting unlawful activities which, *inter alia*, occur or are enabled by encrypted messaging services.

120 Tejasi Panjiar and Prateek Waghre, 'Censorship, Surveys, and Seizures: Developments around the BBC Documentary' (*Internet Freedom Foundation*, 3 March 2023) <https://internetfreedom.in/developments-around-the-bbc-documentary/>; Sukumar Muralidharan, 'Media in India: Shackled and Spied on – The Leaflet' (The Leaflet, 3 May 2022) <https://theleaflet.in/media-in-india-shackled-and-spied-on/>.

121 Dhruv Bhatnagar, Evaluating MIB's emergency blocking power under Rule 16 of the 2021 Intermediary Guidelines (Part II), CCG Blog, Centre for Communication Governance, National Law University Delhi, June 2022, https://ccgnludelhi.wordpress.com/2022/06/03/guest-post-evaluating-mibs-emergency-blocking-power-under-rule-16-of-the-2021-it-rules-part-ii/>.

122 'IT Rules #2' (Supreme Court Observer, 27 July 2022) <https://www.scobserver.in/reports/it-rules-2-sc-to-decide-whether-to-transfer-pending-challenges/>.

123 Intermediary Guidelines 2021, Rule 18(3).

124 Shirin Ghaffary, 'How India Runs on WhatsApp' (The Verge, 24 August 2022) <https://www.theverge.com/23320306/whatsapp-india-messaging-business-privacy-land-of-the-giants>.

125 Rama Lakshmi, 'Video Recordings of Gang Rapes on Rise in India in Effort to Shame, Silence the Victim' Washington Post (15 April 2023) <https://www.washingtonpost.com/world/video-recordings-of-gang-rapes-on-rise-in-india-in-effort-to-shame-silence-the-victim/2014/08/13/41d8be42-3360-4081-9ff0-dee2df54f629_story.html>.

In India, for instance, authorities have sought to investigate unlawful user activities and interactions on encrypted platforms. This creates an inherent tension between the government's legal/regulatory mandate to secure security and public order and users' rights linked with privacy and free speech.

Section 69 of the IT Act seeks to break the impasse. It grants designated LEAs and intelligence agencies the power to issue orders to intercept, monitor, or decrypt „information through any computer resource".[126] Such monitoring and interception orders are meant to be directed towards offences/crimes related to state security or public order. After recording the reasons in writing, authorised agencies may issue orders to investigate an offence by gathering information from people's communication devices. These information requests can be extended to person's information which is stored on computer resources owned, operated and controlled by internet intermediaries.[127]

Social media platforms are required to assist LEAs with their users' personal information when they receive an order under section 69 of the IT Act.[128] When they fail to comply with interception/decryption requests, they become subject to criminal penalties — up to seven years imprisonment and/or fines. The government has supplemented section 69 with the Interception Rules, 2009.

These rules provide that interception/decryption orders can only be issued by a competent authority. They allow other government officers of a senior designation ('Joint Secretary' or higher) to issue information/decryption orders during "unavoidable circumstances".[129] These officers must be duly authorised by the designated competent authority of the government.

According to the Interception Rules, 2009 the competent authority and the overseeing review committee are both situated within the executive branch of government. The review committee is tasked with the responsibility of reviewing the legal and constitutional

126 IT Act 2000, s 69.

127 IT Act 2000, s 69(3).

128 See Jhalak M. Kakkar and others, 'The surveillance law landscape in India and the impact of Puttaswamy' [2023], Centre for Communication Governance, <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/the-surveillance-law-landscape-in-india-and-the-impact-of-puttaswamy-476.pdf>.

129 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 3, 5 and 8.

validity of interception/decryption orders. One common criticism of the Interception Rules 2009, is that they do not provide for judicial oversight to adjudicate upon the validity of interception orders.[130] (see section 3.5.5 for more detail)

This overarching legislative framework forms the legal baseline upon which the traceability debate in India has emerged. In 2019, the Supreme Court highlighted that if decryption is easily available, it would defeat the fundamental right to privacy and should only be allowed in special circumstances.[131] The Supreme Court emphasised that certain content on social media, such as content that incites violence, content against the sovereignty and integrity of the country, pornographic or paedophilic content, selling of contraband objects, etc, is harmful.[132] In such instances the first originator of said unlawful content must be traced as "it is imperative that there is a properly framed regime to find out the persons/institutions/bodies who are the originators of such content/messages."[133]

[134]In this regard, the Intermediary Guidelines 2021, introduced a provision which stated that SSMIs which act primarily as messaging services "... shall enable the identification of the first originator of the information on its computer resource".[135] This may be done pursuant to (i) a judicial order from a court of competent jurisdiction or (ii) an order from a competent authority as provided in section 69 of the IT Act read with the Interception Rules, 2009.[136]

This request for information on the first originator must be recorded in an order in an electronic format. In a case where the first originator resides outside India the liability of such content would be on the first originator of that content within the territory of

130 Rishab Bailey and others, 'Use of Personal Data by Intelligence and Law Enforcement Agencies' [2018] Macro/Finance Group, National Institute of Public Finance and Policy.

131 Facebook Inc v Union of India TP (C) 1943-46 of 2019 (Supreme Court of India, 24 September 2019) https://main.sci.gov.in/supremecourt/2019/27178/27178_2019_13_24_17064_Order_24-Sep-2019.pdf.

132 Ibid p 4.

133 Ibid p 4.

134 Ibid.

135 Intermediary Guidelines 2021, Rule 4(2).

136 Intermediary Guidelines 2021, Rule 4(2).

India. The provision does have a clarification that states that in complying with an order for identification of the first originator, the concerned messaging intermediary will not be required to disclose the contents of any electronic message, or any other information related to the first originator.

It has also been argued[137] that the traceability provisions mandated under the Intermediary Guidelines 2021 impose more stringent obligations on the intermediaries as compared to the Interception Rules 2009. This is because the Interception Rules state that decryption "shall be limited to the extent the information is encrypted by the intermediary or the intermediary has control over the decryption key."[138] This does not appear to require creating backdoors or altering platform design to enable decryption.[139] However, the Intermediary Guidelines mandate intermediaries to "enable the identification of the first originator"[140]

India's traceability provision under the Intermediary Guidelines 2021 has been extensively critiqued by scholars[141] as a technical mandate which is: (a) difficult to implement and likely ineffective; (b) weakens ecosystem-level cybersecurity, (c) erodes the data minimisation principle; (d) and is inconsistent with the proportionality threshold for reasonable restrictions to citizens' fundamental right to privacy. Based on such factors the constitutionality of the traceability provision has been challenged in multiple High Courts across India.[142]

137 Jhalak M. Kakkar and others, 'The surveillance law landscape in India and the impact of Puttaswamy' (CCG 2023).

138 Interception Rule 2009, Rule 13.

139 Vrinda Bhandari, Rishab Bailey and Faiza Rahman, 'Backdoors to Encryption: Analysing an Intermediary's Duty to Provide "Technical Assistance"' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3805980> ; Jhalak M. Kakkar and others, 'The surveillance law landscape in India and the impact of Puttaswamy' (CCG 2023).

140 Intermediary Guidelines 2021, Rule 4 (2).

141 Grover, Gurshabad, Rajwade, Tanya and Katira, Divyank. "The Ministry and the Trace: Subverting End-to-End Encryption. *NUJS L. Rev*, Vol. 14 (2), 2021. <http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption>; Katitza Rodriguez, 'Why Indian Courts Should Reject Traceability Obligations' (*Electronic Frontier Foundation*, 2 June 2021) <https://www.eff.org/deeplinks/2021/06/why-indian-courts-should-reject-traceability-obligations>.

142 Legal Challenges to the Traceability Provision: What is Happening in India?, Software Freedom Law Centre, May 2021, https://sflc.in/legal-challenges-traceability-provision-what-happening-india.

3.3.5 Grievance Appellate Committee (GAC) Framework

More recently, in October 2022—after a public consultation, the Indian Government amended the Intermediary Guidelines 2021.[143] Via this amendment, the government has created certain minimum institutional compliance requirements relating to content moderation for all intermediaries—and, in effect, social media intermediaries as well.[144]

This amendment creates an obligation on intermediaries for expedited resolution of certain categories of content[145] and acknowledgement of user complaints within 24 hours of receipt.[146] It also establishes an external GAC framework through which users can contest a social media platform's content moderation decisions.[147] The October 2022 amendment to the intermediary guidelines further states that intermediaries must make what it describes as "reasonable efforts" to make users not "host, display, upload, modify, publish, transmit, store, update or share" a broad list of "prohibited content".[148]

This appears to go beyond the traditional notice and takedown content moderation regime which has governed social media platforms. Specifically, the vagueness of "prohibited content" can end up imposing a general monitoring obligation on social media platforms, which shifts the burden on platforms from actual knowledge to a constructive knowledge standard.[149] Among other things, the list of prohibited content under this notice and action regime includes misinformation and content that promotes enmity between different groups on the grounds of religion or caste with an intent to incite violence.[150, 151]

143 Aashish Aryan and Dia Rekhi, 'Govt Notifies Changes to IT Rules 2021, Grievance Panel to Hear Complaints' *The Economic Times* (29 October 2022) <https://economictimes.indiatimes.com/tech/technology/govt-notifies-changes-to-it-rules-2021-grievance-panel-to-hear-complaints/articleshow/95152142.cms>.

144 Vasudev Devadasan, 'Report on Intermediary Liability in India (December 2022)' (2023) Centre for Communication Governance.

145 Intermediary Guidelines 2021, Rule 3(2)(i) mandates certain categories of content to be removed within 72 hours of reporting. These include content related to child sexual abuse material, NCII, obsenity, impersonation, misinformation, and "threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence, or prevents investigation of any offence, or is insulting other nation" among others.

146 Intermediary Guidelines 2021, Rule 3(2)(i).

147 Ibid.

148 Intermediary Guidelines 2021, Rule 3(1)(b).

149 Vasudev Devadasan, 'Report on Intermediary Liability in India (December 2022)' (2023) Centre for Communication Governance.

150 PTI, 'New Intermediary Guidelines to Put More Obligations on Social Media Platforms to Act against Unlawful Content, Misinformation: Rajeev Chandrasekhar' *The Hindu* (29 October 2022) <https://www.thehindu.com/news/national/new-it-rules-to-put-more-obligations-on-social-media-platforms-to-act-against-unlawful-content-misinformation-rajeev-chandrasekhar/article66069010.ece>.

151 Intermediary Guidelines 2021, Rule 3(1).

Additionally, the October 2022 amendment introduces a new GAC framework to oversee the content moderation decisions of social media platforms. This framework will apply to any scenario where a user feels aggrieved by the content moderation decision of a social media intermediary's grievance officer. Such appeals can be filed with the GAC within 30 days from the date of receipt of the order from the social media platform.[152] The October 2022 amendment allows users to appeal against a platform's decision to moderate/remove their content as well as a platform's decision to host another user's content.[153]

Any GAC which is registered under the framework must comprise one chairperson and two members who are appointed by India's central government. One member of a GAC will be ex-officio and the other two will be independent members.[154] They will be required to attempt to address appeals within thirty days from the filing of an appeal via the mode of online dispute resolution.[155] They also have the option of seeking the assistance of any person who has expertise in the concerned subject.[156] To retain safe harbour protection, social media intermediaries will be required to comply with any decision of GACs, and are also required to publish transparency reports on their websites which document compliance with the framework.[157] This requirement for compliance with the GAC framework is essential to highlight since it represents another institutional requirement that social media platforms must adhere to avail the benefits of safe harbour protection.

The above GAC framework has been criticised by several scholars and field experts.[158] These include issues with the independence of GAC members from the government. This is essential to highlight since content disputes before the GAC could involve contestations between social media platforms and the government. This lack of independence could be inconsistent with rule of law principles.

152 October 2022 Amendment, addition of r. 3A(2).

153 Vasudev Devadasan, 'Report on Intermediary Liability in India (December 2022)' (2023) Centre for Communication Governance.

154 Intermediary Guidelines 2021, Rule 3A(2).

155 Intermediary Guidelines 2021, Rule 3A(4).

156 Intermediary Guidelines 2021, Rule 3A(5).

157 Intermediary Guidelines 2021, Rule 4(1)(d).

158 Ibid; Prateek Waghre and Tejasi Panjiar, 'The Next Step in Government-Led Internet Censorship Without Transparency Is Here' *The Wire* (18 March 2023) <https://thewire.in/rights/government-censorship-transparency-gac>; Meri Baghdasaryan, 'New Amendments to Intermediary Rules Threaten Free Speech in India' (*Electronic Frontier Foundation*, 21 July 2022) <https://www.eff.org/deeplinks/2022/07/new-amendments-intermediary-rules-threaten-free-speech-india>.

Second, because the GAC's current process does not provide citizens with essential conditions to exercise their right to be heard as no process is mentioned for citizens to contest GAC decisions before constitutional courts like High Courts or the Indian Supreme Court.[159]

Moreover, the list of prohibited content that the GAC must ensure remains off platforms is broader than the list of constitutionally permissible restrictions on people's right to freedom of speech and expression. Some of these terms, like "misinformation", are vague and leave room for arbitrary implementation. Thus the framework may not be consistent with people's fundamental rights under India's constitution.[160]

Finally, the GAC framework has been critiqued as being inconsistent with the legislative mandate of the Indian Information Technology Act and could be considered a legally excessive measure which has been executed via delegated legislation.[161] This is because the statute does not envision any condition in which the Government can set up a quasi-judicial body to oversee intermediaries' content moderation practices.[162]

The government notified three GACs in early 2023.[163] each dealing with specific types of content and being led by MHA, MIB and MeitY.[164] The functioning of these GACs has come under criticism for lack of transparency in its functioning, the absence of reasoned orders in many instances and the lack of public information on the distribution of cases between different committees.[165]

159 However, there is no bar for appealing GAC decisions under writ to the High Courts or the Supreme Court.

160 Tejasi Panjiar and Prateek Waghre, 'A Public Brief on the IT Amendment Rules, 2022 a.k.a "How the Government Is Trying to Moderate Online Speech"' (*Internet Freedom Foundation*, 10 November 2022) <https://internetfreedom.in/public-brief-on-the-it-amendment-rules-2022/>; Vasudev Devadasan, 'Report on Intermediary Liability in India (December 2022)' (2023) Centre for Communication Governance.

161 Tejasi Panjiar and Prateek Waghre, 'A Public Brief on the IT Amendment Rules, 2022 a.k.a "How the Government Is Trying to Moderate Online Speech"' *Internet Freedom Foundation* (10 November 2022) <https://internetfreedom.in/public-brief-on-the-it-amendment-rules-2022/>.

162 Vasudev Devadasan, 'Report on Intermediary Liability in India (December 2022)' (2023) Centre for Communication Governance.

163 Ministry of Electronics & IT,'Three Grievance Appellate Committees (GACs) Notified on the recently amended "IT Rules 2021"'(*PIB* 28 January 2023) <https://pib.gov.in/PressReleasePage.aspx?PRID=1894258#:~:text=The%20Centre%20today%20established%20three,effect%20has%20been%20published%20today.>.

164 Suraksha P, 'Info Sought on GAC Orders on Pleas against Social Media Companies' *The Economic Times* (20 April 2023) <https://economictimes.indiatimes.com/tech/technology/info-sought-on-gac-orders-on-pleas-against-social-media-companies/articleshow/99620696.cms>.

165 Tejasi Panjiar and Prateek Waghre, 'MeitY's Response to Our RTI Requests on GAC: Delayed, Denied, Deficient.' (*Internet Freedom Foundation*, 19 May 2023) <https://internetfreedom.in/gac-rti-response/>.

3.3.6 Transparency Mandate for Social Media Platforms

The government has introduced provisions within the Intermediary Guidelines 2021 which seek to regulate the domestic operations of social media platforms.

One such regulatory measure relates to platform transparency. Rule 4(1)(d) of the Intermediary Guidelines 2021 requires SSMIs to publish monthly compliance reports. The requirement to publish monthly compliance reports is only applicable to how platforms respond to content-related complaints that they have received from users; and statistics on the number of posts/links which have been disabled from public access as a result of proactive content moderation practices.

The government has clarified that such data can be classified as per the subject under which the complaint is received (for instance copyright).[166] In the case of voluntary takedowns, the intermediary is required to mention the number and type of content it has removed, or to which it has disabled access. Any other relevant information, such as the usage of automated tools employed for filtering, may be highlighted in the reports. However, according to research, while such reports are extremely useful, in their current form, they do not enable meaningful transparency.[167] Therefore, as platforms employ different metrics, definitions and rules for the categorisation of complaints, it limits inter-platform comparison.[168]

What is perhaps most relevant in the legal construction of this platform transparency mandate is that this transparency does not extend to platforms' response to legal content takedown requests, which emanate from either court orders or Government orders. Similarly, there is no transparency mandate imposed on social media platforms to disclose how they respond to government/LEA for user information (and related materials) for government investigation and enforcement purposes. Thus, it is notable that Indian laws selectively institute transparency requirements on social media platforms.

166 MeitY (n 104). [FAQ 20].

167 Aleksandra Urman and Mykola Makhortykh, 'How Transparent Are Transparency Reports? Comparative Analysis of Transparency Reporting across Online Platforms' (2023) 47 Telecommunications Policy 102477 <https://www.sciencedirect.com/science/article/pii/S0308596122001793>; Christopher Parsons, 'The (In)Effectiveness of Voluntarily Produced Transparency Reports' (2019) 58 Business & Society 103 <http://journals.sagepub.com/doi/10.1177/0007650317717957>.

168 Daphne Keller, 'Some Practical Postulates About Platform Data' (18 May 2023) <https://cyberlaw.stanford.edu/blog/2023/05/some-practical-postulates-about-platform-data>.

3.3.7 Dilution of Anonymity and Voluntary Verification of Social Media Platform Users

Recent trends in internet governance and social media regulation confirm the government's overall concerns with online anonymity. Rule 4(7) of the Intermediary Guidelines 2021 for example requires SSMIs to deploy features/avenues which enable registered Indian users to voluntarily verify their accounts.[169] Among other things, the provision specifies this could be executed via people's registered mobile numbers. The provision goes on to state that when a user's identity has been verified by the social media platform they must be assigned with a publicly visible mark (e.g. a blue/golden tick) establishing the same. The rationale behind introducing this provision was "the growing phenomena of misinformation, bots, criminality, and user harms in general".[170]

This provision is tangible evidence that the Indian government views online anonymity, especially on social media, as a challenge in the context of public order and security. These concerns are further demonstrated by various Parliamentary Committee reports on matters relating to data protection.[171] India's Joint Parliamentary Committee's report on Data Protection (December 2021) identifies the publication of information on platforms through fake accounts or accounts impersonating other people or accounts using fake names as a key concern.[172] To limit amplification through bots, it recommends (i) setting up a statutory regulatory authority to regulate online content and (ii) mandatory verification of end-user accounts through government-issued identification. It also recommends that platforms should be held liable for content posted by unverified accounts.

Koo,[173] an Indian social media platform operator, is the first platform to comply with this user verification requirement. Koo allows its users to verify themselves using India's national biometric identification system– Aadhaar.[174]

169 Intermediary Guidelines Rules 2021, Rule 4(7).

170 MeitY, 'Mandatory Verification of Social Media Accounts' (*PIB*, 5 August 2022) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1848736>.

171 Joint Committee on the Personal Data Protection Bill 2019, *Report of the Joint Committee on the Personal Data Protection Bill 2019* (Lok Sabha 2021) para 1.7.1. <http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf>.

172 Ibid.

173 Koo is an Indian microblogging and social networking platform modelled on Twitter.

174 Sarvesh Mathi, 'Koo Enables Aadhaar-Based Self-Verification for All Users' (*MediaNama*, 7 April 2022) <https://www.medianama.com/2022/04/223-koo-self-verification/>.

3.3.8 Automated Content Filtering and Proactive Monitoring

Another key trend in India's intermediary governance framework is the trend towards proactive content oversight obligations on social media platforms. The Intermediary Guidelines 2021 require SSMIs to "endeavour" to deploy technology-based measures (i.e. automated content filtering tools) to proactively identify and remove content which depicts:[175]

- actual or simulated rape,
- explicit or implicit child sexual abuse materials,
- or any content which is identical to unlawful content which has previously been removed under Rule 3(1)(d).

The word 'endeavour' highlighted above conveys that significant social media platforms must deploy automated content filtering tools on a best-efforts basis. However, at the same time, the provision states that such filtering tools must be implemented in a manner which is proportionate to citizens' fundamental rights of freedom of speech and expression, and the right to privacy.[176]

The provision also states that when a platform deploys content filtering tools, social media platforms must mandatorily deploy adequate human oversight and periodic review in the functioning of such systems.[177] The provision further clarifies that such review of automated content filtering tools must involve an assessment of the "accuracy and fairness of such tools, propensity for bias and discrimination, and the impact on user privacy and security."[178]

The Indian law's trend towards general monitoring obligations for social media platforms across broad categories of online content is interesting. It is, firstly, a departure from the neutral and passive intermediary liability/safe harbour protection regime which has traditionally subsisted both within India and in more mature internet governance

175 Intermediary Guidelines Rules 2021, Rule 4(4).
176 Intermediary Guidelines 2021, Rule 4(4) 1st Proviso.
177 Intermediary Guidelines 2021, Rule 4(4) 2nd Proviso.
178 Intermediary Guidelines 2021, Rule 4(4) 3rd Proviso.

jurisdictions like Europe—which has explicitly barred general monitoring obligations for internet intermediaries in the past.[179] Moreover, it is also inconsistent with jurisprudence within Indian courts which have previously viewed such requirements on internet intermediaries rather unfavourably.[180]

3.3.9 Legal Challenges Against India's Social Media Regulatory Framework

As detailed in prior sections the Intermediary Guidelines 2021 is the key legal framework which governs India's social media landscape. Readers must be mindful that these regulations—which have been brought into force via delegated legislation by India's executive rather than through a Parliamentary enactment—have been legally challenged across multiple High Courts.[181]

As per researchers,[182] these challenges include nine distinct challenges against Part II of the Intermediary Guidelines 2021, which prescribes the social media intermediary liability and diligence framework.[183] Additionally the Digital Media Ethics Code under Part III of the Rules which, among other forms of curated over-the-top services, also governs news aggregation features of social media platforms has been challenged across Indian High Courts.[184]

179 Directive 2000/31/EC of 8 June 2000 on electronic commerce, Art. 15.

180 *UTV Software Communications Ltd v 1337x* CS (Comm) 724 of 2017 (High Court of Delhi, 10 April 2019); *Kent RO Systems Ltd v Amit Kotak* 2017 SCC OnLine Del 7201; *Myspace Inc v Super Cassettes Industries Ltd* 2016 SCC OnLine Del 6382; *Dept of Electronics and Information Technology v Star India Pvt Ltd* FAO (OS) 57 of 2015 (High Court of Delhi, 29 July 2016).

181 'Table summarising challenges to Intermediary Guidelines, 2021 pending before High Courts,' *Internet Freedom Foundation* <https://docs.google.com/document/d/1kmq-AlRO1XpPaThvesl5xQq2nVkZv6UdmaKFAJ8AMTk/edit>.

182 Vasudev Devadasan, 'Report on Intermediary Liability in India (December 2022)' (2023) Centre for Communication Governance.

183 *LiveLaw Media Pvt Ltd v Union of India* WP (C) 6272 of 2021 (High Court of Kerala); *Sanjay Kumar Singh v Union of India* WP (C) 3483 of 2021 (High Court of Delhi); *Uday Bedi v Union of India* WP (C) 6844 of 2021 (High Court of Delhi); *Praveen Arimbrathodiyil v Union of India* WP (C) 9647 of 2021 (High Court of Kerala); *TM Krishna v Union of India* WP (C) 12515 of 2021 (High Court of Madras); *Sayanti Sengupta v Union of India* WPA (P) 153 of 2021 (High Court of Calcutta); *Nikhil Wagle v Union of India* PIL (L) 14204 of 2021 (High Court of Bombay); *Facebook Inc v Union of India* WP (C) 7281 of 2021 (High Court of Delhi); *WhatsApp LLC v Union of India* WP (C) 7284 of 2021 (High Court of Delhi).

184 See Vasudev Devadasan, 'Report on Intermediary Liability in India (December 2022)' (2023) Centre for Communication Governance. The list of cases is as follows: "*Press Trust of India Limited v Union of India* WP (C) 6188 of 2021 (High Court of Delhi); *Foundation for Independent Journalists v Union of India* WP (C) 3125 of 2021 (High Court of Delhi); *The Leaflet (Nineteen One Media Pvt Ltd) v Union of India* WPL 14172 of 2021 (High Court of Bombay); *Quint Digital Media Ltd v Union of India* WP (C) 3659 of 2021 (High Court of Delhi); *Pravda Media Foundation v Union of India* WP (C) 5973 of 2021 (High Court of Delhi); *News Broadcasters Association v Ministry of Electronics and Information Technology* WP (C) 13675 of 2021 (High Court of Kerala); *Truth Pro Foundation of India v Union of India* WP (C) 6941 of 2021 (High Court of Karnataka); *Digital News Publishers Association v Union of India* WP (C) 13055 of 2021 (High Court of Madras); *Nikhil Wagle v Union of India* PIL (L) 14204 of 2021 (High Court of Bombay); *Indian Broadcasting & Digital Foundation v Ministry of Electronics and Information Technology* WP 25619 of 2021 (High Court of Madras)".

Due to the numerous legal challenges across different High Courts, the Indian government has requested the Supreme Court to consolidate and hear all legal challenges against the intermediary guidelines and hear them as a single matter.[185] While the Supreme Court has not made a ruling on this request, it has directed High Courts to not hear any challenges against the Intermediary Guidelines 2021.[186]

Given this procedural context, it is still useful to consider the primary grounds on which the legality of the intermediary guidelines has been challenged. The challenges range from violations of fundamental rights of speech and privacy, right to practise any profession, challenges on the Rule's arbitrary nature, etc.[187]

Specific challenges have been made to technical provisions, such as the liability and implication of non-compliance with due diligence obligations for SMIs. Mr T. M. Krishna, a prominent vocalist, has challenged the entirety of Intermediary Guidelines in the Madras High Court.[188] His petition argued that the Intermediary Guidelines restrict his fundamental rights to privacy, expression and profession. The Madras High Court recognised that there is "substantial basis to the petitioners" assertion that Article 19 (1) (a) of the Constitution may be infringed in how the Rules may be coercively applied to intermediaries."[189]

Meta-owned WhatsApp has challenged Rule 4(2) of Part II of the Intermediary Guidelines 2021. The rule imposes a due diligence obligation to identify the 'first originator' of a message (i.e. the traceability mandate) .[190] WhatsApp's challenge pertains to the security and privacy concerns arising from attempts to weaken encryption.[191] Google has also

185 Sohini Chowdhury, 'Intermediary Guidelines 2021 : Supreme Court To Hear Centre's Plea To Stay Interim Orders Passed By High Courts On July 27' (Live Law, 20 July 2022) accessed January 2023.

186 *Skand Bajpai v Union of India* WP (C) 799 of 2020 (Supreme Court of India, 9 May 2022),

187 Krishnesh Bapat, Anandita Mishra, and Tanmay Singh, 'May Threaten "Independence of Media": Madras HC on Intermediary Guidelines' (*Internet Freedom Foundation*, 17 September 2021) <https://internetfreedom.in/madras-high-court-affirms-the-pan-india-stay-on-rule-9-3-of-the-it-rules-and-provides-relief-on-part-ii/>.

188 The Wire Staff, 'Musician T.M. Krishna Moves Madras High Court Against IT Rules' *The Wire* (New Delhi, 10 June 2021) <https://thewire.in/law/musician-t-m-krishna-moves-madras-high-court-against-it-rules>.

189 'May Threaten "Independence of Media": Madras HC on Intermediary Guidelines' (*Internet Freedom Foundation*, 17 September 2021) <https://internetfreedom.in/madras-high-court-affirms-the-pan-india-stay-on-rule-9-3-of-the-it-rules-and-provides-relief-on-part-ii/>.

190 'Delhi HC Asks Centre to Respond to Pleas by FB, WhatsApp Challenging New Intermediary Guidelines' (*India Today*) <https://www.indiatoday.in/law/story/delhi-hc-asks-centre-respond-pleas-fb-whatsapp-it-rules-1846088-2021-08-27>.

191 Joseph Menn, 'WhatsApp sues Indian government over new privacy rules' *Reuters* (26 May 2021) <https://www.reuters.com/world/india/exclusive-whatsapp-sues-india-govt-says-new-media-rules-mean-end-privacy-sources-2021-05-26/>.

approached the Delhi High Court, challenging its characterisation as a social media intermediary under the Intermediary Guidelines.[192]

Other petitions which challenged the legality of Part III of the Rules i.e. the Digital Media Ethics Code, claim that the rules are arbitrary, vague, impose unreasonable restrictions on the freedom of the press and suffer from excessive delegation of powers as they have established a non-judicial adjudicatory process.[193]

Petitions also challenged Rule 9(1) and (3) of the Intermediary Guidelines, which require digital media and OTT platforms to adhere to the Code of Ethics and enable anyone to raise a complaint to the three-tier grievance redressal mechanism. The top of the three-tier redressal mechanism is the executive-led Inter-Departmental Committee.

The Madras[194] and Bombay High Courts[195] have stayed the implementation of Rule 9(1) and (3) of the Intermediary Guidelines. The order issued by the Chief Justice of Madras High Court stated that the government-led redressal mechanism "may rob the media of its independence and the fourth pillar, so to say, of democracy may not at all be there."[196]

The Kerala High Court has also stayed the implementation of the aforementioned provisions. It has further directed that the Union Government cannot take coercive action for non-compliance with Part III of the Intermediary Guidelines 2021.[197] At the time of writing, the Union Government has subsequently challenged the stay orders at the Supreme Court.[198]

192 'Google Claims New Intermediary Guidelines Not Applicable to Its Search Engine: HC Seeks Centre's Stand' (The New Indian Express) <https://www.newindianexpress.com/nation/2021/jun/02/google-claims-new-it-rules-not-applicable-to-its-search-engine-hc-seeks-centres-stand-2310739.html>.

193 'Kerala High Court Stays Intermediary Guidelines' (Supreme Court Observer) <https://www.scobserver.in/journal/kerala-high-court-stays-it-rules/>.

194 'Madras High Court stays certain sub-clauses of new Intermediary Guidelines that may 'rob media's independence',' Livemint (16 September 2021) <https://www.livemint.com/news/india/madras-high-court-stays-certain-sub-clauses-of-new-it-rules-that-may-rob-media-s-independence-11631803788378.html>.

195 Mustafa Shaikh, Bombay High Court stays two provisions of Intermediary Guidelines 2021, *India Today*, (14 August 2021) <https://www.indiatoday.in/india/story/bombay-hc-bench-chief-justice-information-technology-it-rules-stay-clauses-rule9-1840891-2021-08-14>.

196 *Digital News Publishers Association v. Union of India*, W.P.Nos.13055 and 12515 of 2021 <https://drive.google.com/file/d/1uaUYSD-0RZlO7AixvndPnwEGraq_4fNk/view>.

197 Tanmay Singh, 'Kerala HC Grants a Stay of the Operation of Part III of the Intermediaries Rules, 2021 to LiveLaw' (*Internet Freedom Foundation*, 10 March 2021) <https://internetfreedom.in/kerala-hc-grants-a-stay-of-the-operation-of-part-iii-of-the-intermediaries-rules-2021-to-livelaw/>.

198 The Wire Staff, 'Setback for Centre, SC Refuses to Stay HC Hearings on IT Rules' (*The Wire*, July, 2021) <https://thewire.in/law/it-rules-supreme-court-high-court-proceedings-stay-refuse>.

3.4 India's Administrative Landscape

India's Ministry of Electronics and Information Technology (MeitY) and the Ministry of Home Affairs (MHA) play integral roles in both cybersecurity and social media regulation. For cybersecurity, these ministries operate in tandem with specialised bodies, namely the Office of the National Cyber Security Coordinator (NCSC), the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Computer Emergency Response Team of India (CERT-In).

For social media, the Ministry of Information and Broadcasting (MIB)– specifically its new media wing– is an important institution since it is responsible for the governance/ regulation of digital media.

MeitY, MIB, and MHA are thus the key administrative institutions responsible for India's social media regulatory landscape. However, there have been some challenges of jurisdictional overlap and ambiguity. We have previously observed efforts by the Telecom Regulatory Authority of India (TRAI) to contemplate regulations which would bring certain social media apps within the jurisdiction of India's telecom authorities.[199] Until recently, MIB had negligible relevance for social media regulation. However, a 2021 amendment to a set of executive rules[200] designated MIB as the nodal Ministry for digital/online media and news and current affairs content on online platforms.[201]

This amendment set the stage for MIB to regulate citizen engagement with news in social media environments. Keeping this background in mind let us consider how each of these institutions regulate India's social media landscape.

199 Consultation Paper on Regulatory Framework for Over-The-Top (OTT) Communication Services, Telecom Regulatory Authority of India, Government of India, (November 2018) <https://trai.gov.in/consultation-paper-regulatory-framework-over-top-ott-communication-services?page=6>.

200 The Government of India (Allocation of Business) Rules, 1961.

201 Vikram Jeet Singh and Kalindi Bhatia, Online News Portals, OTT Platforms Brought Under Purview Of MIB, Mondaq (April 2021) <https://www.mondaq.com/india/broadcasting-film-tv-radio/1055594/online-news-portals-ott-platforms-brought-under-purview-of-mib>.

1. Ministry of Home Affairs (MHA)

The primary division under the MHA is the Cyber and Information Security (C&IS) Division. The C&IS Division steers India's (a) Cyber Crime Wing; and (b) Information Security Wing. It anchors the Indian Cyber Crime Coordination Centre (I4C) and the National Cyber Crime Reporting Portal. It also coordinates with other agencies in administering India's lawful interception framework, internet suspension framework, and the blocking of websites, apps, and online content.[202]

The MHA oversees social media through a cyber crime and information security lens. It issues occasional advisories and typically engages in informal oversight of social media on matters of security, radicalisation, terrorist recruitment[203] and online extremist content.[204] MHA has constituted various cyberspace monitoring measures such as the cybercrime portal.[205]

One initiative was proposed to authorise a multi-agency war room to analyse threats on social media 24*7.[206] Another initiative appoints the Indian Cyber Crime Coordination Centre (I4C) as the primary point of reference for citizen volunteers to report unlawful and "anti-national activities" online by other citizens.[207] This pilot programme is planned to begin its operations in different parts of the country like Tripura, Jammu and Kashmir.[208]

202 Ministry of Home Affairs, 'Expression of Interest for Selection of Systems Integrators for Implementing Entity Extraction, Visualization & Analytics (EVA) System (29 October 2017) 14 <https://www.mha.gov.in/sites/default/files/EOIEVA_29092017.pdf>; Vrinda Bhandari, 'Facial Recognition: Why We Should Worry About the Use of Big Tech for Law Enforcement', The Future of Democracy in the Shadow of Big and Emerging Tech (Centre for Communication Governance, National Law University Delhi 2020) <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/thefuture-of-democracy-in-the-shadow-of-big-and-emerging-tech-ccg-248.pdf>.

203 'India concerned over use of social media for recruitment of terrorists: US', *The New Indian Express* (2nd November 2019) <https://www.newindianexpress.com/world/2019/nov/02/india-concerned-over-use-of-social-media-for-recruitment-of-terrorists-us-2056154.html>.

204 Shruti Pandalai, 'ISIS in India: The Writing on the (Facebook) Wall,' *The Diplomat* (6th May 2016) <https://thediplomat.com/2016/05/isis-in-india-the-writing-on-the-facebook-wall/>.

205 Social Media Crimes, Cyber Crime Cell, Delhi Police < http://www.cybercelldelhi.in/socialmediacrimes.html>.

206 Abhishek Bhalla, 'India wants 24x7 online war room to tackle cyber threat from ISIS,' *India Today* (24 December 2015) <https://www.indiatoday.in/mail-today/story/government-plans-social-media-scanning-centre-to-take-on-isis-278697-2015-12-24>.

207 Ashish Aryan, 'Govt looks for cyber volunteers to report 'anti-national activities,' *The Indian Express* (9th February 2021) <https://indianexpress.com/article/india/anti-national-activities-cyber-volunteers-uapa-7180444/>.

208 Ibid.

2. Ministry of Electronics and Information Technology (MeitY)

MeitY is the nodal agency responsible for policy matters relating to information technology, electronics and the internet– barring issues relating to the licensing of telecom/internet service providers. MeitY has a discrete group of officials dedicated to "Cyber Laws" and is responsible for administering the IT Act. As a result, it is the nodal authority which administers India's intermediary liability and social media intermediary governance framework. As per Part II of Intermediary Guidelines, MeitY is the nodal authority responsible for intermediary regulation and this enables it to oversee platforms qualifying as SMIs and SSMIs.

3. MIB

Part III of the Intermediary Guidelines 2021, i.e. the Digital Media Ethics Code, assigns MIB as the nodal administrative authority for digital media, online news and current affairs content, and online news aggregation. Under Part III, MIB can appoint a ministerial official as the chairperson to head an inter-departmental committee.[209] This committee has powers to hear complaints of alleged violations of any applicable code of ethics relevant to digital media.[210] This committee has the power to warn, censure, admonish, reprimand violators and/or seek apologies from entities that violate the Digital Media Ethics Code.[211] MIB's authorised officer/chairperson, *inter alia*, has the authority to make recommendations to the top bureaucratic official (Secretary) at MIB to issue interim emergency orders to block public access to online information.[212]

4. Computer Emergency Response Team of India (CERT-In)

CERT-In is a statutory organisation (under MeitY) which functions as India's nodal cyber incident response agency under the IT Act. CERT-In is largely concerned with ecosystem-wide resilience and security. This includes threat prevention, detection and discovery, cyber incident response, information sharing, knowledge dissemination and circulation of best practices.

209 This Inter-departmental Committee consists of members from India's Ministry of Women and Child Development, Ministry of Law and Justice, MHA, MeitY, the Ministry of External Affairs, Ministry of Defence and CERT-In.

210 Intermediary Guidelines Rules 2021, Rule 14(2).

211 Intermediary Guidelines Rules 2021, Rule 14(5).

212 Intermediary Guidelines Rules 2021, Rule 16(4).

3.5 Regulating the Online Information Ecosystem

In the previous sections, we provided an overview of the overarching legal framework which governs social media platforms as well as the cybersecurity and ICT regulations applicable to such platforms.

In this section, we outline the regulatory mechanisms and other channels that can be mobilised by the state to regulate the flow of information in the digital realm, and their impact on the governance of social media platforms and their users. These become particularly significant as social media platforms are a critical arena for public debate and information sharing as well as peer-to-peer communication. It must be noted here that tighter regulation of intermediary behaviour also enables the State to maintain its primacy in determining what speech is allowed to exist online.

In India, the following mechanisms are widely used to regulate the online information ecosystem: (a) criminalisation of online speech (b) law enforcement access to citizen information; (c) internet suspension; (d) blocking public access to online content on social media; (e) informal channels of communication between state and social media platforms; and (f) statutory fact-checking bodies.

3.5.1 Criminalisation of Online Speech

The Constitution of India protects freedom of speech and expression as a fundamental right.[213] Within the ambit of this right, citizens enjoy a right to receive and impart information.[214] This right is subject to reasonable restrictions.[215]

In the exercise of that power to restrict speech under certain circumstances, India has several penal laws which criminalise certain types of speech, like sedition, defamation, obscenity and hate speech.[216] Most of these criminal provisions have colonial roots, and

213 Constitution of India 1949, Article 19(1)(a).

214 *Union of India v. Assn. for Democratic Reforms*, (2002) 5 SCC 294.

215 Constitution of India 1949, Article 19(2).

216 According to Bhatia, section 295A (insulting religious feelings) and section 153A (causing disharmony or enmity between different castes and communities) of the Indian Penal Code, section 123 of the Representation of the People Act (restricting certain kinds of speech during elections), and section 3(1)(x) of the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act can be viewed as hate speech legislation in India Gautam Bhatia, 'Offend, shock, or disturb: Free speech under the Indian Constitution' (Oxford University Press, 2016).

have been critiqued in scholarly works.[217] Their constitutionality continues to be challenged within Indian Courts.[218, 219]

Against this backdrop of the criminalisation of speech under legacy criminal laws, readers must also factor in the speed, scale, and dynamism of online distribution and virality. These factors make speech issues over the internet, and specifically social media, pertinent.

India's IT Act also has multiple provisions[220] which restrict and criminalise harmful online speech and are often implemented to proscribe citizens' speech over social media.

- **Section 66A of the IT Act**

A notable case is section 66A of the IT Act, which was ultimately deemed unconstitutional by the Indian Supreme Court.[221] This section criminalised a range of vague and ambiguous communications for being -"offensive" in nature. In practice, it was used to arrest people for ordinarily permissible speech like political satire and criticism of political leaders.[222]

---

217 Elizabeth Kolsky, 'Codification and the Rule of Colonial Difference: Criminal Procedure in British India' (2005) 23 Law and History Review 631 <https://www.jstor.org/stable/30042900>; Maryam Kanna, 'Furthering Decolonization: Judicial Review of Colonial Criminal Laws Notes' (2020) 70 Duke Law Journal 411 <https://heinonline.org/HOL/P?h=hein.journals/duklr70&i=410>.

218 'In a Petition Filed by the Journalist Union of Assam, Supreme Court Directs Governments to Not Use Section 124A' (*Internet Freedom Foundation*, 11 May 2022) <https://internetfreedom.in/jua-sc-sedition/>.

219 Gautam Bhatia, 'A Sullivan for the Times: The Madras High Court on the Freedom of Speech and Criminal Defamation' (*Indian Constitutional Law and Philosophy*, 16 May 2020) <https://indconlawphil.wordpress.com/2020/05/16/a-sullivan-for-the-times-the-madras-high-court-on-the-freedom-of-speech-and-criminal-defamation/>.

220 Section 67 of the IT Act criminalises transmitting or publishing obscene content "which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons" while section 67A deals with publishing or transmitting material that is sexually explicit. These sections have been criticised for curtailing freedom of expression of individuals based on paternalistic notions of morality.

Section 66E on the other hand takes into account consent of individuals and criminalises the act of "capturing, publishing or transmitting the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person".

Section 67B criminalises punishes publishing, transmitting or facilitating child pornography.

221 Section 66A criminalised sending information through a computer resource or communication device:(a) information that is "grossly offensive or has menacing character"; (b) information known to be false but shared with the aim of causing "annoyance, inconvenience, danger , obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently"; (c)any email or message for causing annoyance or inconvenience or to deceive or mislead about the origin of such messages.

222 See Samiksha Bhardwaj, 'Section 66A: Six Cases That Sparked Debate' (*Mint*, 24 March 2015) <https://www.livemint.com/Politics/xnoW0mizd6RYbuBPY2WDnM/Six-cases-where-the-draconian-Section-66A-was-applied.html>;FP Staff, 'Arrest of Palghar Girls over Facebook Post Is Abuse of Power: Centre Tells SC' *Firstpost* (10 December 2014) <https://www.firstpost.com/india/arrest-mumbai-girls-facebook-post-abuse-power-centre-1842579.html>; HT Correspondent, 'JU Prof, Arrested for Forwarding CM Banerjee's Cartoon, Discharged from Case' *Hindustan Times* (20 January 2023) <https://www.hindustantimes.com/cities/kolkata-news/ju-prof-arrested-for-forwarding-mamata-cartoon-11-years-ago-discharged-by-court-101674198013858.html>.Prakash Kamat, 'Goan Shipbuilding Professional Faces Jail for Anti-Modi Comment on Social Media' *The Hindu* (23 May 2014) <https://www.thehindu.com/news/national/other-states/goan-shipbuilding-professional-faces-jail-for-antimodi-comment-on-social-media/article6041143.ece>.

In 2015, India's Supreme Court determined that this section was unconstitutional in the landmark *Shreya Singhal* case.[223] The Court held that the section was vague and did not define the criminal offence with precision. This meant that (a) ordinary people could not distinguish what fell within the ambit of the offence and what conduct was permissible; (b) the section created risks of arbitrary and discriminatory law enforcement practices. Due to the use of subjective terms, the Supreme Court finally held that section 66A created a chilling effect, since it, "arbitrarily, excessively and disproportionately invades the right of free speech and upsets the balance between such right and the reasonable restrictions that may be imposed on such right".[224]

- **The Indian Penal Code (IPC)**

Apart from the IT Act, sections of the IPC have also been used routinely to criminalise online content/speech. The 2021 annual report of the National Crime Records Bureau (NCRB)[225] recorded 688 cases registered under "cyber blackmailing/threatening",[226] 179 cases registered for "fake news on social media",[227] 31 cases under "defamation/morphing",[228] and 1154 cases under "cyberstalking/bullying of women and children".[229]

It is also interesting to note that the NCRB cites[230] "Inciting Hate against Country",[231] "Terrorist activities",[232] and "Political motives"[233] as motives for cybercrime among 20 others (like fraud, personal revenge and terrorist activities).

Other provisions of the IPC that are frequently invoked in criminalising online speech are "promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc";[234] "imputations, assertions prejudicial to national integration";[235]

223 *Shreya Singhal v Union of India*, Writ Petition No. 167 of 2012.
224 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [82].
225 National Crime Records Bureau, 'Crime in India 2021' (Ministry of Home Affairs 2022), table 9A.2.
226 The Indian Penal Code, 1860, ss. 506, 503 and 384.
227 IPC 1860, s 505.
228 IPC 1860, s 469; The Indecent Representation of Women (Prohibition) Act, 1986.
229 IPC 1860, s 354D.
230 National Crime Records Bureau, 'Crime in India 2021' (Ministry of Home Affairs 2022), table 9A.3.
231 As per the NCRB data, 31 cases of cybercrime had "inciting hate against country" as the motive.
232 As per the NCRB data, 9 cases of cybercrime had "Terrorist activities" as the motive.
233 As per the NCRB data, 309 cases of cybercrime had "political motives".
234 IPC 1860, s 153A.
235 IPC 1860, s 153B.

"obscenity";[236] "outraging religious feelings of a class of citizens";[237] "sedition",[238] etc. Between January 2010 and February 2021, as per a study conducted by Aricle 14, "152 persons across India have been charged with sedition for creating audios, photos or videos or for sharing content on social media."[239]

A 2019 case study helps demonstrate how criminal provisions are invoked arbitrarily to restrict political speech online. Three people were arrested under charges of criminal intimidation[240] and public mischief[241] for allegedly sharing "objectionable posts" relating to a State/Province level Chief Minister, which included sharing a fake wedding invite for the concerned official.[242] In a related incident, a New Delhi-based journalist was arrested on charges of defamation[243] and public mischief[244] for a post where a woman expressed her interest in marrying the same official.[245]

There is also evidence of wide interpretation of legacy or analogue laws to address speech on social media. For example, to regulate COVID-19 disinformation, Indian authorities arrested individuals under section 54 of the DMA 2005, which broadly criminalises the promotion of false claims and warnings that cause panic.[246]

---

236 IPC 1860, s 293.

237 IPC 1860, s 295A.

238 IPC 1860, s 124A.

239 See Mohit Rao, 'Karnataka Has More Sedition Cases Based On Social-Media Posts Than Any State. Most Are Illegal —' *Article 14* (13 July 2021) <https://article-14.com/post/karnataka-has-more-sedition-cases-based-on-social-media-posts-than-any-state-most-are-illegal-60ecf64da7945>; Dhirendra K Jha, 'Hindutva Groups Ordered UP Police To File Sedition Cases, And Yogi's Police Obeyed' *Article 14* (8 February 2022) <https://www.article-14.com/post/hindutva-groups-ordered-up-police-to-file-sedition-cases-and-yogi-s-police-obeyed--6201d68cc0bb7>.

240 IPC 1860, s 503.

241 IPC 1860, s 505.

242 Aditi Vatsa, 'Now, Yogi Govt Arrests Farmer & Village Head for Social Media Posts on "CM Wedding Video"' *ThePrint* (10 June 2019) <https://theprint.in/india/now-yogi-govt-arrests-farmer-village-head-for-social-media-posts-on-cm-wedding-video/248094/>;'Fifth Arrest over Yogi Posts, Two Arrested in Gorakhpur' *The Times of India* (11 June 2019) <https://timesofindia.indiatimes.com/city/varanasi/fifth-arrest-over-yogi-posts-two-arrested-in-gorakhpur/articleshow/69730989.cms>.

243 IPC 1860, s 500.

244 IPC 1860, s 505.

245 Apoorva Mandhani, 'UP Police Struggles to Justify Journo Prashant Kanojia Arrest for Yogi Tweet, Law Doesn't' *The Print* (9 June 2019) <https://theprint.in/india/up-police-struggles-to-justify-journalist-prashant-kanojias-arrest-for-yogi-tweet/247859>; Press Trust of India, 'Journalist Prashant Kanojia Arrested for "Objectionable" Social Media Post about Yogi Adityanath; Charged with Defamation, Sections of ITA' *Firstpost* (Lucknow, 9 June 2019) <https://www.firstpost.com/india/journalist-prashant-kanojia-arrested-for-objectionable-social-media-post-about-yogi-adityanath-charged-with-defamation-sections-of-ita-6780551.html>.

246 See HT Correspondent, 'Police Crack down on Covid-19 "Misinformation", Activists Concerned' *Hindustan Times* (New Delhi, 29 April 2020) <https://www.hindustantimes.com/india-news/about-500-cases-lodged-in-india-for-social-media-posts-on-covid-19/story-PBaxt7oNs9IdPNUCVRiUUM.html>; Subimal Bhattacharjee, "Fake news, that other pandemic," *The Economic Times* (18 March 2020) https://economictimes.indiatimes.com/blogs/et-commentary/fake-news-that-other-pandemic/>; "One year jail, fine for spreading fake news on coronavirus: Hyderabad Police," The New Indian Times (15 March 2020) <https://www.newindianexpress.com/cities/hyderabad/2020/mar/15/one-year-jail-fine-for-spreading-fake-news-on-coronavirus-hyderabad-police-2117007.html>.

3.5.2 Internet Suspension

While criminal laws can curb and control information dissemination at the individual level, internet suspensions can affect citizens across particular areas and regions. India's use of state-mandated internet shutdowns for security, and law and order purposes is well documented.[247] It has recorded the world's maximum number of internet shutdowns each year since 2018, with 106 recorded instances in 2021[248] and 84 times in 2022.[249] Shutdowns are often used by central and state governments as precautionary measures to prevent the spread of misinformation, prevent cheating in exams or maintain public order.[250]

- **Telegraph Act, 1885**

The Indian Telegraph Act 1885, provides the legal foundation for internet suspension by state and central governments in cases of "public emergency" or in the interest of "public safety".[251] The Telecom Rules were introduced in 2017 to lay down the procedural guidelines for such orders. The suspension rules provide a procedure through which the government can assign designated authorities the power to issue suspension orders at the central and state levels,[252] recording reasons for shutdown in the orders,[253] and the constitution[254] and working of a review committee.[255]

247 Jayant Pankaj, 'Mapping the Rising Internet Shutdowns in India Since 2016' *The Wire* (9 October 2022) <https://thewire.in/government/mapping-the-rising-internet-shutdowns-in-india-since-2016>.

248 *Access Now*, 'The Return of Digital Authoritarianism: Internet Shutdowns in 2021' (2022).

249 *Access Now*, 'Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022'(2023).

250 See Diksha Munjal, 'In India, Are Internet Shutdowns in Accordance with Law? Not Always' (Newslaundry, 29 October 2021) <https://www.newslaundry.com/2021/10/29/in-india-are-internet-shutdowns-in-accordance-with-law-not-always>; Jayant Pankaj, 'Mapping the Rising Internet Shutdowns in India since 2016' (*The Wire*, 9 October 2022) <https://thewire.in/government/mapping-the-rising-internet-shutdowns-in-india-since-2016>; Software Freedom Law Centre, 'IT Standing Committee's Report on Internet Shutdowns' (SFLC.in, 12 August 2021) <https://sflc.in/it-standing-committeesreport-internet-shutdowns>.

251 The Indian Telegraph Act, 1885, s 5(2) lays down that internet can be suspended by the state or the centre if it is necessary or expedient so to do in the interests of the internet as in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence for reasons to be recorded in writing.

252 The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, Rule 2(1) designates the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and Secretary to the State Government in-charge of the Home Department in the case of a State Government.

253 Telecom Rules 2017, Rule 2(2).

254 Telecom Rules 2017, Rule 2(5).

255 Telecom Rules 2017, Rule 2(6) states that the Review Committee shall meet within five working days of internet suspension order.

Additional procedural safeguards were read into the rules in the landmark *Anuradha Bhasin v. Union of India* case.[256] In it, the Supreme Court held that the internet is a medium for exercising fundamental rights, and therefore, restrictions on internet access must conform to the constitutional standards and stand the test of "proportionality".[257]

In effect, this meant that under certain circumstances the Government of India was constitutionally justified in suspending the public's access to the internet and other similar mediums. However, shutdown decisions must be necessary and proportionate, and this must be demonstrated through adherence to certain safeguards.

The Supreme Court held that internet suspension orders have to be made publicly available and subjected to judicial review, and periodic reviews of suspension orders must be conducted by the executive.[258] Consequently, the telecom suspension rules were amended to include fifteen days as the upper limit for an order to be in operation.[259]

- **Code of Criminal Procedure**

Prior to the Telecom Suspension Rules in 2017, section 144 of the Code of Criminal Procedure (CrPC) was widely used to order internet shutdowns by district administration authorities. Even today, several years after the introduction of the rules, the procedural safeguards under it are routinely flouted as states continue to pass internet shutdown orders under section 144 of the CrPC.[260] Additionally, the issuance of orders on vague and arbitrary grounds, such as "cheating in public examinations", has also come under scrutiny.[261]

256 *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

257 *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 [152].

258 Ibid [100; 129]; The Review Committee constituted under Rule 2(5) of the Suspension Rules must conduct a periodic review within seven working days of the previous review, in terms of the requirements under Rule 2(6).

259 'Temporary Suspension of Telecom Services (Amendment) Rules' (Department of Telecommunications 2020) <https://dot.gov.in/sites/default/files/2020_11_11%20PEPS%20AS.pdf>.

260 Munjal (n 1).

261 ANI, 'SC issues notice to MeitY on plea challenging internet shutdowns during competitive exams' (*The Economic Times*, 9 September 2022) <https://economictimes.indiatimes.com/news/india/sc-issues-notice-to-meity-on-plea-challenging-internet-shutdowns-during-competitive-exams/articleshow/94094259.cms?from=mdr>.

States also typically fail to comply with the Supreme Court's mandate on publishing orders.[262] Moreover, the Indian Government does not maintain a central database of internet shutdowns ordered by the State Governments.[263] Consequently, there is a lack of transparency which permeates India's internet suspension practices.

A prominent example which helps illustrate the unique ways in which India's telecom/internet suspension framework can be used to curtail the public's access to social media is detailed below.

WHITELISTING IN KASHMIR | NETWORK LEVEL SOCIAL MEDIA CENSORSHIP

India's network-level censorship practices under its internet suspension framework is highly unusual. This process is known as whitelisting and was used to target, among other things, the public's access to social media. This case is worth highlighting since constitutional scholars argue that whitelisting affords excessive power to the State as compared to its opposite and more widely used option of blacklisting (via blocking and banning or specific content takedown under the IT Act which is discussed later).[264]

In the blacklisting paradigm, the public's access to information on the internet is considered the default state. The banning of certain content is the exception to the norm. The opposite is true in the case of whitelisting where the State's restriction of the internet becomes the norm.

Further, in the case of blacklisting, some experts contend that the onus rests with the State to provide a rationale for why the public cannot access a particular piece of content.[265] In the case of whitelisting the onus shifts onto citizens, where the entire

262 Samriddhi Sakunia, '3-Year-Old Supreme Court Order Restricting Internet Outages Is Ignored in India, World's Leading Offender' (*Article 14*, 27 January 2024) <https://article-14.com/post/3-year-old-supreme-court-orders-restricting-internet-outages-is-ignored-in-india-world-s-leading-offender-65b4783e28559>; *Internet Freedom Foundation*, '6 Months after *Anuradha Bhasin v. UoI*, State Governments Are Still Not Publishing Internet Shutdown Orders #KeepUsOnline' (*Internet Freedom Foundation*, 14 July 2020) <https://internetfreedom.in/publication-internet-shutdown-orders/>.

263 LOK SABHA, Internet Shutdowns, UNSTARRED QUESTION NO.1305, 9th February, 2022 <http://164.100.24.220/loksabhaquestions/annex/178/AU1305.pdf>.

264 Gautam Bhatia, 'The Kashmir Internet Ban: "Restoration", White-Listing, and Proportionality' (*Indian Constitutional Law and Philosophy*, 25 January 2020) <https://indconlawphil.wordpress.com/2020/01/25/the-kashmir-internet-ban-restoration-white-listing-and-proportionality/>.

265 Gautam Bhatia, 'The Kashmir Internet Ban: "Restoration", White-Listing, and Proportionality' (*Indian Constitutional Law and Philosophy*, 25 January 2020) <https://indconlawphil.wordpress.com/2020/01/25/the-kashmir-internet-ban-restoration-white-listing-and-proportionality/>.

internet is seen as dangerous and access to every section has to be secured by proving its harmlessness. Keeping this in mind let us consider how it was operationalised in Kashmir.

In August 2019, internet services were shut down in the erstwhile state of Jammu and Kashmir as the central government altered the region's legal status via a constitutional amendment. This indefinite suspension was challenged in the Supreme Court in the aforementioned *Anuradha Bhasin* case.[266] Among other things, the Supreme Court directed authorities to review the suspension in Kashmir, as well as restore the public's access to essential services online.[267] This triggered authorities to periodically review the situation in Kashmir and restore internet access in a phased manner.[268]

The manner of execution stirred controversy. Initially, internet services in the region were limited to only 2G mobile services and internet users were only permitted to visit a narrow list of white-listed websites. This whitelist excluded social media. This ban on access to social media through the country's internet suspension framework was extended till March 2020– a total period of seven months.[269]

Additionally, people's access to information online was further controlled by regulating the speed at which they access sites/apps. 4G internet/mobile services were only restored on February 6th, 2021, after 552 days of slow, limited or no internet access.[270]

The orders for whitelisting of websites directed ISP(s) to restrict all social media applications allowing peer-to-peer communication, and VPN applications.[271] The orders directed ISPs to install necessary firewalls and carry out white-listing of sites that would enable access to only the URL(s) approved by the government.[272] In the first order on

266 *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

267 'J&K adds 1,000 more websites to internet whitelist: Here are all 1,485 URLs' (*The Indian Express*, 16 February 2020) <https://indianexpress.com/article/india/jk-internet-websites-whitelist-urls-6270463/>.

268 Ibid.

269 Naveed Iqbal and Arun Sharma, 'J&K Admin Lifts Social Media Curbs, 7 Months after Clampdown' *The Indian Express* (4 March 2020) <https://indianexpress.com/article/india/jammu-kashmir-social-media-curbs-removed-6298847/>.

270 SFLC, 'Internet Shutdowns Tracker' (Internet Shutdowns Tracker by - SFLC.in) <https://internetshutdowns.in/>.

271 Ipsita Chakravarty, 'No social media, only institutional access and 'whitelisted' sites: Kashmir net curbs still severe' (*Scroll.in*, 16 January 2020) <https://scroll.in/article/950011/no-social-media-only-institutional-access-and-whitelisted-sites-kashmir-net-curbs-still-severe>.

272 Ibid.

January 18th, 2020 ,[273] 153 sites were whitelisted while a total of 301 URLs were included by January 24th, 2020[274] and 1485 URLs by 15th February 2020.[275]

Initially, only mail, banking, education, employment, travel, weather, utilities, entertainment, automobiles, and web services made it to the "whitelist". However, in subsequent orders, many news websites were included but social media remained conspicuously absent.

The first order on 14th January 2020 explains this absence since it justified the partial restoration as aiming to control threats from "separatists/ anti-national elements attempting to incite people by the transmission of fake news, targeted messaging to propagate terrorism, rumour-mongering, support fallacious proxy wars, spread propaganda/ideologies and cause dissatisfaction and discontent".[276]

3.5.3 Blocking Public Access to Information

Section 69A of the IT Act is a major statutory mechanism through which the State regulates information dissemination over cyberspace and social media.[277] Designated officers, primarily under MeitY, can issue content takedown orders for reasons relating to "sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognisable offence relating to above."[278] Such orders can only be issued[279] following procedures and safeguards prescribed by the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009.

According to this legal framework, any request for blocking issued by the government's nodal officer is sent to a designated officer and the examining committee, which reviews the legal validity of the nodal officer's request to block a piece of content.[280]

273 Home Department, Government of Jammu and Kashmir, 'Temporary suspension of Telecom Services- directions reg', Home-04(TSTS)of 2020 18 January 2020).

274 Home Department, Government of Jammu and Kashmir, 'Temporary suspension of Telecom Services- directions reg',Home-05(TSTS) of 2020 (24 January 2020).

275 Home Department, Government of Jammu and Kashmir, 'Temporary suspension of Telecom Services- directions reg', Home-13(TSTS)of 2020 (15 February 2020).

276 Home Department, Government of Jammu and Kashmir, 'Temporary suspension of Telecom Services- directions reg', Home-03(TSTS)of 2020(14 January 2020). <https://dot.gov.in/sites/default/files/Amendment_CMTS_6-2-06_2.pdf>.

277 IT Act 2000, Section 69A.

278 IT Act 2000, Section 69A(1).

279 IT Act 2000, Section 69A(2).

280 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, Rule 8.

Subsequently, if the examining committee and the Secretary approve a request, the designated officer issues the blocking order. The designated officer also has to notify the intermediary and identifiable content originator that a hearing will take place before the examining committee, in which they will get an opportunity to defend the validity of the impugned content.[281]

However, in case of an emergency, the designated officer can issue a content-blocking direction without giving notice to the intermediary and content originator and without consulting the examining committee.[282] In this scenario, the designated officer directly submits content-blocking recommendations to the Secretary, who then issues an interim blocking order. The interim order is then placed before the examining committee within 48 hours. Upon receiving the recommendations of the committee, the Secretary then issues a final emergency blocking order.

The Blocking Rules mandate strict confidentiality of government orders.[283] Therefore, in cases of issuance of blocking orders under section 69A, affected end-users are often not provided with a copy of the blocking order or any reasoning behind the government's decision to take down or block content.[284] This secrecy limits end users' ability to appeal the legality of government-issued content/information blocking orders.[285]

Twitter (now X) challenged blocking orders containing 39 URL(s) issued by MeitY under section 69A of the IT Act.[286] The petition argued that the blocking orders were arbitrary as they were 'substantively and procedurally' non-compliant with the Blocking Rules.[287] X had argued that the government does not have the power to block entire accounts (instead of specific unlawful tweets) as it restricts freedom of speech. Additionally, X also argued that the government failed to provide reasoned orders to the users under Rule 8 of the Blocking Rules.[288] The Karnataka High Court upheld the blocking orders and expanded the government's power to block entire accounts in cases of imminent

281 *Shreya Singhal v Union of India* 2015 (5) SCC 1 [121].

282 Blocking Rules 2009, Rule 9.

283 Blocking Rules 2009, Rule 16.

284 'Finding 404: A Report on Website Blocking in India,' *Software Freedom Law Centre* (2023) <https://sflc.in/finding-404-report-website-blocking-india/>.

285 Ibid.

286 Anushka Jain, 'Twitter Challenges Blocking Orders: Karnataka HC to Hear Plea in August' *MediaNama* (26 July 2022) <https://www.medianama.com/2022/07/223-twitter-blocking-orders-karnataka-hc-hearing-august-25/>.

287 *X Corp. v. Union of India* WP No. 13710 of 2022 (High Court of Karnataka, decision dated 30 June 2023).

288 Ibid.

societal harm.[289] Similarly, the Court ruled that communication of reasons to X sufficed the procedural requirement and the government does not need to share a reasoned order with the aggrieved user. X Corp has since appealed the single judge order as it allowed non disclosure of reasons to restrict online content.[290] As of February 2024, the case is being heard by a division bench at the Karnataka High Court.[291]

The Indian Government issues content takedown orders towards internet intermediaries, including social media platforms, very frequently. Between 2014 and 2021, MeitY has issued 25,368 take-down orders under section 69A, which include websites and social media content.[292] Meanwhile, MIB, which oversees the country's Digital Media Ethics Code and the digital media landscape in general, also issues content takedown directives under the IT Act's content-blocking framework. MIB has issued directions to block access to 56 YouTube-based news channels in 2021-2022.[293] This marks a 2000% increase in government blocking requests between 2014 and 2020.[294]

This trend towards content blocking is also reflected in Twitter's (now X) global transparency reports, which showed an increase of more than 48,000% between 2014 to 2020 in all legal demands (including courts, state governments, and central government) being made from India.[295]

The Indian Government has utilised this provision to block public access to certain content, apps and websites on grounds of national security.[296] For example, public access to Chinese apps has largely been banned, against the backdrop of cross-border tensions since 2020.[297]

289 Archit Lohani, 'Decoding the Karnataka High Court Ruling: Blocking Accounts vs Tweets' The CCG Blog (July 2023) <https://ccgnludelhi.wordpress.com/2023/07/19/decoding-the-karnataka-high-court-ruling-blocking-accounts-vs-tweets/>.

290 'Blocking of posts: X Corp challenges Centre's non-disclosure of orders at Karnataka HC' *The Indian Express* (January 2024) <https://indianexpress.com/article/cities/bangalore/tweets-x-corp-centre-karnataka-hc-9136051/>.

291 Ibid.

292 The Wire Staff, 'Govt Blocked Over 25,000 Web Pages, Sites, Social Media Pages From 2014-2021' *The Wire* (17 March 2022) <https://thewire.in/government/govt-blocked-over-25000-web-pages-sites-social-media-pages-from-2014-2021>.

293 Ibid.

294 Soumyarendra Barik, 'Content Blocking Orders by Govt and Courts to Twitter Soar 48,000%' *The Indian Express* (11 July 2022) <https://indianexpress.com/article/technology/social/content-blocking-orders-by-govt-and-courts-to-twitter-soars-48000-8021423/>.

295 Ibid.

296 *PIB*, 'Government Bans 59 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order' (29 June 2020) <https://pib.gov.in/PressReleasePage.aspx?PRID=1635206>.

297 'India bans 59 mostly Chinese apps amid border crisis' (*Reuters*, 29 June 2020) <https://www.reuters.com/article/idUSKBN24025A/>.

In June 2020, it first banned 59 Chinese apps, and since then, over 250 Chinese apps have been banned.[298] Notably, this includes apps like social media platform TikTok, WeChat, UC Browser, Mi Community, etc.[299]

The Indian government has also evoked this provision to block access to dissenting opinions around major political events like "abrogation of Article 370 of the Indian Constitution,[300] the passing of the Citizenship Amendment Act,[301] and the farmer protests[302]".[303]

In April 2021, Twitter (now X) took down 52 tweets that criticised the government's management of the pandemic, including tweets by a sitting Member of Parliament and a state minister.[304] The public officials argued that the content was blocked to counter misuse of social media to spread panic in society, but the move raised concerns about arbitrary state control of online criticism and political speech.

298 Divya Bharti, 'Full List of Chinese Apps Banned in India so Far: PUBG Mobile, Garena Free Fire, TikTok and Hundreds More' *India Today* (New Delhi, 21 August 2023) <https://www.indiatoday.in/technology/news/story/bgmi-garena-free-fire-tiktok-and-more-banned-in-india-check-the-full-list-1990048-2022-08-19>.

299 Surabhi Agarwal, 'Centre Issues Order to Ban 54 Chinese Apps' *The Economic Times* (15 February 2022) <https://economictimes.indiatimes.com/tech/technology/union-government-issues-fresh-orders-to-ban-over-54-chinese-apps/articleshow/89551062.cms?from=mdr>.

300 Article 370 of the Indian Constitution granted special status to the former state of Jammu and Kashmir. The abrogation of Article 370 has been challenged in the Supreme Court of India.

See *The Hindu Bureau, 'Challenge to the Abrogation of Article 370' The Hindu (19 August 2023)* <https://www.thehindu.com/news/national/challenge-to-the-abrogation-of-article-370/article67204414.ece>; *Mubashir Hussain, 'The Blocking Of "The Kashmir Walla" And Clampdown On Free Press In Kashmir' Outlook (29 August 2023)* <https://www.outlookindia.com/national/the-blocking-of-the-kashmir-walla-and-clampdown-on-free-press-in-kashmir-news-314170>; *Auqib Javeed, 'Police Question Kashmir Twitter Users For "Anti-Govt" Posts' (Article 14, 17 September 2020)* <https://www.article-14.com/post/the-real-cyber-bully-police-in-kashmir-question-twitter-users>.

301 The Citizenship Amendment Act led to widespread protests across India for instilling religious discrimination in granting of citizenship for immigrants and asylum seekers.

302 See 'Citizenship Amendment Bill: India's New "anti-Muslim" Law Explained' *BBC News* (9 December 2019) <https://www.bbc.com/news/world-asia-india-50670393>; Syed Mohammed, 'Twitter Asked to Take down Posts of Anti-CAA Activists' *The Hindu* (20 February 2020) <https://www.thehindu.com/news/national/telangana/twitter-notice-to-anti-caa-npr-activists/article30873222.ece>; The Wire Staff, 'On "Request", Twitter Removes Poster Calling for Protest Against Anti-CAA Activists' Arrests' *The Wire* (11 June 2020) <https://thewire.in/rights/twitter-poster-safoora-natasha-devangana-caa-protest>.

In 2020-2021 farmers led a massive protest against proposed agricultural reform bills that aimed to deregulate sale of crops among other things.

See Mujib Mashal, Emily Schmall and Russell Goldman, 'What Prompted the Farm Protests in India?' *The New York Times* (27 January 2021) <https://www.nytimes.com/2021/01/27/world/asia/india-farmer-protest.html>; Karan Deep Singh, 'Twitter Blocks Accounts in India as Modi Pressures Social Media' *The New York Times* (10 February 2021) <https://www.nytimes.com/2021/02/10/technology/india-twitter.html>; Anuj Srivas, 'Here Are Some Farmers' Protest Tweets That Twitter Blocked in Response To a Govt Order' *The Wire* (11 February 2021) <https://thewire.in/tech/farmers-that-twitter-blocked-government-order-list>

303 Paroma Soni, 'Online Censorship Is Growing in Modi's India' *Columbia Journalism Review* (14 December 2021) <https://www.cjr.org/investigation/modi-censorship-india-twitter.php>.

304 Aroon Deep, 'Twitter Censors Tweets from MP, MLA, Editor Criticising Pandemic Handling', *MediaNama* (blog), 24 April 2021, <https://www.medianama.com/2021/04/223-twitter-mp-minister-censor/>.

3.5.4 State Fact-Checking Unit

In April 2023, the government notified an amendment to the Intermediary Guidelines, Under Rule 3(1)(b)(v), wherein intermediaries - including social media platforms – have to "make reasonable efforts" to remove any information about the business of the central government that has been identified as "fake or false or misleading" by the Fact Check Unit of the central government notified for this purpose.[305] The Fact Checking Unit was notified in March 2024 and was subsequently stayed by the Supreme Court as the validity of the amendment remains under scrutiny at the Bombay High Court.[306]

The amendment has been heavily criticised for empowering the Indian Government to determine truth and subsequently shape public discourse over the internet, and more specifically on social media.[307] This regulation has raised significant concerns about government censorship and potential infringement on free speech rights,[308]

3.5.5 Law Enforcement Access to Information

The interception of communications for investigative purposes constitutes a significant part of India's legal framework for safeguarding national security and public order. In particular, it is a tool through which governments can, in specific instances, monitor how information is flowing through cyberspace, the sender and receiver of such communication, or even the content of such information.[309] Monitoring and interception frameworks are naturally applicable to social media platforms as well.

305 Ministry of Electronics and Information Technology,'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023'(6 April 2023).

306 Ananthakrishnan G, 'Supreme Court stays Centre's notification on fact-checking unit, says challenge involves free speech' *The Indian Express* (March 2024) <https://indianexpress.com/article/india/supreme-court-stays-notification-of-centres-fact-check-unit-9226286/>.

307 Vasudev Devadasan and Archit Lohani, 'CCG NLUD Comments on the draft amendments to the IT Rules' Centre for Communication Governance (January 2023) <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccgnlud-comments-on-it-rules-jan-23-368.pdf>; Archit, ,IT Rules amendments: Can PIB be given carte blanche to decide what is 'fake'?' *Alt News* (January 2023) <https://www.altnews.in/it-rules-amendments-can-pib-be-given-carte-blanche-to-decide-what-is-fake/>; Sarvesh Mathi, 'Indian Government Can Now Fact Check And Censor Any News Related To The Government: Amended IT Rules' *Medianama* (April 2023) <www.medianama.com/2023/04/223-it-rules-fact-check-amendments-censorship/>.

308 Vasudev Devadasan and Archit Lohani, 'CCG NLUD Comments on the draft amendments to the IT Rules' Centre for Communication Governance (January 2023) <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccgnlud-comments-on-it-rules-jan-23-368.pdf>.

309 Jhalak M. Kakkar and others, 'The surveillance law landscape in India and the impact of Puttaswamy' (CCG 2023).

In India, LEAs pursue interception and investigation in electronic and ICT environments through three primary legislations namely:

- The Telegraph Act 1885;
- IT Act 2000; and
- CrPC 1973

Interception and monitoring provisions under the Telegraph Act apply to network service operators, who operate as licensed telecom and ISPs.[310] These service providers are required to comply with security and interception requirements as prescribed in their licensing conditions.[311]

Local police often use section 91 of the CrPC, 1973 — a broad provision which gives police officers in charge of a police station the power to ask any person, including internet intermediaries, for the production of any document in their possession for an investigation, inquiry or proceeding.[312] Specifically, information request orders under section 91 of the CrPC are known to be inconsistent with the principle of proportionality and thus unreasonably compromise people's right to privacy guaranteed under the Indian Constitution.[313] Privacy concerns were brought to the fore when it was reported that a website was being investigated for violation of the Foreign Contribution Regulation Act (FCRA). During this investigation, the payment gateway disclosed donor information to the Delhi Police based on a CrPC section 91 order.[314]

310 Section 5(2) of the Indian Telegraph Act 1885, provides the Central and State governments powers under public emergency or in the interest of public safety, to intercept communication for the preservation of India's sovereignty or integrity, security of the state, public order, and maintaining friendly relations with foreign states

311 Licence Agreement for Unified License, Department of Telecommunications, Ministry of Communications, Government of India, <https://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf>.

312 Sashwata Saha, 'Razorpay Hands over Customer Data to Police in Alt News-Zubair Case' (*MediaNama*, 13 July 2022) <https://www.medianama.com/2022/07/223-razorpay-alt-news-customer-data-section-91-powers/>; The Leaflet, 'SC Relief to Twitter User Facing Allegations by Tripura Police' NewsClick (1 December 2022) <https://www.newsclick.in/SC-Relief-Twitter-User-Facing-Allegations-Tripura-Police>; Software Freedom Law Center, 'S.91 of CrPC – the Omnipotent Provision?' (19 March 2013) <https://sflc.in/s91-crpc-omnipotent-provision/>;

313 Krishnesh Bapat, '#Privacyofthepeople: 91 Problems but This Ain't One' (*Internet Freedom Foundation*, 16 July 2022) <https://internetfreedom.in/privacyofthepeople-91-problems-but-this-aint-one/>.

314 Srikanth Lakshmanan, 'The Razorpay-Alt News Controversy Opens Up a Can of Worms That Should Be Addressed' *The Wire* (8 July 2022) <https://thewire.in/tech/razorpay-alt-news-controversy-digital-payments-privacy>; Pranay Dutta Roy, '"Complied With Notice Sent by Authorities": Razorpay Amid Alt News FCRA Charges' *TheQuint* (5 July 2022) <https://www.thequint.com/news/india/razorpay-handed-over-doner-data-to-police-alt-news-amid-fcra-charge>.

Parallelly, providers of digital services and platforms (including online intermediaries[315] like social media intermediaries) are required to comply with interception and investigation conditions under the IT Act. Critically, from a proportionality standpoint, the scope of monitoring and interception under the IT Act is wider than the Telegraph Act.[316]

This is because section 69[317] doesn't have the pre-conditions of "public emergency" and "public safety" to authorise an interception.[318] Investigation under this provision can be invoked under additional grounds, including "defence of India" and the "investigation of any offence".[319] This final open-ended ground significantly lowers the threshold of circumstances under which interception can take place in ICT environments.[320]

Notably, section 69(3) calls upon intermediaries including social media companies to "extend all facilities and technical assistance". Section 69B of the IT Act also provides the central government with the power to authorise any agency to monitor traffic data or information (i.e. metadata) to enhance cyber security, and to analyse the status/reach of intrusions/malicious software. All interception and monitoring provisions mandate the recording of reasons for such orders in writing.

As noted earlier (see section 3.3.4), the Intermediary Guidelines 2021 introduced a provision which stated that SSMIs, which act primarily as messaging services, "shall enable the identification of the first originator of the information on its computer resource"[321] which has come under criticism[322] and its constitutionality has been challenged in multiple High Courts across India.[323]

315 IT Act 2000, s 2(1)(w).

316 Rishab Bailey and others, 'Use of Personal Data by Intelligence and Law Enforcement Agencies' [2018] Macro/Finance Group, National Institute of Public Finance and Policy.

317 Section 69 of the IT Act deals with interception, monitoring or decryption of information transmitted, received or stored through any computer resource.

318 Jhalak M. Kakkar and others, 'The surveillance law landscape in India and the impact of Puttaswamy' (CCG 2023).

319 The grounds include, "sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states, public order, preventing incitement to the commission of any cognisable offence or for investigation of any offence".

320 Jhalak M. Kakkar and others, 'The surveillance law landscape in India and the impact of Puttaswamy' (CCG 2023).

321 Intermediary Guidelines 2021, Rule 4 (2).

322 Grover, Gurshabad, Rajwade, Tanya and Katira, Divyank. "The Ministry and the Trace: Subverting End-to-End Encryption. *NUJS L. Rev*, Vol. 14 (2), 2021. <http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption>/.

323 Legal Challenges to the Traceability Provision: What is Happening in India?, Software Freedom Law Centre, May 2021, <https://sflc.in/legal-challenges-traceability-provision-what-happening-india>; Jhalak M. Kakkar and others, 'The surveillance law landscape in India and the impact of Puttaswamy' (CCG 2023).

Data retention is another regulatory mechanism to assist LEA(s) with accessing electronic evidence. The IT Act authorises the central government to mandate the duration, format, and manner in which intermediaries should preserve and retain information.[324] ISPs have data retention requirements through the licensing agreements under the Telegraph Act,[325] while the social media intermediaries have these mandates under their due diligence obligations.[326]

However, long retention requirements without explicitly mandating the destruction of such information after the completion of the requisite time[327] raise privacy and cybersecurity concerns.[328] Such requirements are inconsistent with the data minimisation principle, which is meant to, among other things, reduce the vulnerability surface of data environments in cyberspace. As observed previously (in section 3.3.5), the recent passing of Data Protection Legislation in India provides that data fiduciaries must erase personal data when (a) the data principal withdraws their consent or (b) the specified purpose of processing is no longer being served. However, this is not applicable when data retention is "necessary for compliance with any law for the time being in force".[329] This leaves sufficient room for the State to mandate longer retention periods.

---

324 IT Act, 2000, s 67C.

325 Ministry of Communications, "Amendment in Unified Licence (UL) Agreement for change in time period of storage of Call Detail Record (CDR)/Exchange Detail Record (EDR)/ IP Detail Record (IPDR)- regarding", No.20-271/2010 AS-1 (Vol.-III) (21 December 2021) amends the Unified Licence (UL) Agreement to increase retention of information of call data records, IP Detail records, log-in/log-out details of subscribers for services like internet access, email etc. for two years as compared to the one year timeline mandated earlier.

326 Intermediary Guidelines 2021, Rule 3(1)(g) mandates preserving information (and associated records) which has been taken down or blocked for a minimum period of one hundred and eighty days and longer duration if prescribed by the courts or authorised government agencies; Intermediary Guidelines 2021, Rule 3(1)(h) mandates retaining user registration information for a period of one hundred and eighty days after the user cancels/ withdraws such registration which is double the period mandated under the Technology (Intermediaries guidelines) Rules, 2011.

327 SPDI Rules 2011, Rule 5(4) mandates body corporate to not retain sensitive personal data longer than it is necessary to meet the purpose for which it was collected except in accordance with law. This provision has limited application as it deals with only sensitive personal data with body corporates. The DPDPA 2023, has more expansive provisions with respect to personal data.

328 Extensive data retention requirements have been imposed on VPN providers, which has pushed many of them over the edge.

See Explainer: New VPN Rules, Why Companies Are Upset and What They Mean for You' (*The Times of India*, 17 June 2022) <https://timesofindia.indiatimes.com/gadgets-news/explainer-new-vpn-rules-why-vpn-companies-are-upset-and-what-they-mean-for-you/articleshow/92270798.cms>.

329 DPDPA 2023, s 7.

Access to data for the investigation of crimes was also one of the key factors driving India's data localisation proposals under various drafts of the proposed data protection laws which were subsequently dropped in DPDPA 2023 (as seen in section 3.2.5). Such proposals were driven to resolve challenges LEAs have faced in securing access to electronic evidence– most often data– which is stored or processed in computing facilities/servers located in other jurisdictions.[330] Such problems arise as a result of systemic issues with cross-border Mutual Legal Assistance Treaties (MLATs).[331]

3.5.6 Other Measures

In this section, we discuss relevant non legislative measures deployed by the Indian Government which impact social media. These measures supplement the regulatory framework and assist in contextualising the on-ground state of affairs, as it demonstrates a clearer picture of the political economy around social media regulation.

For instance, it has been reported that the Indian Government has explored avenues to monitor people's behaviour over social media and cyberspace through non-legislative measures and programmes. In 2018, it was reported that a public sector undertaking ("PSU") affiliated with MIB issued a tender for vendors to develop and operationalise a social media communications hub.[332] The proposed hub was envisaged to have listening and responding capabilities across multiple platforms, sentiment analysis, influencer insights analysis, real-time alerts, campaign management and a conservation archive to maintain a record of user conversations. The tender was withdrawn after the Supreme Court observed that the wide scope of the proposed hub could lead to "creating a surveillance State".[333]

330 Committee of Experts under Chairmanship of Justice B.N Srikrishna Submitted to Ministry of Electronics and Information Technology, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians (2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf>.

331 Bedavyasa Mohanty and Madhulika Srikumar, *Hitting Refresh: Making India-US Data Sharing Work*, Observer Research Foundation, August 2017, https://www.orfonline.org/research/hitting-refresh-india-us-data-sharing-mlat/.

332 Aroon Deep, 'Government Withdraws Social Media Communications Hub Tender' (*MediaNama*, 3 August 2018)<https://www.medianama.com/2018/08/223-government-withdraws-social-media-communications-hub-tender/>.

333 Express Web Desk, 'Govt Withdraws "Social Media Hub" Plan after SC's Surveillance State Remark' *The Indian Express* (3 August 2018) <https://indianexpress.com/article/india/govt-withdraws-proposal-to-create-social-media-hub-after-snooping-allegations/>.

The same PSU has reportedly invited bids for tracking online sentiments for government-related activities, disinformation detection, etc.[334] Several State governments are also instituting social media monitoring cells for LEAs to monitor unlawful, false, extremist or inflammatory content. It has been reported that Tamil Nadu recently announced a state-level social media monitoring cell as a part of the Cybercrime Investigation Centre.[335] The Manipur police have reportedly issued an order to establish monitoring cells in every district of the state.[336] Similar cells have also reportedly been established in Delhi,[337] Maharashtra,[338] Telangana,[339] and Punjab.[340]

Similarly, it has been reported that the MHA oversees social media and occasionally issues advisories and engages in informal oversight of social media on matters of security, radicalisation, terrorist recruitment[341] and online extremist content.[342] It has also been reported that the MHA has also previously proposed setting up a multi-agency war room to analyse threats on social media 24*7,[343] and other initiatives to address the "misuse" of

334 Soumyarendra Barik, 'The Government Wants to Surveil Social Media Users, and Track Their "Sentiments"' *MediaNama* (8 October 2020) <https://www.medianama.com/2020/10/223-india-social-media-surveillance/>.

335 SELVARAJ A, 'Tamil Nadu: Special Police Unit to Monitor Fake Social Media Posts' *The Times of India* (19 March 2022) <https://timesofindia.indiatimes.com/city/chennai/tamil-nadu-special-police-unit-to-monitor-fake-social-media-posts/articleshow/90315927.cms>.

336 Indrajit Kundu, 'Manipur Police to Set up Social Media Monitoring Cell to Ensure "prompt Action" against "Unlawful Content"' *India Today* (Imphal, 21 July 2021) <https://www.indiatoday.in/india/manipur/story/manipur-police-social-media-monitoring-cell-prompt-action-against-unlawful-content-1830608-2021-07-21>.

337 RAJ SHEKHAR, 'Special Cell to Monitor Social Media, Youth Activity' *The Times of India* (10 May 2016) <https://timesofindia.indiatimes.com/city/delhi/special-cell-to-monitor-social-media-youth-activity/articleshow/52196626.cms>.

338 Mustafa Shaikh Mumbai, 'Maharashtra Cyber Police Acts Tough on People Making "Communal" Posts on Social Media' *India Today* (21 April 2022) <https://www.indiatoday.in/india/story/maharashtra-cyber-police-communal-posts-social-media-1939911-2022-04-21>.

339 TNN, 'Hyderabad Cops to Monitor Provocative Posts on Social Media' *The Times of India* (2 September 2022) <https://timesofindia.indiatimes.com/city/hyderabad/hyderabad-cops-to-monitor-provocative-posts-on-social-media/articleshow/93937437.cms>.

340 Tribune News Service, 'Social Media Monitoring Cell Established in Patiala District' *Tribuneindia News Service* (Patiala, 2 May 2022) <https://www.tribuneindia.com/news/patiala/social-media-monitoring-cell-established-in-patiala-district-391129>.

341 'India concerned over use of social media for recruitment of terrorists: US', *The New Indian Express* (2nd November 2019) <https://www.newindianexpress.com/world/2019/nov/02/india-concerned-over-use-of-social-media-for-recruitment-of-terrorists-us-2056154.html>.

342 Shruti Pandalai, 'ISIS in India: The Writing on the (Facebook) Wall,' *The Diplomat* (6th May 2016) <https://thediplomat.com/2016/05/isis-in-india-the-writing-on-the-facebook-wall/>.

343 Abhishek Bhalla, 'India wants 24x7 online war room to tackle cyber threat from ISIS,' *India Today* (24 December 2015) <https://www.indiatoday.in/mail-today/story/government-plans-social-media-scanning-centre-to-take-on-isis-278697-2015-12-24>.

social media by monitoring activity that "conspires against India" or spreads "anti-national propaganda".[344] Recent news reports have stated that the Indian Government regularly conducts informal meetings with social media platform operators on content moderation and law enforcement-related issues.[345]

3.5.7 Whistleblower Disclosures Indicate Informal Channels and State Influence

Multiple whistleblowers have highlighted the lack of transparency and accountability within social media platforms. In the Facebook Papers reports, whistleblower Frances Haugen revealed a multitude of internal documents to the US Congress. The documents showed that Facebook lacked any inclination to invest in efforts that curb online harms in India.[346]

The documents disclose that Facebook "routinely makes exceptions for powerful actors when enforcing content policy," even when the content violates its community guidelines on Coordinated Inauthentic Behaviour (CIB).[347] The disclosures reveal that unlawful content has not been moderated due to the "political sensitivities".[348]

Similar findings have been corroborated by the whistleblower Sophie Zhang, a former data scientist at Facebook. Zhang reported four sophisticated networks that were producing inorganic engagement during the 2019 elections.[349] Out of the four, it was reported that two networks were attributed to the opposition party. Facebook's staff reportedly took repeated action against one of them. However, it was reported that Facebook refused to take

344 PTI, 'Home Ministry to Come up with a New Social Media Policy' *The Indian Express* (New Delhi, 22 June 2017) <https://indianexpress.com/article/india/home-ministry-to-come-up-with-a-new-social-media-policy-4717466/>.

345 Karishma Mehrotra and Joseph Menn, 'How India Tamed Twitter and Set a Global Standard for Online Censorship' Washington Post (9 November 2023) <https://www.washingtonpost.com/world/2023/11/08/india-twitter-online-censorship/>.

346 Newley Purnell and Jeff Horwitz, 'Facebook Services Are Used to Spread Religious Hatred in India, Internal Documents Show' Wall Street Journal (23 October 2021) <https://www.wsj.com/articles/facebook-services-are-used-to-spread-religious-hatred-in-india-internal-documents-show-11635016354>.

347 Cat Zakrzewski and others, 'How Facebook Neglected the Rest of the World, Fueling Hate Speech and Violence in India' Washington Post (24 October 2021) <https://www.washingtonpost.com/technology/2021/10/24/india-facebook-misinformation-hate-speech/>.

348 Ibid.

349 Julia Carrie Wong and Hannah Ellis-Petersen, 'Facebook Planned to Remove Fake Accounts in India – until It Realised a BJP Politician Was Involved' *The Guardian* (15 April 2021) <https://www.theguardian.com/technology/2021/apr/15/facebook-india-bjp-fake-accounts>.

any action against the two networks related to the ruling party.[350] After going public with their findings, Zhang offered to provide their deposition before the Indian Parliamentary Standing Committee on Information Technology.[351] However, they were not given an opportunity to depose before the parliament did not materialise.[352]

The Cambridge Analytica case study also highlights the importance of revelations made by whistleblowers. In this case, whistleblower Christopher Wylie reportedly disclosed that various political parties have allegedly consulted the political consultancy group for its services.[353]

These whistleblower disclosures, along with reports of the Government's reliance on closed-door meetings,[354] highlight deeper concerns about the role of executive discretion.

3.6 Social Media Governance as a Security Issue

Globally, social media platforms are being regarded as important theatres to combat various security threats to the State such as radicalisation[355] and foreign influence operations.[356] The Indian government typically invokes national security and public order exceptions to combat various forms of internal and external threats to the State, which results in the

350 Ibid.

351 Haripriya Suresh, 'Facebook Whistleblower Tells TNM Why She Hasn't given a Deposition in India Yet' The News Minute (3 June 2022) <https://www.thenewsminute.com/news/facebook-whistleblower-tells-tnm-why-she-hasnt-given-deposition-india-yet-164640>.

352 It has been reported, that as per Parliamentary Rules, permission for Ms. Zhang's testimony was soughted from the Speaker of the Lok Sabha by the chairperson of the Standing Committee on Information Technology. However, ther Speaker neither granted nor denied persmission for the same. See Sobhana K Nair, 'Facebook Whistleblower Sophie Zhang Not to Depose before House Panel' *The Hindu* (21 April 2022) <https://www.thehindu.com/news/national/fb-whistleblower-not-to-depose-before-house-panel/article65341724.ece>; Arvind Kurian Abraham, 'Preventing Sophie Zhang from Testifying Is a Blow to Indian Parliamentary Democracy The Wire (1 July 2022) <https://thewire.in/rights/preventing-sophie-zhang-from-testifying-is-a-blow-to-indian-parliamentary-democracy>;

353 PTI, 'Indian Laws Inadequate to Deal with Data Theft, Say Experts' *The Economic Times* (1 April 2018) <https://economictimes.indiatimes.com/tech/internet/indian-laws-inadequate-to-deal-with-data-theft-say-experts/articleshow/63566404.cms?from=mdr>.

354 Aditya Kalra, 'EXCLUSIVE In Heated Meeting, India Seeks Tougher Action from U.S. Tech Giants on Fake News' *Reuters* (2 February 2022) <https://www.reuters.com/world/india/exclusive-heated-meeting-india-seeks-tougher-action-us-tech-giants-fake-news-2022-02-02/>.

355 Robin Thompson, 'Radicalization and the Use of Social Media' (2011) 4 Journal of Strategic Security 167 <https://www.jstor.org/stable/26463917>.

356 Arild Bergh, 'Understanding Influence Operations in Social Media' (2020) 19 Journal of Information Warfare 110.

restriction of fundamental rights. The deployment of such exceptions is often justified by arguing that online spaces such as social media platforms now pose unique threats to State security.[357]

For instance, as discussed previously, the government has banned over 250 Chinese apps since June 2020, including the popular social media platform TikTok, reportedly in the backdrop of escalating border skirmishes with China in the Ladakh region.[358] Initially, MeitY blocked 59 Chinese apps on grounds of "sovereignty and integrity of India, defence of India, security of state and public order"[359] and, the press release announcing the ban explicitly notes that protecting the "safety and sovereignty of Indian cyberspace" is its goal.[360] These apps are viewed as potential sites for the collection and mining of Indian users' data by foreign entities.

Security considerations also shape how the MIB administers the Digital Media Ethics Code portion of the Intermediary Guidelines, 2021. Since December 2021, the Authorised Officer under the MIB has blocked a significant amount of content across social media for emergency purposes.[361] Specifically, it has reportedly blocked over 90 YouTube-based news channels, many of which originate in Pakistan, on grounds of national security, sovereignty and integrity of India, public order, etc. Through these actions, it aimed to maintain a "safe and secure information environment in India across print, television and online media".[362] In one instance, reportedly MIB blocked 20 YouTube Channels and two websites for coordinated behaviour in spreading "anti-India propaganda" and divisive

357 See *Devesh K Pandey, 'Social Media Exploited to Promote Anti-India Activities, Say Experts'* The Hindu *(15 April 2022)* <https://www.thehindu.com/news/national/capacity-building-vital-for-countering-online-threats-say-experts/article65324361.ece>; *PTI, 'Anti-National Groups Using Social Media for Propaganda: Ravi Shankar Prasad'* The Economic Times *(25 February 2015)* <https://economictimes.indiatimes.com/news/politics-and-nation/anti-national-groups-using-social-media-for-propaganda-ravi-shankar-prasad/articleshow/46370571.cms>;

358 Amy Kazmin and Christian Shepherd, 'India Bans 118 Chinese Apps as Himalayan Border Tensions Surge' *Financial Times* (2 September 2020).

359 "Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order" *PIB* (29 June 2020) < https://pib.gov.in/PressReleseDetail.aspx?PRID=1635206>.

360 Ibid.

361 Intermediary Guidelines 2021, Rule 16.

362 "Ministry of I&B blocks 16 YouTube news channels for spreading disinformation related to India's national security, foreign relations and public order" *PIB* (25 April 2022) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1819892>.

content.[363] This was followed by more Pakistani YouTube channels and other social media handles, and websites[364] being reportedly blocked in January 2022.[365]

The government is usually not forthcoming about information on blocking and banning online content under section 69A of the IT Act. But in this case, the MIB held a press conference[366] to publicise and justify its actions. It stated that the blocked social media handles propagated a "war of misinformation against the country".[367] These blocking orders were passed under the emergency provisions,[368] reportedly to thwart coordinated disinformation networks which were a threat to the "sovereignty" of the country.

Further, the MIB has released press notes[369] giving detailed viewership statistics and examples/screenshots of the fake content posted by these handles. Reasons cited for these blocking orders include "anti-India" fake news on "sensitive topics like Indian Army, Jammu and Kashmir, India's foreign relations" and content that could interfere with elections.[370] In April 2022, MIB banned[371] several YouTube channels (both from India and Pakistan) for spreading fake news related to Ukraine with the potential of, *inter alia*, harming India's foreign relations.

363 "India dismantles Pakistani coordinated disinformation operation. The Ministry of Information and Broadcasting blocks Pakistan sponsored fake news networks. 20 YouTube Channels, 2 websites blocked for spreading anti-India propaganda" *PIB* (21 December 2021) <https://pib.gov.in/PressReleasePage.aspx?PRID=1783804>.

364 35 Youtube Channels, two websites, two Instagram accounts and one Facebook account were blocked.

365 "India Strikes Hard on Pakistani Fake News Factories. Ministry of Information and Broadcasting Blocks Pakistan Funded Fake News Networks.35 YouTube Channels, 2 Websites Blocked for Spreading Anti-India Fake News" *PIB* (21 January 2022)<https://www.pib.gov.in/PressReleasePage.aspx?PRID=1791547>.

366 The Hindu Bureau, 'Centre Orders Ban on 35 Pakistan-Based YouTube Channels' *The Hindu* (New Delhi:, 21 January 2022) <https://www.thehindu.com/news/national/centre-orders-ban-on-35-pakistan-based-youtube-channels/article38303797.ece>.

367 ibid.

368 Intermediary Guidelines 2021, Rule 16.

369 See "Ministry of I&B blocks 16 YouTube news channels for spreading disinformation related to India's national security, foreign relations and public order" *PIB* (25 April 2022) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1819892>; "India dismantles Pakistani coordinated disinformation operation. Ministry of Information and Broadcasting blocks Pakistan sponsored fake news network. 20 YouTube Channels, 2 websites blocked for spreading anti-India propaganda" *PIB* (21 December 2021< https://pib.gov.in/PressReleasePage.aspx?PRID=1783804>.

370 See "India Strikes Hard on Pakistani Fake News Factories. Ministry of Information and Broadcasting Blocks Pakistan Funded Fake News Networks.35 YouTube Channels, 2 Websites Blocked for Spreading Anti-India Fake News" *PIB* (21 January 2022)https://www.pib.gov.in/PressReleasePage.aspx?PRID=1791547.

371 "Ministry of I&B blocks 22 YouTube channels for spreading disinformation related to India's national security, foreign relations and public order" *PIB* (5 April 2022) https://pib.gov.in/PressReleasePage.aspx?PRID=1813603; "Ministry of I&B blocks 16 YouTube news channels for spreading disinformation related to India's national security, foreign relations and public order" *PIB* (25 April 2022) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1819892>.

Misuse of Security Exceptions and Censorship

Although there are legitimate security and geopolitical interests that guide States' approach to social media regulation, security considerations have also been extensively employed by governments globally to limit the free speech of their citizens. Mechanisms to curb online content have been reported to be deployed by the State to curtail journalistic reportage,[372] political dissent and debate.[373] This is done by restricting access to information and regulating user behaviour by characterising political issues as security concerns.[374]

To this end, concerns have been raised about the arbitrary nature of certain blocking orders by the MIB.[375] More recently, in January 2023, it curtailed the circulation of a controversial BBC documentary.[376] Concerns have also been raised concerning blocking orders issued by MeitY under section 69A of the IT Act.[377]

372 See Amnesty International, *Access Now*, *Human Rights Watch*, Freedom House, International Commission of Jurists, 'India: Authorities Should Stop Targeting, Prosecuting Journalists and Online Critics' (May 3 2022)<https://www.amnesty.org/en/latest/news/2022/05/india-authorities-should-stop-targeting-prosecuting-journalists-and-online-critics/>; Katy Migiro, 'India Blocks Journalists' Tweets about Violence against Muslims' (*Committee to Protect Journalists*, 12 September 2023) <https://cpj.org/2023/09/india-blocks-journalists-tweets-about-violence-against-muslims/>; Vakasha Sachdev, 'Is the Ban on Twitter Accounts of Caravan, Farm Activists Legal?' (*TheQuint*, 1 February 2021) <https://www.thequint.com/news/law/legal-basis-twitter-accounts-caravan-withheld-69a-it-act-blocking-rules-review-and-challenges>;

373 See Shirin Ghaffary, 'A Major Battle over Free Speech on Social Media Is Playing out in India during the Pandemic' (Vox, 1 May 2021) <https://www.vox.com/recode/22410931/india-pandemic-facebook-twitter-free-speech-modi-covid-19-censorship-free-speech-takedown>; 'India: Activists Detained for Peaceful Dissent' (*Human Rights Watch*, 15 April 2020) <https://www.hrw.org/news/2020/04/15/india-activists-detained-peaceful-dissent>; Sameer Yasir, 'Climate Activist Jailed in India as Government Clamps Down on Dissent' *The New York Times* (15 February 2021) <https://www.nytimes.com/2021/02/15/world/asia/climate-activist-jailed-india.html>

374 Kilroy defines "Securitization as the process through which non politicised (issues are not talked about) or politicised (issues are publicly debated) issues are elevated to security issues that need to be dealt with urgency, and that legitimate the bypassing of public debate and democratic procedures."

See Richard J Kilroy, 'Securitization' in Anthony J Masys (ed), Handbook of Security Science (Springer International Publishing 2018) <https://doi.org/10.1007/978-3-319-51761-2_11-1>

375 Dhruv Bhatnagar, 'Government Blocks YouTube Channels: I&B Ministry's Take-down Procedures Lack Transparency' *The Indian Express* (19 August 2022) <https://indianexpress.com/article/opinion/columns/government-blocks-youtube-channels-ib-ministry-procedures-transparency-8100205/>; Tanmay Singh, 'No, I&B Ministry Does Not Have Power to Block YouTube Accounts' Newslaundry (29 September 2022) <https://www.newslaundry.com/2022/09/29/no-ib-ministry-does-not-have-power-to-block-youtube-accounts>.

376 Manish Singh, 'India Blocks YouTube Videos and Twitter Posts on BBC Modi Documentary' (*TechCrunch*, 21 January 2023) <https://techcrunch.com/2023/01/21/india-blocks-youtube-videos-and-twitter-posts-on-bbc-modi-documentary/>

377 See section 3.5.3 for details.

Similar critiques have been made about internet shutdown orders, which tend to bypass procedural safeguards. According to an Access Now report on internet shutdowns, in India "national security" was the most frequently relied upon justification for imposing shutdowns in instances of protest.[378] In 2021, India was reportedly one of 18 countries to impose mobile internet shutdowns as a response to political protests.[379]

India's legal system allows both state and central government authorities to carry out such measures. At the national level, mobile internet shutdowns were reportedly observed during two widespread protest movements.[380] At the state level, authorities suspended mobile internet services as pre-emptive measures in anticipation of protests. For example, in the state of Rajasthan, the Government imposed an internet shutdown ahead of protests called by a community demanding reservations in government jobs and academic institutions.[381]

The suspension of the internet in the Indian state of Kashmir during the abrogation of Article 370[382] and the recent shutdown in the state of Manipur, engulfed in sectarian violence, has elicited criticism.[383] Such shutdowns hinder the freedom of the press and the freedom of ordinary citizens to document violence, particularly against vulnerable groups in times of conflict.[384] Experts argue that such measures are excessive, do not address public emergency or public safety concerns and negatively affect the livelihood of local communities.[385]

---

378 *Access Now*, 'The Return of Digital Authoritarianism: Internet Shutdowns in 2021' (2022).

379 Ibid.

380 'In Pictures | How 2020 Was Bookended by Anti-CAA and Farmer Protests' (*The Indian Express*, 26 December 2020) <https://indianexpress.com/article/india/2020-protests-caa-jnu-jamia-shaheen-bagh-7118839/> accessed 7 June 2022.

381 Express News Service, 'Ahead of Nov 1 Gujjar Stir, Internet Suspended in Parts of Rajasthan' *The Indian Express* (31 October 2020) <https://indianexpress.com/article/india/ahead-of-nov-1-gujjar-stir-internet-suspended-in-parts-of-rajasthan-6910677/>

382 See 3.5.2 for more details.

383 Parth M.N., 'An Internet Shutdown Means Manipur Is Burning in the Dark' [2023] Wired UK <https://www.wired.co.uk/article/internet-shutdown-manipur-burning-in-the-dark>.

384 Namrata Maheshwari and Shruti Narayan, 'Manipur Internet Shutdowns: Forgetting the Lessons from Kashmir' *The Indian Express* (28 July 2023) <https://indianexpress.com/article/opinion/columns/manipur-internet-shutdown-kashmir-8864472/>;Kavitha Iyer, 'In India, World's Internet Shutdown Capital, Blockades Undermine Livelihood, Food Security, Human Rights' (*Article 14*, 14 June 2023) <https://article-14.com/post/in-india-world-s-internet-shutdown-capital-blockades-undermine-livelihood-food-security-human-rights--64892c096a39a>;Astha Rajvanshi, 'How Internet Shutdowns Wreak Havoc in India' [2023] TIME <https://time.com/6304719/india-internet-shutdowns-manipur/>

385 Rituraj Kumar, 'Internet Suspension in India: A Call for Balancing Security and Rights' (ORF) <https://www.orfonline.org/expert-speak/internet-suspension-in-india/> accessed 9 October 2023.

The Department of Telecom (DoT) has been criticised by the Parliamentary Standing Committee[386] for exercising internet suspension powers without[387] (i) any empirical studies on the impact of such orders, (ii) recording reasons for such suspensions, and (iii) maintaining a database for issued orders.

When it comes to criminalising individual users, the reported instances of use of the sedition provision by LEAs against journalists, first-time internet users and minorities have been criticised.[388] In addition, it has been reported that the Government has recently started mobilising citizens to police other people's behaviour in online environments like social media.[389] The MHA's Cyber Crime Volunteers program launched by the I4C calls for citizens to register as anonymous volunteers and flag unlawful content to aid law enforcement agencies.[390] The portal lists content that threatens the "sovereignty and integrity of India, defence of India, security of the state, friendly relations with foreign states, public order, communal harmony and content involving child sexual abuse" as categories of unlawful content to be reported by volunteers to law enforcement.[391] Such

386 PTI, 'Parliamentary Panel Pulls up DoT on Internet Shutdowns; Asks to Keep Record, Assess Its Impact' *The Economic Times* (9 February 2023) <https://economictimes.indiatimes.com/news/india/parliamentary-panel-pulls-up-dot-on-internet-shutdowns-asks-to-keep-record-assess-its-impact/articleshow/97774813.cms>.

387 Standing Committee on Communications and Information Technology, Action Taken by the Government on the Observations/Recommendations of the Committee contained in their Twenty-sixth Report (Seventeenth Lok Sabha) on 'Suspension of Telecom Services/Internet and its impact' (Lok Sabha 2022-23 37).

388 See Mohit Rao, 'Karnataka Has More Sedition Cases Based On Social-Media Posts Than Any State. Most Are Illegal —' *Article 14* (13 July 2021) <https://article-14.com/post/karnataka-has-more-sedition-cases-based-on-social-media-posts-than-any-state-most-are-illegal-60ecf64da7945>; 'India: Government Policies, Actions Target Minorities' *Human Rights Watch* (New York, 19 February 2021) <https://www.hrw.org/news/2021/02/19/india-government-policies-actions-target-minorities>;Vijayta Lalwani, 'Backgrounder: What Is Delhi Police's Riots Conspiracy Case?' *Scroll.in* (8 October 2020) <https://scroll.in/article/974904/backgrounder-what-is-delhi-polices-riots-conspiracy-case>; Aneesha Bedi, 'Delhi Minorities Commission Chief Charged with Sedition for "Provocative" Social Media Post' *ThePrint* (2 May 2020) <https://theprint.in/india/delhi-minorities-commission-chief-charged-with-sedition-for-provocative-social-media-post/413112/>; Zeba Siddiqui, 'Indian Journalists Accused of Sedition over Protest Reporting' *Reuters* (1 February 2021) <https://www.reuters.com/article/idUSKBN2A11I7/>.

389 See Sushovan Sircar, 'Govt's Cyber Volunteers Move Raises Social Media "Vigilante" Fears' The Quint (10 February 2021) <https://www.thequint.com/cyber/policy/mha-cyber-volunteer-anti-national-social-posts-vigilante-fears>; Vijaita Singh, 'Cyber Crime Volunteers Plan Fraught with Dangers: *Internet Freedom Foundation*' *The Hindu* (2 March 2021) <https://www.thehindu.com/news/national/cyber-crime-volunteers-plan-fraught-with-dangers-internet-freedom-foundation/article33973393.ece>.

390 Ministry of Home Affairs, Government of India, 'Cyber Crime Volunteers Concept' (National Cyber Crime Reporting Portal) <https://cybercrime.gov.in/Webform/cyber_volunteers_concept.aspx>.

391 Ministry of Home Affairs, Government of India, 'What Is Unlawful Content' (National Cyber Crime Reporting Portal) <https://cybercrime.gov.in/Webform/about_unlawful_content.aspx>.

schemes have been criticised by scholars and civil society for increasing cyber vigilantism, lateral surveillance,[392] and censorship.[393]

3.7 Balancing State Security Imperatives Against Fundamental Rights

Article 19(2) of the Indian Constitution empowers the government to make laws that impose reasonable restrictions on fundamental freedoms of citizens in the interest of "sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order", among others. The laws governing internet suspension, government blocking of online content, LEA access to user information and several laws criminalising offline and online speech like sedition are all grounded in the exceptions granted under Article 19(2).

Unfortunately, as analysed in this chapter, the executive enforces these laws arbitrarily. So, in practice, they exceed the limited remit granted by Article 19(2) and over restrict speech. For instance, the procedural rights enshrined within these laws, such as Internet Suspension Rules and the Blocking Rules, are routinely not adhered to.

As discussed in this chapter, the social media regulatory framework has constantly been put to the test in various courts in the country, which has resulted in an expansion of the jurisprudence on substantive and procedural rights of citizens. However, the legislative framework provides wide discretion in the context of the security considerations of the state,[394] and also does not compel transparency and accountability.

392 Mira Swaminathan, Now, an expanded horizon of surveillance, *The Hindu*, March 2021, https://www.thehindu.com/opinion/lead/now-an-expanded-horizon-of-surveillance/article34014308.ece, accessed August 09, 2022; Also see: Mira Swaminathan and Shubhika Saluja, Widening the Horizons of Surveillance | Lateral Surveillance Mechanisms: Issues & Challenges, The Centre for Internet & Society, January 2021, https://cis-india.org/horizonsofsurveillance, accessed August 08, 2022.

393 *Internet Freedom Foundation*, 'MHA's New Programme Allows Volunteers to Report "Anti-National" Online Content for Removal' (*Internet Freedom Foundation*, 23 February 2021) <https://internetfreedom.in/cyber-volunteer/>.

394 Regina Heller, Martin Kahl and Daniela Pisoiu, 'The "Dark" Side of Normative Argumentation – The Case of Counterterrorism Policy' (2012) 1 Global Constitutionalism 278 <https://www.cambridge.org/core/journals/global-constitutionalism/article/abs/dark-side-of-normative-argumentation-the-case-of-counterterrorism-policy/E6E2D85F5FB95A6CE089E51D58F30186>.

To properly enforce security imperatives, the government must comply with prescribed substantive and procedural safeguards. Specifically, it must effectuate such actions through a specific law that serves a legitimate aim, and the action must be proportionate and necessary. To evaluate the legality of the restrictions placed upon online information or services through laws, the order to restrict and the process to restrict the information or service must satisfy certain standards to efficiently resolve the tension between fundamental freedoms, due process and security objectives of the state.

These standards are already enshrined within Indian jurisprudence. They include:

(i) Legal basis: The government cannot invoke vague and arbitrary limitations on speech. Limitations can be invoked "when there exist adequate safeguards and effective remedies against abuse."[395] These must be codified in a law passed by Parliament.

(ii) Grounds for restriction must be specific: Limitations on speech accruing directly out of security considerations of the state must be specific and demonstrate the precise nature of the threat. The law in question must establish a direct and immediate connection between such limitations and the security threat .[396]

(iii) Clearly defined :[397] Laws containing security-related restrictions must clearly define terms such as "safety and sovereignty of Indian cyberspace", or "war of misinformation against the country" or "anti-India" content. This will ensure that the limitation placed on online speech and access to information is not unnecessary and disproportionate.

(iv) Proportionality and necessity: Security-related laws that restrict free speech must be necessary.[398] This is to ensure that the security provisions are invoked for the prescribed reason and for the purpose they are predicated on, to achieve the protective function. Additionally, the measure must be proportional to the type of

395 See 1 *Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors.*, (2017) 10 SCC 1; United Nations Economic and Social Council, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, UN Doc. No. E/CN.4/1985/4, Annex (1985), Principle 31.

396 *Modern Dental College and Research Centre v State of Madhya Pradesh*, (2016) 7 SCC 353.

397 *Maneka Gandhi v Union of India*, 1978 AIR 597.

398 *Anuradha Bhasin v Union of India*, W.P. (C) No. 1031 of 2019

action invoked in order to address the harm. To test the proportionality of a restrictive action, the authorities should be able to provide reasons and elucidate why this is the least restrictive measure to address the harm.[399]

(v) Procedural fairness: The observance of procedural safeguards is an imperative component of principles of natural justice.[400]

Overall, the regulation of information and services online often impacts the fundamental rights accorded to citizens by the Constitution of India. The government's approach has been criticised as it exercises discretion in dispensing its duties, bypassing safeguards. Furthermore, due to a lack of checks and balances within the social media regulation frameworks, there are limits on judicial, parliamentary and public oversight. Therefore rights restricting executive action (i) must be subject to judicial review, (ii) have a legal basis, (iii) have a proportionate nexus with the harm it seeks to restrict and (iv) observe procedural fairness.

3.8 Evolving Threat Perception in Cybersecurity and Information Security

Cybersecurity has always had an outsized focus on the interests of nation-states as compared to the interests of individuals.[401] This cultivates an approach that looks at cyber governance issues primarily through a state security lens. In this section, we look at the possibility of the state using its regulatory toolbox to regulate information flow as a cybersecurity or information security threat.

We have outlined "cybersecurity" regulation in India (see section 3.2). As discussed earlier, certain reports suggested[402] that the threat perception in cybersecurity could potentially focus more closely on disinformation, influence operations and narrative

399 1 *Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors.*, (2017) 10 SCC 1.

400 Madhyamam Broadcasting Limited vs Union Of India, 5 April, 202, Civil Appeal No. 8129 of 2022 <https://main.sci.gov.in/supremecourt/2022/6825/6825_2022_1_1501_43332_Judgement_05-Apr-2023.pdf>.

401 Ronald J Deibert, 'Toward a Human-Centric Approach to Cybersecurity' (2018) 32 Ethics & International Affairs 411 <https://www.cambridge.org/core/journals/ethics-and-international-affairs/article/abs/toward-a-humancentric-approach-to-cybersecurity/4E8819984202A24186BB0F52E51BC1E4>.

402 Sunetra Choudhury, 'Cyber Policy to Factor in Threat from State Actors' *Hindustan Times* (New Delhi, 5 March 2021) <https://www.hindustantimes.com/india-news/cyber-policy-to-factor-in-threat-from-state-actors-101614897658901.html >.

warfare in the upcoming policies. The increasing emphasis on "narrative wars" in cybersecurity discourse is also evident from discussions on the need for unified public relations commands for the three wings of the armed forces and clearly defining "information warfare" and "narrative warfare" at the national level.[403]

With respect to "information security", though India does not have a comprehensive national doctrine, the National Information Security Policy and Guidelines (NISPG) in 2014 offers a theoretical window into the Government of India's approach.[404] The MHA released these guidelines that articulate India's approach to protecting classified State information which affects national security. The NISPG aims to prevent information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction.

Broadly, India's Information Security Policy appears to be motivated to prevent the interruption of services, and non-availability of information, ensure compliance with law and regulations, and mitigate losses due to disclosure/theft of information. Protecting digital information that has a bearing on national security has become the core concern of national information security.

Thus, the information security guidelines for social media focus on preventing those working in government offices from wilfully or inadvertently leaking official information on such platforms. This understanding of information security is also evident in directives concerning the download, installation and use of certain apps issued to armed forces personnel and their families.[405]

However, these definitions are ever-evolving and in a constant state of flux. The Indian Government's emphasis on "information security" to maintain the sanctity of online information is reflected in MeitY's response to a parliamentary question

403 PTI, 'Pakistan Has Got Its Act Together in Narrative Warfare with Its DGISPR: Indian Cybersecurity Chief' *The Economic Times* (21 December 2019) <https://economictimes.indiatimes.com/news/defence/pakistan-has-got-its-act-together-in-narrative-warfare-with-its-dgispr-indian-cybersecurity-chief/articleshow/72915729.cms?from=mdr> accessed 17 March 2022.

404 National Information Security Policy and Guidelines, Ministry of Home Affairs, Government of India (9th October 2014) < http://faridkotpolice.in/guidlines.pdf >.

405 Prabhjote Gill, List of 89 apps banned for Indian army soldier, Business Insider, 9 July 2020, <https://www.businessinsider.in/tech/apps/news/checkout-the-list-of-89-apps-banned-for-indian-army-soldiers/articleshow/76865942.cms>.

This directive was challenged unsuccessfully in the Delhi High Court recently Lt. Col. PK Choudhary v. Union of India WP(C) 4181/2020, Delhi High Court Judgement dated 5th August 2020. <https://indiankanoon.org/doc/52271519/>.

about the government's efforts to curb fake news. Here, MeitY cited its Information Security Education & Awareness (ISEA) programme as a counteraction to mis/disinformation.[406] Apart from advice on fake news, this programme's website contains information and guidelines for protection against trolling, hate crimes, cyberbullying, doxxing, online sexual abuse and scams.[407]

Furthermore, since the Indian Government has initiated consultations to overhaul the IT Act,[408] recommendations and views of Parliamentary Committee reports could be instructive in projecting future law and policy approaches. For instance, a recent report by a Parliamentary Committee on External Affairs when discussing cybersecurity has stated that "fake news propagation, election interference, inflammatory messages on social media leading to social and civil unrest, propagation of obscene material over cyberspace, online radicalisation of youth, etc., these increasingly threaten the safety, security and stability of nations."[409]

Even at the global level, some experts have advocated for a conception of cybersecurity beyond the technical CIA triad, encompassing a broader threat perception that will include disinformation campaigns.[410]

It is worth noting at this point that cybersecurity definitions have never been "purely technical" and have always been imbued with significant political values.[411] National security imperatives have driven cybersecurity threat perceptions to varying degrees. For instance, in the USA, concerns about terrorism have been driving these security interests historically.[412] While in countries like Russia and

406 Ministry of Electronics and Information Technology, Lok Sabha, "Authentication of Social Media Accounts" (Starred Question No 385, 30 March 2022) <http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=36991&lsno=17>

407 Information Security Awareness <https://www.infosecawareness.in>.

408 From Internet Dependency to Need for New Digital Law: MoS Rajeev Chandrasekhar Explains it All, News18, March 2022, <https://www.news18.com/news/tech/from-internet-dependency-to-need-for-new-digital-law-mos-rajeev-chandrasekhar-explains-it-all-4901222.html>.

409 India And International Law Including Extradition Treaties with Foreign Countries, Asylum Issues, International Cyber-Security And Issues of Financial Crimes, Page 29, Parliament Committee on External Affairs, Ninth Report, Lok Sabha Secretariat, Ministry of External Affairs, Government of India, September 2021, <http://164.100.47.193/lsscommittee/External%20Affairs/17_External_Affairs_9.pdf>.

410 Kathleen M Carley and others, 'Social Cyber-Security' (Springer 2018).

411 Helen Nissenbaum, 'Where Computer Security Meets National Security' (2005) 7 Ethics and Information Technology 61.

412 Ibid.

China, the information security and sovereignty approach to internet governance,[413] has always factored in socio-political, socio-economic, spiritual, moral, and State-specific cultural dynamics whilst classifying information security threats.[414]

As India contemplates a new cybersecurity policy, it will be important to trace how conceptions of cybersecurity and information security evolve and impact the online information ecosystem.

3.9 Assessing the Impact on the Rule of Law

India's security-first outlook on social media regulation has impacted the democratic rule of law. Our analysis relies on the United Nations' (UN) characterisation of 'rule of law'.[415] In 2004, the UN Secretary-General described the rule of law as a governance principle which holds all persons, institutions, and entities (including the State) accountable to public laws which are equally enforced and independently adjudicated. Such laws must be consistent with human rights benchmarks.[416] In this context, our analysis benchmarks Indian social media regulation against the following parameters :[417]

1) supremacy of law,
2) equality before the law,
3) accountability to the law,
4) fairness in application,
5) separation of powers,
6) participatory decision-making,

413 Bruna Toso de Alcântara, 'SCO and Cybersecurity: Eastern Security Vision for Cyberspace' (2018) 6 International Relations 549 <https://www.researchgate.net/publication/330732964_SCO_and_Cybersecurity_Eastern_Security_Vision_for_Cyberspace>.

414 Shanghai Cooperation Organization (SCO), 'Agreement between the Governments of State Members of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring the International Information Security' (2009) notes "dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of the states" as a threat to information security.

415 United Nations General Assembly 'Declaration of the High-level Meeting of the General Assembly on the Rule of Law at the National and International Levels' (2012) A/Res/67/1 <https://www.un.org/ruleoflaw/files/A-RES-67-1.pdf>.

416 Report of the Secretary-General, 'The rule of law and transitional justice in conflict and post-conflict societies' (2004) S/2004/616, Para 6 <https://digitallibrary.un.org/record/527647>.

417 Ibid.

7) legal certainty,
8) avoidance of arbitrariness, and
9) procedural plus legal transparency.

(a) Supremacy of Law

According to this principle, governments derive their authority from established law, and they cannot exercise powers beyond the defined scope of their mandate. This principle limits the scope of discretionary action and clearly defines the contours of governmental powers.[418] Additionally, under the principle, a person/entity can only be held accountable upon breach of a distinct codified law, otherwise, discretionary application of law can jeopardise the freedoms of legal persons/entities.[419]

The following instances demonstrate that India's approach to social media governance contradicts both aspects of this principle. First, the government is inclined to use non-statutory mechanisms in overseeing cyberspace and social media within it. These include periodic informal meetings with social media platform operators on online content issues, calls for private sector vendors to develop social media monitoring tools to monitor citizen behaviour online, and recruiting anonymous citizen volunteers to flag online content for LEAs through a national cybercrime reporting tool without any statutory basis (as seen in previous sections).

Second, the government's indirect influence on social media platforms' internal functioning has come to the fore with leaked internal documents and whistleblower accounts from Meta. According to the platform's internal communication, "political sensitivities" and commercial considerations in their biggest market often dictate Facebook's actions in India.[420] Politically affiliated users and content are often not sanctioned, even when found to violate Facebook's own hate speech community guidelines[421] and inauthentic

418 *Minerva Mills Ltd. and Ors. v. Union of India and Ors*. AIR 1980 SC 1789.

419 Eugenef Miller, 'Hayek's The Constitution of Liberty,' <https://iea.org.uk/sites/default/files/publications/files/Hayek%27s%20Constitution%20of%20Liberty.pdf>.

420 Newley Purnell and Jeff Horwitz, 'Facebook's Hate-Speech Rules Collide With Indian Politics' (WSJ, 14 April 2020) <https://www.wsj.com/articles/facebook-hate-speech-india-politics-muslim-hindu-modi-zuckerberg-11597423346>.

421 Ibid.

behaviour policies.[422] Taking a contrary position to the government may also invite retaliatory measures. After Twitter (now X) labelled a tweet by a ruling party spokesperson as manipulated by the media, it was reported that officers of the Delhi police visited the company's India headquarters.[423]

Additionally, the police across different states have continued to rely on section 66A of the IT Act to arrest critics of the government, despite it having been struck down by the Supreme Court years ago for being unconstitutional.[424]

These activities take place outside the scope of any established law or policy. They demonstrate that when it comes to overseeing information ecosystems like social media, there is a trend wherein the government's actions contradict the supremacy of law principle.

(b) Equality Before the Law

Laws must be non-discriminatory and extend equal protection to everyone.[425] This means that no individual or group of individuals are privileged with unequal legal protection over others.[426] In the Indian context, the Constitution prohibits the State from passing any discriminatory laws.[427] Similarly, equal protection of the law also affords similar rights and liabilities to all citizens in similar circumstances.

The takedown of journalistic publications and arrest of critics has serious ramifications for the principle of equal protection. Such actions are accomplished through an overbroad interpretation of penal provisions.

422 Devesh Kumar, 'Facebook Inaction: Whistleblower Documents Name BJP MP Vinod Sonkar in "Fake Account" Controversy' *The Wire* (6 June 2022) <https://thewire.in/tech/facebook-inaction-whistleblower-documents-name-bjp-mp-vinod-sonkar-in-fake-account-controversy>.

423 The Wire Staff, 'Twitter Gets Police Visit After Agreeing With Congress That BJP Leader Used "Manipulated Media"' (*The Wire*, 24 May 2021) <https://thewire.in/tech/delhi-police-twitter-office-raid-sambit-patra-toolkit>.

424 See Express News Service, 'Scrapped 6 Yrs Ago, 66A Still in Use: Shocked Supreme Court Seeks Govt Reply' *The Indian Express* (New Delhi, 6 July 2021) <https://indianexpress.com/article/india/shocking-scrapped-section-66a-it-act-supreme-court-7389766/>;Deeksha Bhardwaj, 'Several Examples of 66(A) Being Used despite Being Struck Down' *Hindustan Times* (New Delhi, 6 July 2021) <https://www.hindustantimes.com/india-news/3several-examples-of-66-a-being-used-despite-being-struck-down-101625510533292.html>.

425 Tom Bingham, The Rule of Law, Penguin (2010) p. 3.

426 *Shayara Bano v Union of India*, WP (C) 118/2016.

427 Constitution of India, 1947, *Article 14*.

A journalist was arrested for a four-year-old tweet,[428] allegedly for hurting religious sentiments following a complaint by an anonymous handle.[429] The arrest reportedly came in the backdrop of his recent work highlighting Islamophobic comments made by a political official in a television debate,[430] which sparked a diplomatic backlash and widespread international condemnation.[431] This arrest led to a series of cases being filed against the journalist's various tweets and fact-checking posts, such that the Uttar Pradesh state government constituted a Special Investigation Team to investigate the six cases registered in the state.[432] These charges reflect a reported trend of misuse of the law against citizens,[433] like journalists who highlight the rising prevalence of hate speech against minorities in India. This in contrast with reports of Facebook's alleged inaction on hate speech against minorities being perpetrated by politicians or groups affiliated or allegedly associated with the ruling party, even when it was flagged internally by company employees.[434]

At a systemic level, the principle of equality before the law is impinged when members of the public criticise elected representatives and political officials. For example, a noted filmmaker was arrested for posting a picture of a prominent cabinet minister with a suspended officer charged with corruption,[435] and a Youtuber was arrested for derogatory

428 The 2018 tweet was a screenshot from a satire scene in a 1983 Hindi movie.

429 'Mohammed Zubair: Indian Police Arrest Journalist over Tweets' *BBC News* (28 June 2022) <https://www.bbc.com/news/world-asia-india-61956108>.

430 Sudhi Ranjan Sen, 'Indian Fact Checker Who Highlighted Anti-Islam Comments Arrested' Bloomberg.com (28 June 2022) <https://www.bloomberg.com/news/articles/2022-06-28/indian-fact-checker-who-highlighted-anti-islam-comments-arrested>.

431 The Wire Staff, 'The Full List of 20 Countries and Bodies That Have Condemned the BJP Leaders' Remarks' (*The Wire*, 7 June 2022) <https://thewire.in/communalism/the-full-list-of-18-countries-and-bodies-that-have-condemned-the-bjp-leaders-remarks>.

432 The Quint, 'UP Police Forms SIT To Probe Cases Against Alt News Co-Founder Mohammed Zubair' (*TheQuint*, 12 July 2022) <https://www.thequint.com/news/india/uttar-pradesh-police-special-investigation-team-alt-news-co-founder-mohammed-zubair>.

433 Mani Chander, 'Jailed Or Punished, With Or Without Trial: How The State Misuses The Law Against India's Inconvenient Citizens — *Article 14*' (19 July 2022) <https://article-14.com/post/jailed-or-punished-with-or-without-trial-how-the-state-misuses-the-law-against-india-s-inconvenient-citizens-62d615129ab71>.

434 See Newley Purnell and Jeff Horwitz, 'Facebook's Hate-Speech Rules Collide With Indian Politics' Wall Street Journal (14 August 2020) <https://www.wsj.com/articles/facebook-hate-speech-india-politics-muslim-hindu-modi-zuckerberg-11597423346>;Billy Perrigo, 'Facebook Let an Islamophobic Conspiracy Theory Flourish in India Despite Employees' Warnings' [2021] *Time* <https://time.com/6112549/facebook-india-islamophobia-love-jihad/>.

435 Scroll Staff, 'Filmmaker Avinash Das Arrested for Sharing Photo of Amit Shah with Suspended IAS Officer' (*Scroll.in*, 21 July 2022) <https://scroll.in/latest/1028713/filmmaker-avinash-das-arrested-for-sharing-photo-of-amit-shah-with-suspended-ias-officer>.

comments against the West Bengal Chief Minister,[436] and charged under various sections of the IPC and IT Act.[437]

(c) Accountability to the Law and Fairness in Application

Everyone should be subject to the law of the land and the law should be applied uniformly not arbitrarily.[438] The principle of accountability to the law enables the enforcement of checks and balances on authorities to limit any misuse of power.[439] To ensure accountability, mechanisms of oversight and redressal are institutionalised to address any threats to the rule of law.

In December 2021, India's Parliamentary Standing Committee on Information Technology criticised the lack of transparency on such orders by state governments.[440] The committee highlighted the lack of adequate safeguards contributing to the arbitrary application of internet suspensions.[441]

The report identifies instances wherein local authorities have misused internet suspensions for routine policing and administrative imperatives, such as preventing cheating in exams and preventing local crime.[442] This is in contravention of the grounds of suspension i.e., 'public emergency' and 'public safety.' Unfortunately, these grounds remain undefined and susceptible to arbitrary implementation.

436 Umang Poddar, 'How the Law Is Being Misused to Stop Indians from Criticising Politicians' (*Scroll.in*, 23 July 2022) <https://scroll.in/article/1028742/how-the-law-is-being-misused-to-stop-indians-from-criticising-politicians>.

437 These include sections 120B (criminal conspiracy), 153(A) (promoting enmity between two communities), 295(A) (injuring or defiling place of worship with intent to insult the religion of any class), 504 (intentional insult with intent to provoke breach of peace), 506 (criminal intimidation) of the Indian Penal Code.

438 AV Dicey, Introduction to the Study of the Law of the Constitution, 1885.

439 *Kesavananda Bharati v State of Kerala* (AIR 1973 SC 1461).

440 Standing Committee on Communications and Information Technology, Suspension of Telecom Services/Internet and its Impact (Lok Sabha 2021-22 26) p 40; Moshumi Das Gupta, Internet suspension rules 'grossly misused', caused huge economic loss, says Parliament panel," *The Print*, December 2, 2021, <https://theprint.in/india/governance/internet-suspension-rules-grossly-misused-caused-huge-economic-loss-says-parliament-panel/775119/>.

441 Standing Committee on Communications and Information Technology, Suspension of Telecom Services/Internet and its Impact (Lok Sabha 2021-22 26) p 45.

442 Standing Committee on Communications and Information Technology, Suspension of Telecom Services/Internet and its Impact (Lok Sabha 2021-22 26) p 36.

Internet suspensions, ordered by executive authorities, are only subject to executive oversight and there is no judicial or parliamentary oversight. Consequently, there are no adequate mechanisms to ensure accountability over executive action and prevent the harming of the interests of citizens due to the detrimental impact of suspensions.

The fairness in application principle implies that law must be equally applied to all individuals, entities and communities.[443] As discussed in the chapter in various recent instances, the inconsistent and discriminatory application of legal measures such as the takedown of political speech has led to criticism of government actions.

Content blocking that is driven by state security imperatives can disproportionately impact the rights of citizens living in regions of conflict. For instance, a CPJ study,[444] on takedown notices sent by the Indian government to Twitter (now X) between August 2017 and 2019, found that as many as 45% of the accounts subject to takedown notices mentioned 'Kashmir' in their handle/bio or in content recently posted by the account holder.

Further, as discussed in this chapter, the lack of transparency from the government regarding takedown orders and from social media platforms regarding their compliance with such orders has led to concerns about the disproportionate curtailment of online information through opaque legal arrangements.[445]

As illustrated in this chapter, the ad-hoc and discretionary application of criminal law provisions such as sedition to social media speech is also concerning. Similarly, the overbroad application of section 54 of the DMA (discussed in 3.5.1) to curtail disinformation also highlights an inconsistent and haphazard approach to the application of the law. Such an incongruous application goes well beyond the legislative intent of the framers of the DMA.

443 Eugenef Miller, 'Hayek's The Constitution of Liberty,' <https://iea.org.uk/sites/default/files/publications/files/Hayek%27s%20Constitution%20of%20Liberty.pdf>.

444 Avi Asher-Schapiro and Ahmed Zidan, 'India Uses Opaque Legal Process to Suppress Kashmiri Journalism, Commentary on Twitter' (*Committee to Protect Journalists*, 24 October 2019) <https://cpj.org/2019/10/india-opaque-legal-process-suppress-kashmir-twitter/>.

445 Al Jazeera Staff, 'Social Media Giants Accused of "Silencing" Kashmir Voices' (1 October 2021) <https://www.aljazeera.com/news/2021/10/1/kashmir-report-accuses-us-social-media-giants-of-censorship>.

The lack of accountability and clear redressal mechanisms for overbroad executive curtailment of speech as as seen throughout this report, creates an atmosphere of inconsistent application of laws and diminishes individual rights to freedom of speech and expression and the right to access information. This causes a "chilling effect" on fundamental rights.

(d) Separation of Powers

This principle confers the ability to limit and check institutional violations of rule of law principles.[446] It ensures accountability by limiting imbalances between the judicial, legislative and executive branches of government.[447]

Both the Blocking Rules, 2009 and the Intermediary Guidelines, 2021 have emergency blocking provisions that empower the government to issue takedown orders without rigorous checks and balances involving the different branches of government. The Blocking Rules 2009, even mandate the confidentiality of takedown orders. It, therefore, paves the way for the concentration of power in the hands of the executive. Indeed, the confidentiality of blocking orders means that (i) the reasons for such orders are not subject to public scrutiny, (ii) there are very limited opportunities for judicial review of such orders (iii) the right to seek reddressal for impacted users is constrained by lack of information

Similarly, the monitoring and interception orders under section 69 of the IT Act do not mandate any judicial sanction raising similar concerns of executive discretion. Additionally, the Intermediary Guidelines 2021, require SSMIs that are primarily messaging services to furnish the details of the first originator of a message upon receiving an order by a either a court or a competent authority notified in section 69 of the IT Act.[448] This provision aims to assist LEAs in investigating various crimes and offences (see section 3.3.4 and section 3.5.5).

446 *Kesavananda Bharati v State of Kerala* (AIR 1973 SC 1461).

447 *State Of U.P. & Ors vs Jeet S. Bisht*, (Special Leave Petition (Civil) No.6928 of 1999).

448 In 2018, the Ministry of Home Affairs authorised ten Security and Intelligence Agencies to intercept, monitor and decrypt any electronic information in any computer resource. These include the Intelligence Bureau, Narcotics Control Bureau, Enforcement Directorate, Central Board of Direct Taxes, Directorate of Revenue Intelligence, Central Bureau of Investigation; National Investigation Agency, Cabinet Secretariat (R&AW), Directorate of Signal Intelligence (For service areas of Jammu & Kashmir, North-East and Assam only) and Commissioner of Police, Delhi.

See Ministry of Home Affairs (Cyber and Information Security Division) Order 2018, S.O. 6227(E).

As noted earlier, the limited parliamentary and judicial oversight and lack of effective public consultations during the drafting of this provision reveal the erosion of checks and balances.

To reiterate, as discussed in this chapter, the separation of powers principle is compromised as a result of the current mechanism under the IT Act through which Indian authorities issue legal orders for (a) content blocking; and (b) monitoring, interception and investigation of user activities in social media. Specifically, both procedures are entirely executive driven and even the mechanism for review of orders is situated within the executive.

The constitutional validity of the Interception Rules, 2009 has also been challenged before the Supreme Court in *Internet Freedom Foundation v. Union of India*.[449] In it, the petitioners have stated that the absence of judicial oversight makes the interception/monitoring framework inconsistent with the thresholds for reasonable restrictions of the right to privacy articulated by the Supreme Court in the case of *KS Puttaswamy v Union of India*.[450]

Established mechanisms for parliamentary oversight have also not been effective recently. The Facebook whistleblower Sophie Zhang did not receive the Lok Sabha Speaker's permission to testify before the Parliamentary Standing Committee on Communication and Information Technology despite repeated efforts by the Committee and the whistleblower.[451]

(e) Participatory Decision Making

This principle promotes multi-stakeholder processes, which serve as consensus-building methods among stakeholders.[452] Holding public consultations is a hallmark of multistakeholder law-making processes. However, governmental bodies have been criticised for limited public engagement. For instance, the Intermediary Guidelines, 2021 were brought into force without meaningful public consultation.[453]

449 *Internet Freedom Foundation v. Union of India* [W.P. (C) No. 44 of 2019].

450 (2017) 10 SCC 1, AIR 2017 SC 4161.

451 Arvind Kurian Abraham, 'Preventing Sophie Zhang from Testifying Is a Blow to Indian Parliamentary Democracy' (*The Wire*, 1 July 1022) <https://thewire.in/rights/preventing-sophie-zhang-from-testifying-is-a-blow-to-indian-parliamentary-democracy>; Sobhana K Nair, 'Facebook Whistleblower Sophie Zhang Not to Depose before House Panel' *The Hindu* (21 April 2022) <https://www.thehindu.com/news/national/fb-whistleblower-not-to-depose-before-house-panel/article65341724.ece>.

452 John Stuart Mill, "Considerations on representative government," 1873.

453 Torsha Sarkar, 'New Intermediary Guidelines: The Good and the Bad' [2021] *Down To Earth* <https://www.downtoearth.org.in/blog/governance/new-intermediary-guidelines-the-good-and-the-bad-75693>.

Another key feature of the participatory decision-making principle involves passing laws after undertaking appropriate legislative debate and voting procedures involving elected representatives. In this context, the Intermediary Guidelines 2021 were brought into force as delegated legislation under the IT Act, even though they introduce substantive concepts which were not envisioned under the parent statute. This raises concerns around its constitutionality as it appears inconsistent with established jurisprudential principles against excessive delegation of law-making powers to the executive.[454] The decision to forego a legislative amendment and operationalise through a law is contrary to the principle of participatory decision-making.

Additionally, due to an overburdened scrutiny process and other structural issues with parliamentary oversight of delegated legislation,[455] participatory decision making often becomes limited. For instance, an RTI has revealed that the Committees of Subordinate Legislation of Lok Sabha and Rajya Sabha have not discussed the Intermediary Guidelines 2021.[456]

(f) Legal Certainty

This principle is essential to enable citizens to adhere to the laws of the country. It requires the law to be consistent, clear, publicly accessible, binding, and reasonable to maintain legal certainty.[457]

Several examples help explain how this principle has been impacted when it comes to information and social media regulation.

An important case study is the laws which apply to social media platforms and the dilution of the safe harbour protections. We have cited many instances of legal uncertainty concerning the platform's compliance with due diligence obligations. These include the

454 Torsha Sarkar and others, On the legality and constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Centre for Internet and Society, June 2021, https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021, accessed June 30, 2022.

455 'Parliamentary Scrutiny of Executive Rule Making' *PRS India* (2012) <https://prsindia.org/files/parliament/discussion_papers/1370586704_Parliamentary%20Scrutiny%20of%20Executive%20Rule%20Making.pdf>.

456 The Wire Staff, 'New IT Rules Used But Not Considered by Committees of Subordinate Legislation of LS, RS' *The Wire* <https://thewire.in/government/new-rules-under-it-act-used-several-times-but-not-yet-tabled-in-lok-sabha>.

457 James Maxeiner, "Some Realism About Legal Certainty in the Globalization of the Rule of Law," *University of Baltimore Law*, 2008, <https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?article=1409&context=all_fac>.

use of automated filtering technologies in removing unlawful content, keeping unlawful content from resurfacing on platforms, and the concept of identifying "first originators" of unlawful content.

Moreover, the prohibited content for social media platforms—as stated in the due diligence obligations—under the Intermediary Guidelines 2021 remain undefined and ambiguous. In many ways, its vagueness can be said to replicate the ambiguity of the unconstitutional section 66A of the IT Act, which was struck down by the Supreme Court in the Shreya Singhal case.

Such legal uncertainty means that there is a likelihood that platforms will err on the side of caution and engage in over-censorship of user behaviour to avoid liability. This is an example of legal uncertainty leading to what Balkin describes as collateral censorship.[458] Other instances of legal uncertainty arise from LEAs' repeated use of provisions under both the IT Act and general criminal law to criminalise people's behaviour in social media and cyberspace.

(g) Avoidance of Arbitrariness; Procedural and Legal Transparency

Arbitrary action or inaction by the executive can lead to non-compliance with lawful directives, this is often inconsistent with the fair application of the law.[459] Lack of procedural safeguards and oversight mechanisms can diminish accountability, allowing abuse of power.[460] Due process (procedural safeguards and redressal mechanisms) defined within the law is a key feature which restricts arbitrariness and helps ensure predictability.

For instance, as discussed in this chapter, the arbitrary application of the Blocking Rules 2009 and non-adherence with the procedural safeguards, severely implicates citizens' fundamental right to freedom of speech and expression. Without access to the reasoning behind such a ban, congruence and legal certainty of such provisions are adversely impacted as well.

458 Jack Balkin, Free speech is a triangle, Columbia Law Review, Volume 118, Issue no. 7, 2018, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3186205>.

459 *Indra Nehru Gandhi V Raj Narayan*, (1975 AIR 2299, 1976 (2) SCR 347).

460 *Maneka Gandhi v. Union of India*, 1 SCC 248 (Supreme Court of India 1978).

In this regard, transparency measures foster the rule of law by exposing any secret or arbitrary action by the authorities.[461] Procedural safeguards and transparency measures can enable greater predictability of law enforcement and expose any inconsistent application of the law.[462] Indian courts have attempted to engender greater procedural transparency within India's information, internet governance, and social media landscape.

For instance, in the *Anuradha Bhasin* case, the Supreme Court mandated that all internet suspension orders must necessarily be publicly available so that the public has a reasonable opportunity to seek legal remedies against authorities' decisions. Similarly, MeitY was asked by the Delhi High Court to provide the petitioner with a post-decisional hearing and provide the original copy of the content blocking order under section 69A of the IT Act and the Blocking Rules 2009 in the *Tanul Thakur* case .[463]

3.10 Conclusion

A key component of democratic societies is adherence to the rule of law. However, in this chapter, we have pointed to systemic challenges of the adherence with rule of law principles in India, when it comes to the regulation of the flow of information online, especially when dealing with state security concerns.

This is due to the lack of adequate procedural safeguards and robust institutional checks and balances leading to over-centralisation of power with the executive. As a result, executive action is often taken arbitrarily and without transparency, as well as without meaningful parliamentary and judicial oversight. Further, the overbroad and vague definitions of state security exceptions contribute to enabling broad executive discretion. This leaves room for potential misuse and indiscriminate use of security exceptions, which can lead to overstepping critical fundamental rights, including free speech and privacy. As observed across multiple examples in this chapter, reliance on state security exceptions have resulted in the overbroad curbing of speech.

As India is contemplating a major overhaul of its social media and other ICT regulatory frameworks, it becomes important to rethink how state security concerns and the freedoms of citizens can be balanced.

461 Robert Vaughn, "Transparency in the Administration of Laws: The Relationship between differing justifications for Transparency and differing views of Administrative Law," <https://www.corteidh.or.cr/tablas/r29844.pdf>.

462 Murat Jashari and Islam Pepaj, "The Role of the Principle of Transparency and Accountability in Public Administration," Danubis University, 2018, <https://core.ac.uk/download/pdf/229465497.pdf>.

463 'Delhi HC Orders MeitY to Give Copy of Ban Order and Hearing to Mr Tanul Thakur for Banning His Website #WhatTheBlock' (*Internet Freedom Foundation*, 16 May 2022) <https://internetfreedom.in/delhi-hc-directs-meity-to-provide-a-copy-of-the-blocking-order-and-a-post-decisional-hearing-to-mr-tanul-thakur-whattheblock/>.

4. BANGLADESH'S LANDSCAPE ON SOCIAL MEDIA REGULATION AND IMPACT ON RULE OF LAW

4.1 Introduction

Presently, the Cyber Security Act 2023 (CSA) is the primary legislation for the governance of social media platforms and end-user behaviour online.[1] In addition to laying down the intermediary liability and content blocking framework, it encompasses cybercrime provisions and also codifies the cybersecurity framework.

Other ICT laws and policies like the Bangladesh Telecommunications Act 2001 (BTA), the Information and Communication Technology Act 2006 (ICTA), and the National Cyber Security Strategy 2014 also have implications for social media platforms and end-users. Statutes like the Bangladesh Penal Code 1860 and the Anti-Terrorism Act 2009 (ATA) have also been used to govern users' speech and actions on social media platforms.

It is to be noted that the Cyber Security Act 2023 replaced the Digital Security Act 2018 on 18 September 2023.[2] Before that, the DSA was the main legislation for social media regulation between the first week of October 2018 and the second week of September 2023. It is also to be noted that the DSA has been repealed by section 59(1) of the CSA. However, according to section 59(2) of the CSA, any proceeding or case initiated before or taken cognisance by the Cyber Tribunal under any section(s) of the DSA, if remains pending at any stage of the trial, the proceeding or case will continue as if the said section(s) of DSA had not been

1 Cyber Security Act No. 39 of 2023 ("CSA") repealed the Digital Security Act No. 46 of 2018 ("DSA").

2 'Digital Security Act Goes, CSA Succeeds' *The Financial Express* (8 August 2023) <https://today.thefinancialexpress.com.bd/first-page/digital-security-act-goes-csa-succeeds-1691431379>.

repealed, and the trial will continue. In the future, as incidents get registered under the CSA, it will be appropriate to analyse the impact and effectiveness of the CSA. However, for now, most of the analysis in this chapter is based on the implementation of the DSA.

Two proposed legislative developments that impact the social media governance framework are the Draft Regulation for Digital, Social Media, and OTT Platforms 2021 and the Draft Personal Data Protection Act (PDPA) 2023. Interestingly, the Bangladesh Telecommunication Regulatory Commission (BTRC) submitted an English draft titled "The Bangladesh Telecommunication Regulatory Commission Regulation for Digital, Social Media and OTT Platforms" ("Draft OTT Policy") to the High Court Division of the Supreme Court of Bangladesh in 2021. The Ministry of Information and Broadcasting (MIB) of Bangladesh submitted a Bangla draft titled "Over the Top (OTT) Content-based Service Provide and Regulations Policy – 2022"("proposed OTT policy by MIB") to the High Court in January 2023.[3] Both drafts have not been approved yet. On the other hand, the Cabinet approved the draft of PDPA 2023 in November 2023.[4] However, the PDPA has yet to receive parliamentary approval and is yet to come into effect.

This chapter begins by mapping key developments in social media governance in Bangladesh. It delves into (a) cybersecurity regulations and other relevant ICT regulations impacting social media in Bangladesh; (b) the intermediary liability regime applicable to social media platforms; (c) speech laws and counter-terrorism laws; (d) relevant administrative institutions which oversee Bangladesh's social media ecosystem; and (e) proposed and upcoming laws to regulate social media.

After mapping key legislative developments, the chapter analyses how these frameworks regulate the flow of online information. Next, the chapter examines how state security imperatives shape such a regulation of social media.

The final section of the chapter examines how social media regulatory frameworks fare against rule of law principles. It concludes that laws and regulations governing social media platforms and end-users have several shortcomings in this regard.

3 *Ashutosh Sarkar and Mahmudul Hasan, 'OTT Regulation: Revised Draft Bans a Whole Lot of Content' The Daily Star (9 January 2023)* <https://www.thedailystar.net/news/bangladesh/news/ott-regulation-revised-draft-bans-whole-lot-content-3215876>.

4 *Staff Correspondent, 'Draft Data Protection Act: Cabinet Okays It Giving Free Rein to Law Enforcers' The Daily Star (28 November 2023)* <https://www.thedailystar.net/news/bangladesh/news/draft-data-protection-act-cabinet-okays-it-giving-free-rein-law-enforcers-3480656>.

4.2 Cybersecurity and ICT Regulation Applicable to Social Media

4.2.1 Critical Information Infrastructure (CII) and Computer Protected System

The government adopted a National Cyber Security Strategy for the first time in 2014 which identified measures to reduce threats and vulnerability of CIIs from external attacks.[5] Action 3 of the strategy deals with the protection of CIIs and the identification, designation and accreditation of important systems as CIIs as a priority. It envisages a process of national vulnerability assessments to understand the consequences arising out of any threat or vulnerabilities online.

CII has since been an important component of cybersecurity, and this is reflected in the Draft Cybersecurity Strategy 2021-2025,[6] the DSA and the CSA. The CSA defines CII as any gazetted,[7] external or virtual information infrastructure that controls, processes, circulates or preserves critical information and if damaged or critically affected, may adversely impact "public safety, financial security, public health, national security, national integrity or sovereignty."[8] Furthermore, the CSA also states that any malicious intervention or damage to CIIs shall be deemed to be an offence with imprisonment between three to six years and a fine of up to one crore BDT.[9]

The Director General of the National Cyber Security Agency (see section 4.6) can inspect CIIs and investigate matters concerning the safety of CIIs to ensure that security requirements under the CSA are being met.[10] The CSA also requires that the Government and the Director General are presented with a yearly monitoring report.[11]

5 National Cyber Security Strategy, 2014 <https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/policies/3e8d0018_757f_4033_8b9c_47ee17e88c2c/Cyber_Security_Guideline-1.pdf>.

6 Bangladesh Cybersecurity Strategy 2021-2025 <https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/nothi_10314_2021_07_30_31627641428.pdf>.

7 CSA 2023, s 15.

8 CSA 2023, s 2(g).

9 CSA 2023, s 17(1).

10 CSA 2023, ss. 16(1) and (3).

11 CSA 2023, s 16(2).

The CSA, like the DSA includes an overbroad definition of CIIs, as it can include any digital system, platform or application.[12] The criteria for identifying a CII is codified under the Digital Security Rules, it includes broad considerations such as the size of the platform, and its potential detrimental impact on public safety and security.[13] However, the rules for CSA have not been adopted yet.

The CSA also criminalises intentional illegal access to a protected computer, network or system with up to three years of imprisonment and a fine.[14] The Rules further outline various obligations, functions and powers of the Director General, the National Cyber Security Council, the National Computer Emergency Response Team, and the Digital Forensic Lab.[15]

It is important to note that the CSA, like its predecessor DSA, does not clarify which computer systems or networks should be identified as protected systems.[16] Moreover, the ICTA also defines a protected system, where the controller is empowered to declare any computer, computer system, or computer network as a protected system and may authorise individuals to secure access to the protected system.[17]

The Government of Bangladesh identified 34CIIs as of 2023.[18] The enlisted CIIs include institutions such as the Prime Minister's Office, central and state-owned banks, the national identity and immigration departments etc. However, the list excludes ministries like defence, home, and armed forces, as well as the national parliament, the judicial branch, health sector, customs, and ports.

12 Rezaur Rahman Lenin, 'Law Review; DSA 2018 And Questions Of Citizens' Basic Human Rights - শুদ্ধস্বর' (শুদ্ধস্বর, 2021) <https://shuddhashar.com/law-review-digital-security-act-2018-and-questions-of-citizens-basic-human-rights/>.

13 Digital Security Rules, 2020, r 19.

14 CSA, 2023, s 18 (3).

15 CSA, 2023, ss. 9, 10 and 12.

16 Rezaur Rahman Lenin, 'Law Review; DSA 2018 And Questions Of Citizens' Basic Human Rights - শুদ্ধস্বর' (শুদ্ধস্বর, 2021) <https://shuddhashar.com/law-review-digital-security-act-2018-and-questions-of-citizens-basic-human-rights/>.

17 Information & Communication Technology Act 2006, s 47.

4.2.2 LEA Access to User Data

In the backdrop of increasing 'terrorist activities' and the bombing of 17 August 2005, the Bangladeshi government enacted a law to empower the MHA to tap any telephone line on the ground of combating terrorism.[19] In 2006, when the Bangladesh Telecommunications (Amendment) Act 2006[20] amended the BTA [21] to include Section 97(A), the LEAs were able to monitor and intercept user communications on broad grounds. Section 97(A) states that, to preserve the "security of the state" and ensure "public tranquillity", the Government can conduct investigations without a warrant or court order.[22] It empowers any LEA (includes intelligence agencies, national security agencies, investigation agencies, or any officer of any LEA)[23] to record and collect information on communications made by any person through a telecommunications service.[24] Through the Bangladesh Telecommunication (Amendment) Act 2010, the BTA has been renamed as the Bangladesh Telecommunication Regulatory Act 2001 (BTRA).[25]

18 See 'Five More Govt Organisations Announced as Critical Information Infrastructure' *The Daily Star* (9 August 2023) <https://www.thedailystar.net/business/news/five-more-govt-organisations-announced-critical-information-infrastructure-3390381>; Staff Correspondent, '29 Institutions "Critical Info Infrastructure"' *The Daily Star* (4 October 2022) <https://www.thedailystar.net/news/bangladesh/news/29-institutions-critical-info-infrastructure-3134666>.

The critical information infrastructures include the PMO; the President's Office; Bangladesh Bank; National Board of Revenue; Immigration and Passport Department; Bridges Division; National Data Center Company Ltd; National Data Centre, Bangladesh Computer Council; BTRC; Election Commission's national identity database; Central Procurement Technical Unit; Sonali Bank; Agrani Bank; Rupali Bank; Janata Bank; Rooppur Nuclear Power plant project site; Biman Bangladesh Airlines; Immigration, Bangladesh Police; Bangladesh Telecommunication Company Ltd; Power Grid Company of Bangladesh; Bangladesh Power Development Board; Power Grid Company of Bangladesh; Titas Gas Transmission and Distribution Company; Central Depository Bangladesh; Bangabandhu Satellite Company; Bangladesh Securities and Stock Exchange Commission; Civil Aviation Authority Bangladesh; Registrar General's Office, birth and death registration; and Dhaka and Chittagong Stock Exchange.

19 Star Digital Report, 'Looking Back at Aug 17, 2005 Series Bomb Blasts' *The Daily Star* (16 August 2022) <https://www.thedailystar.net/news/bangladesh/news/looking-back-aug-17-2005-series-bomb-blasts-3096396>;Arafat Amin, 'National Security or Infringement on Civil Rights?' [2006] *Law & Our Rights* <https://www.thedailystar.net/law/2006/05/01/index.htm>.

20 Bangladesh Telecommunication Act, Act No. XVIII of 2001.

21 Arafat Amin, Odhikar, 'Bangladesh Telecommunication (amendment) Ordinance, 2005: National Security or Infringement on Civil Rights?' <http://odhikar.org/wp-content/uploads/2012/09/Bangladesh-telecommunication-ordinance-Article-2006.pdf>.

22 The Penal Code, 1860 s 141.

23 Country Legal Framework Resources, Provision of Real-time Lawful Interception Assistance (2017) <https://clfr.globalnetworkinitiative.org/country/bangladesh/#:~:text=Under%20section%2097(Ka)%20BTRA,of%20any%20data%20or%20any>.

24 Bangladesh Telecommunication Regulatory Act, 2001 s. 97 (A).

25 The Bangladesh Telecommunication Regulatory Act 2001 <http://bdlaws.minlaw.gov.bd/act-details-857.html>.

In addition, the Government can order any service provider to provide assistance in a case. This includes any person or operator providing telecommunication service or operating a system in cyberspace. No limitations have been placed on the duration of such interception orders, and such information has been accepted as evidence in cases.[26]

Although the BTRA penalises eavesdropping on communications, the state security and public order exception within the framework allows section 97(A) to supersede the user's safeguard for the right to privacy.[27]

Article 43 of the Constitution recognises that the right to "privacy of correspondence and other means of communication" may be "subject to reasonable restrictions imposed by law in the interests of the security of the state, public order, public morality, or public health." Therefore, section 97(A) of the BTRA is an exception that enables LEAs to unquestionably intercept and monitor communications. However, it lacks adequate checks and balances to evaluate the proportionality and necessity of restrictions placed upon a user's constitutional right to privacy, especially given the lack of judicial oversight in interception orders.

4.2.3 Internet Shutdowns

The Bangladesh Telecommunication Regulatory Commission (BTRC) has in the past (i) suspended internet access;[28] (ii) slowed down internet access;[29] and (iii) blocked access to selected websites, including social media platforms.[30] The legal basis of such measures is not entirely clear.

Article 39(2) of the Bangladesh Constitution enables the government to impose restrictions on speech on the grounds of security and public order and to prevent other offences. The act of restricting access to the internet is often operationalised in the interest of state security or public order, but such restrictions are permissible only if they are clearly provided by law, have a legal basis, are necessary, and are proportional.

26 Arafat Amin, 'National Security or Infringement on Civil Rights?' [2006] *Law & Our Rights* <https://www.thedailystar.net/law/2006/05/01/index.htm>.

27 The Bangladesh Telecommunication Act, 2001 s. 71.

28 'Bangladesh Shuts Down the Internet, Then Orders Blocking of 35 News Websites' (*Global Voices*, 4 August 2016) <https://globalvoices.org/2016/08/04/bangladesh-shuts-down-the-internet-then-orders-blocking-of-35-news-websites/>.

29 Staff Correspondent, 'Mobile Net Slowed Down' *The Daily Star* (5 August 2018) <https://www.thedailystar.net/country/bangladesh-mobile-internet-speed-brought-down-across-for-24hrs-1615909>.

30 'Bangladesh 'blocks Facebook' over political cartoons' (BBC, 30 May 2010) <https://www.bbc.com/news/10192755 >.

Section 97(A) of the BTRA empowers the state to "suspend or prohibit the transmission of any data" in the interest of national security and public order.[31] The broad nature of section 97(A) and the lack of clarity surrounding its limitations indicate that the government might be relying on this section to order internet shutdowns. A broadly drafted provision like section 97(A), which does not impose any time limits for the authorised agencies to exercise powers or does not codify adequate safeguards, is susceptible to misuse for internet shutdowns.

Additionally, section 66(a) of the BTRA empowers the BTRC to ensure that operators comply with orders "to stop any signal, message, or request from any subscriber." This power can be exercised to ensure expedient blocking of services in the interest of the security of Bangladesh, public order, or for preventing incitement of a legally recognised offence.[32]

Due to these broad powers to restrict online services, Bangladesh is ranked 5th in the world on internet shutdowns, recording six shutdowns in 2022 alone.[33] Even before 2022, there were many notable internet shutdowns. For instance, in 2010, Facebook was banned for a week by the BTRC following a controversial religious post.[34] In 2012, YouTube was also blocked for hosting controversial religious videos to forestall the incitement of violence.[35]

In 2015, the BTRC banned Facebook, Viber, Whatsapp and other social messaging applications in response to a controversial Supreme Court ruling.[36] In August 2016, the BTRC conducted a series of "test shutdowns" in an "internet shutdown drill".[37]

31 Bangladesh Telecommunications (Amendment) Act, 2006 <http://www.btrc.gov.bd/sites/default/files/files/btrc.portal.gov.bd/law/5d2dae4a_6fe8_4240_9930_fe8ae9f22448/2022-02-05-19-27-f4102d8f3d4f6217daa08544b9c25beb.pdf> (only available in Bangla).

32 'Provision of Real-time Lawful Interception Assistance' (Country Legal Framework Analysis, 2018) <https://clfr.globalnetworkinitiative.org/country/bangladesh/>.

33 'Internet Shutdowns in 2022' (Access Now, 2022) <https://www.accessnow.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf>.

34 'Bangladesh 'blocks Facebook' over political cartoons' (BBC, 30 May 2010) <https://www.bbc.com/news/10192755 >.

35 Bangladesh blocks YouTube over anti-Islam video (Phys org, 18 September 2012) <https://phys.org/news/2012-09-bangladesh-blocks-youtube-anti-islam-video.html>.

36 'Bangladesh Keeps Blocking Social Media, Threatens New Surveillance Tactics' (*Global Voices*, 30 November 2015) <https://globalvoices.org/2015/11/30/bangladesh-keeps-blocking-social-media-threatens-new-surveillance-tactics/>.

37 'Bangladesh Shuts Down the Internet, Then Orders Blocking of 35 News Websites' (*Global Voices*, 4 August 2016) <https://globalvoices.org/2016/08/04/bangladesh-shuts-down-the-internet-then-orders-blocking-of-35-news-websites/>.

Various news reports allege that internet access has been frequently restricted and even cut off during opposition rallies in Bangladesh.[38]

In 2018, in response to student protests in Dhaka, LEA ordered the BTRC to deliberately restrict mobile internet speed to 2G levels for 24 hours.[39] This significantly reduced internet speed, impacted access to communication infrastructure, and limited online sharing. NetBlocks, a digital rights organisation, observed that the shutdown was aimed at suppressing the coverage of the protests.[40] Despite social media platforms not being entirely blocked, the slowdown hindered the user's ability to access news, upload audio-visual content to share live footage, and also affected the media coverage of disputed incidents.[41]

Employing internet restrictions during protests and opposition rallies like these raises several rule of law concerns about the impact on information dissemination during such an event.

4.3 Measures for Countering Terrorism

There are two main provisions for countering terrorism in Bangladesh – the Anti-Terrorism Act of 2009 (ATA) and Section 27 of the CSA (the cyberterrorism provision).

Section 27 of the CSA identifies offences in cyberspace, including intentional obstruction or illegal access to harm state integrity, causing harm through malware, disrupting CII, and accessing information detrimental to foreign relations.[42]

Section 6 of the ATA defines a list of terrorist activities, which include any act that threatens the "integrity, public security, or sovereignty of Bangladesh, disrupts the protection of the property of any foreign country, or creates panic among the general public".[43] In

38 'Global Report on Internet Shutdowns: Bangladesh Ranked 5th' (*Asia News Network*, 2 March 2023) <https://asianews.network/global-report-on-internet-shutdowns-bangladesh-ranked-5th/>.

39 Staff Correspondent, 'Mobile Net Slowed Down' *The Daily Star* (5 August 2018) <https://www.thedailystar.net/country/bangladesh-mobile-internet-speed-brought-down-across-for-24hrs-1615909>.

40 'Mobile Internet Speeds Restricted in Bangladesh amid Student Protests' (*NetBlocks*, 4 August 2018) <https://netblocks.org/reports/bangladesh-internet-shutdown-student-protests-jDA37KAW>.

41 Ibid.

42 CSA 2023, s 27(1).

43 ATA 2009, s 6(1).

trials for such terrorist activities, the courts may admit digital content such as videos, photographs, and audio clips from social media platforms such as Facebook, Twitter, and Skype as evidence.[44] Digital evidence can also be produced before the Cyber Tribunal as per section 56 of the CSA. Additionally, it is to be noted that in 2022, the definitions "digital record" and "electronic record"[45] have been inserted into section 3 of the Evidence Act, 1872.[46]

Additionally, the vagueness of section 27 under the CSA and the wide definition of 'terrorist activities' in the ATA may negatively impact fairness in application, legal certainty of such restrictions and pave the way for abuse of these provisions.[47] Laws that prohibit terrorist activities, whether at the national or international level, must be precise and easily accessible. Clear definitions of the elements constituting a terrorist offence and connected "terrorist acts" are essential. Anti-terrorist laws and associated powers should exclusively focus on combating terrorism, ensuring that non-terrorism-related behaviours, even when involving individuals suspected of terrorist activities, are not targeted by counterterrorism measures.[48]

Odhikar (a human rights organisation in Bangladesh) and the International Federation for Human Rights have reiterated that the definition of 'terrorist activities' embodies vague expressions incompatible with Article 15 of the ICCPR.[49] This broad law has enabled the state to abuse safeguards, criminalise social media posts and use them as evidence to determine terrorist activity.[50]

---

44 Ibid.

45 The amendment was brought by section 2(b) of the Evidence (Amendment) Act, 2022 According to this amendment, "digital record" or "electronic record" means any record, data or information generated, prepared, sent, received or stored in magnetic or electro-magnetic, optical, computer memory, micro film, computer generated microfiche including audio, video, Digital Versatile Disc or Digital Video Disc (DVD), records of Closed Circuit Television (CCTV), drone data, records from cell phone, hardware, software or any other digital device as defined in Digital Security Act, 2018 (Act No. 46 of 2018).

46 The Evidence Act No. 1 of 1872<http://bdlaws.minlaw.gov.bd/act-details-24.html>.

47 Laurie Berg, Mouloud Boumghar, Nymia Pimentel Simbulan, 'Bangladesh: Criminal Justice Through The Prism Of Capital Punishment And The Fight Against Terrorism,' (*International Federation for Human Rights*) <https://www.fidh.org/IMG/pdf/Report_eng.pdf> p 29.

48 Ibid; 'Human Rights, Terrorism and Counter-Terrorism' [2008] Office of the United Nations High Commissioner for Human Rights <https://www.ohchr.org/en/publications/fact-sheets/fact-sheet-no-32-terrorism-and-counter-terrorism#:~:text=Specifically%2C%20the%20Fact%20Sheet%20aims,compliance%20with%20human%20rights%20when>.

49 'Bangladesh: New Amendment To Anti-Terrorism Act Gags Freedom Of Expression' (*International Federation for Human Rights*, 2013) <https://www.fidh.org/en/region/asia/bangladesh/bangladesh-new-amendment-to-anti-terrorism-act-gags-freedom-of-expression-13457>.

50 Ibid.

4.4 Criminalisation of Online Speech

From September 2018 to January 2023, a total of 7,001 cases were filed under the DSA.[51] There are allegations and criticisms from civil society members that many of these cases primarily targeted individuals, restricting their right to free speech, dissent, and independent journalistic reporting.[52] Victims of these cases included opposition politicians, journalists, industry, students, and company employees, with ruling party affiliates being the prominent prosecutors, filing cases at an average rate of one per week.[53] Between January 2020 and February 2022, 2,244 individuals, including 254 politicians and 207 journalists, faced charges, with political party members, the Rapid Action Battalion (RAB), and government officials being the major accusers.[54] Roughly 5 cases were filed per day in the DSA's 52 month implementation as of June 2023.[55]

Due to challenges in transparency and accountability of the DSA, there is difficulty in obtaining accurate data from government sources. However, since January 2020 the Centre for Governance Studies (CGS) tracked 1,325 cases and 4,121 individuals accused under the DSA as of May 31, 2023.[56] The average number of people accused in each case is 3.11, and by extrapolating from the sample, it is estimated that at least 21,770 people could have been accused under the DSA.[57]

51 UNB, 'Over 7,000 Cases Filed under DSA: Law Minister | *The Business Standard*' *The Business Standard* (5 June 2023) <https://www.tbsnews.net/bangladesh/over-7000-cases-filed-under-dsa-law-minister-644486>.

52 Ali Riaz, 'How Bangladesh's Digital Security Act Is Creating a Culture of Fear' (*Carnegie Endowment for International Peace*, 9 December 2021) <https://carnegieendowment.org/2021/12/09/how-bangladesh-s-digital-security-act-is-creating-culture-of-fear-pub-85951>.

53 Ali Riaz, 'How Bangladesh's Digital Security Act Is Creating a Culture of Fear' (*Carnegie Endowment for International Peace*, 9 December 2021) <https://carnegieendowment.org/2021/12/09/how-bangladesh-s-digital-security-act-is-creating-culture-of-fear-pub-85951>.

54 Ali Riaz, 'How Bangladesh's Digital Security Act Is Creating a Culture of Fear' (*Carnegie Endowment for International Peace*, 9 December 2021) <https://carnegieendowment.org/2021/12/09/how-bangladesh-s-digital-security-act-is-creating-culture-of-fear-pub-85951>; Ali Riaz, 'What the Law Minister's DSA Statement Reveals' *The Daily Star* (7 June 2023) <https://www.thedailystar.net/opinion/views/black-white-grey/news/what-the-law-ministers-dsa-statement-reveals-3340211>.

55 'What the Law Minister's DSA Statement Reveals | DSA Tracker' (7 June 2023) <https://freedominfo.net/content-details/6325>.

56 'What the Law Minister's DSA Statement Reveals | DSA Tracker' (7 June 2023) <https://freedominfo.net/content-details/6325>.

57 Ali Riaz, 'What the Law Minister's DSA Statement Reveals' *The Daily Star* (7 June 2023) <https://www.thedailystar.net/opinion/views/black-white-grey/news/what-the-law-ministers-dsa-statement-reveals-3340211>.

One in three individuals facing DSA charges experienced arrest, and 60% of the cases were related to the user's Facebook activity.[58] It has also been reported that only 2% of the cases under DSA saw resolution in court, leaving the fate of the majority uncertain.[59]

In August 2023, the government decided to amend the DSA due to the widespread concerns related to the misuse of its provisions for placing restrictions on freedom of expression and human rights.[60] Before introducing the amendments to the DSA, it had been globally criticised by various UN officials, diplomats, and international human rights organisations for the wide powers to block content, impose criminal penalties and investigate without warrant.[61] Volker Türk, the United Nations High Commissioner for Human Rights[62] and Irene Khan, the UN Special Rapporteur on the situation of human rights in Bangladesh,[63] urged Bangladesh to cease the misuse of the DSA and repeal the law. Similarly, critics expressed concerns over its application and emphasised the need for legal measures that align with international human rights standards and foster freedom of expression.[64]

58 Zyma Islam, 'Cases Under DSA: Almost All Accused Kept Hanging' *The Daily Star* (15 January 2023) <https://www.thedailystar.net/news/bangladesh/news/cases-under-dsa-almost-all-accused-kept-hanging-3221031>.

59 Ibid.

60 'The Government of Bangladesh Quietly Passed the New Cyber Security Act 2023' (*Global Voices*, 19 September 2023) <https://globalvoices.org/2023/09/19/the-government-of-bangladesh-quietly-passed-the-new-cyber-security-act-2023/>.

61 See Access Now, 'New Digital Security Act in Bangladesh deepens threats to free expression'(2018) <https://www.accessnow.org/press-release/new-digital-security-act-in-bangladesh-deepens-threats-to-free-expression/>; 'No Place for Criticism : Bangladesh Crackdown on Social Media Commentary' (Human Rights Watch 2018) <https://www.hrw.org/report/2018/05/10/no-place-criticism/bangladesh-crackdown-social-media-commentary>; Forum for Freedom of Expression, Bangladesh, 'Cyber Security Act Will Not Stop Criminalising Freedom of Expression' *The Daily Star* (13 August 2023) <https://www.thedailystar.net/opinion/views/news/cyber-security-act-will-not-stop-criminalising-freedom-expression-3393326>; Diplomatic Correspondent, 'Revise Digital Security Act' *The Daily Star* (10 October 2018) <https://www.thedailystar.net/country/digital-security-act-2018-revise-un-1644727>.

62 Zyma Islam, 'DSA Amendment: A Promise That Rings Hollow' *The Daily Star* (18 April 2023) <https://www.thedailystar.net/news/bangladesh/news/dsa-amendment-promise-rings-hollow-3299366>.

63 SM Najmus Sakib and Md. Kamruzzaman, 'UN Human Rights Chief Urges Bangladesh to Halt Abuse of Digital Law' *Anadolu Ajansı* (Dhaka, 31 March 2023) <https://www.aa.com.tr/en/asia-pacific/un-human-rights-chief-urges-bangladesh-to-halt-abuse-of-digital-law/2860642>.

64 See OHCHR, 'OHCHR Technical Note to the Government of Bangladesh on review of the Digital Security Act' (June 2022) <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf>; Zyma Islam, 'DSA Amendment: A Promise That Rings Hollow' *The Daily Star* (18 April 2023) <https://www.thedailystar.net/news/bangladesh/news/dsa-amendment-promise-rings-hollow-3299366>.

Digital Rights groups called for a comprehensive review of the DSA to address issues related to arbitrary arrests, harassment, and stifling of dissent.[65] Perhaps such huge and multifaceted criticism against the DSA propelled the government to introduce CSA.

While introducing the CSA, the law minister announced that the government has transformed the DSA by incorporating necessary amendments to prevent abuse.[66] However, the introduction of CSA has also been met with similar criticisms.[67] For instance, Irene Khan expressed concern that the recommendations of the United Nations High Commissioner for Human Rights regarding the DSA have not been incorporated into the CSA.[68] Critics also argue that the CSA continues to retain overly broad and vague offences, potentially allowing for misuse by authorities to suppress journalistic reportage and political dissent.[69] Although the DSA has been amended to reduce imprisonment for certain offences, the CSA replaces it with severe financial penalties in some sections that can still be misused against journalists or political dissenters.[70]

The CSA outlines the following key changes to the DSA:

1. CSA has expanded the power of LEAs to conclude investigations of offences under the DSA from a 60-day limit to 90 days in section 39.
2. The CSA removed jail terms for offenders of defamation.71 However, the scope of imprisonment under the penal code remains unclear, and the fines for posting or transmitting defamatory content have been significantly increased, from an upper limit of taka 5 lakhs to taka 25 lakhs.

65 *Freedom House*, 'Freedom on the Net 2021' (2021) <https://freedomhouse.org/country/bangladesh/freedom-net/2021#footnote1_n6eghjo>.

66 Star Digital Report, 'Govt Decides to "Transform" DSA into "Cyber Security Act"' *The Daily Star* (7 August 2023) <https://www.thedailystar.net/news/bangladesh/news/govt-decides-transform-dsa-cyber-security-act-3388526>.

67 Shaikh Azizur Rahman, 'Bangladesh Criticized Over Plan to Replace Controversial Law with One Considered Equally Repressive' *Voice of America* (21 August 2023) <https://www.voanews.com/a/bangladesh-criticized-over-plan-to-replace-controversial-law-with-one-considered-equally-repressive-/7234227.html>.

68 Star Digital Report, 'UN Rights Body's Recommendations on DSA Not Reflected in CSA: Irene Khan' (*The Daily Star*, 31 August 2023) <https://www.thedailystar.net/law-our-rights/news/un-rights-bodys-recommendations-dsa-not-reflected-csa-irene-khan-3407816>.

69 Bangladesh Legal Aid and Services Trust, 'Comments by BLAST on the Cyber Safety Act, 2023 (Draft)' (2023) <https://www.blast.org.bd/content/judgement/Comments-by-BLAST-on-the-Cyber-Safety-Act-2023-(Draft).pdf>.

70 See Rezaur Rahman Lenin and Nowzin Khan, 'From DSA to CSA: The Same Two Bottles of Agony' *The Daily Star* (26 August 2023) <https://www.thedailystar.net/opinion/views/news/dsa-csa-the-same-two-bottles-agony-3403566>; Transparency International Bangladesh, 'Digital Security Act 2018 and the draft Cyber Security Act 2023 : A Comparative Analysis' (2023) <https://www.ti-bangladesh.org/upload/files/position-paper/2023/Position-paper-on-Digital-Security-Act-2018-and-Draft-Cyber-Security-Act-2023.pdf>.

3. Various sections of the CSA are now bailable and non-cognizable offences. For example, under the DSA, fourteen sections (sections 17, 19, 21, 22, 23, 24, 26, 27, 28, 30, 31, 32, 33, and 34) were deemed cognisable and non-bailable. However, under CSA out of the 14 offences, only 3 remain as cognisable and non-bailable.[72]

4. Section 57, which enabled LEA and the government to take '*suo moto*' action in good faith, has been omitted from the CSA.

5. Finally, jail terms for various offences have also been reduced.[73]

The key significance of the amendment can be outlined through the reduction of the number of non-bailable offences, given that the number of pre-trial detainees in jails and the lack of fast-track courts was a significant issue under the DSA. Misuse of non-bailable offences has historically resulted in numerous individuals being held as pre-trial detainees, contributing to overcrowded jails without getting court dates within 60 days.[74] The case of *Mushtaq Ahmed*, an author who died in jail in February 2022 after ten months of detention and six denied bail applications, underscores the serious implications of such provisions.[75]

However, the DSA has not been significantly amended, safeguards against excessive power have not been introduced, and the content-based offences are still vaguely defined, which continues to raise fears of arbitrary application.[76] Criticism has been directed at the lack of safeguards and checks and balances, emphasising the need for clear limitations on state powers to prevent discretion and abuse.[77]

71 Star Digital Report, 'Cyber Security Act: Only Fine, No Jail Time for Defamation' *The Daily Star* (7 August 2023) <https://www.thedailystar.net/news/bangladesh/news/cyber-security-act-only-fine-no-jail-time-defamation-3388541>.

72 Transparency International Bangladesh, 'Digital Security Act 2018 and the draft Cyber Security Act 2023 : A Comparative Analysis' (2023) <https://www.ti-bangladesh.org/upload/files/position-paper/2023/Position-paper-on-Digital-Security-Act-2018-and-Draft-Cyber-Security-Act-2023.pdf>.

73 Ibid.

74 Ali Riaz, 'What the Law Minister's DSA Statement Reveals' *The Daily Star* (7 June 2023) <https://www.thedailystar.net/opinion/views/black-white-grey/news/what-the-law-ministers-dsa-statement-reveals-3340211>.

75 Ibid.

76 See Tribune Desk, 'Cyber Security Act Draft Gets Cabinet Nod' *Dhaka Tribune* (28 August 2023) <https://www.dhakatribune.com/bangladesh/323766/cyber-security-act-draft-gets-cabinet-nod>;Transparency International Bangladesh, 'Digital Security Act 2018 and the draft Cyber Security Act 2023 : A Comparative Analysis' (2023) <https://www.ti-bangladesh.org/upload/files/position-paper/2023/Position-paper-on-Digital-Security-Act-2018-and-Draft-Cyber-Security-Act-2023.pdf>.

77 Shaikh Azizur Rahman, 'Bangladesh Criticized Over Plan to Replace Controversial Law with One Considered Equally Repressive' *Voice of America* (21 August 2023) <https://www.voanews.com/a/bangladesh-criticized-over-plan-to-replace-controversial-law-with-one-considered-equally-repressive-/7234227.html>.

Additionally, the lack of stakeholder consultations and the imposition of stringent penalties, including imprisonment for certain offences, is deemed disproportionate and inconsistent with international human rights standards.[78] Civil Society organisations have called for a comprehensive review and revision of the CSA to address these concerns and ensure compliance with democratic principles and human rights.[79]

The CSA continues to enumerate several speech offences, most of which contain terms that are vague and overbroad, as noted earlier. They are mentioned below:

- Section 21 criminalises "any propaganda or campaign against the liberation war of Bangladesh, spirit of liberation war, national anthem, or national flag." It is important to note that this section does not define the meaning of terms like "propaganda", "campaign", or "spirit of liberation war."

- Similarly, section 25 of the CSA considers the transmission of offensive, false, or threatening online information, with the aim of humiliating or harming a person's reputation or engaging in propaganda to damage the country's image, as an offence.[80] Amongst the widespread criticism of the DSA, a High Court Division had called upon the government to show cause as to why the provision of section 25 of the DSA (now CSA) should not be declared unconstitutional and violative of Article 39 of the constitution.[81]

- Section 29 of the CSA, punishes individuals who publish or transmit defamatory information through digital platforms, with penalties including a fine up to twenty-five lakhs Taka. Earlier, under the DSA, there was a jail term for disseminating such content, which has now been removed.[82] While introducing the CSA, the law

78 US Embassy in Bangladesh, 'U.S. Embassy Statement on the Passage of the Cyber Security Act' (2023) <https://bd.usembassy.gov/30390/>.

79 See Mubashar Hasan, 'Bangladesh Government Scraps Controversial Digital Security Act' (*The Diplomat*, 21 August 2023) <https://thediplomat.com/2023/08/bangladesh-government-scraps-controversial-digital-security-act/>;Kamal Ahmed, 'Relabelling the DSA Won't Protect Citizens from Cybercrimes' *The Daily Star* (21 August 2023) <https://www.thedailystar.net/opinion/views/news/relabelling-the-dsa-wont-protect-citizens-cybercrimes-3399621>.

80 CSA, 2023 s 25 (1) (a).

81 'DSA: HC Asks Govt Why 2 Sections Aren't Unconstitutional' (*The Daily Star*, 2020) <https://www.thedailystar.net/country/digital-security-act-2018-why-2-sections-arent-unconstitutional-1872358>.

82 Star Digital Report, 'Cyber Security Act: Only Fine, No Jail Time for Defamation' *The Daily Star* (7 August 2023) <https://www.thedailystar.net/news/bangladesh/news/cyber-security-act-only-fine-no-jail-time-defamation-3388541>.

minister emphasised that the misuse of the DSA against journalists or users will be addressed through the reduction of non-bailable offences and elimination of jail time for defamation.[83] However, as noted earlier, the scope of imprisonment under criminal defamation provisions of the penal code still remains unclear.

In the case of *Bangladesh Legal Aid Services Trust vs. State*, the Supreme Court held that a law which prohibits any right must be clear and precise.[84] Several critics continue to argue the expressions mentioned under section 29 (online criminal defamation) of the DSA and now the CSA are vague and unclear. Thus, it is not possible to determine which acts constitute defamation and which are prohibited.[85]

Additionally, the CSA has also been criticised as it fails to adequately protect citizens from cybercrimes and still needs substantive reforms to ensure the law aligns with international human rights standards and safeguards freedom of expression.[86]

Finally, section 43 of the DSA empowered LEAs to arrest without warrant if they had reasons to believe that an offence under the act had been committed.[87] Furthermore, the DSA provided that these authorities shall not be subject to any suit or prosecution for actions taken in good faith.[88] For context, from January 2020 to October 2021, 754 cases were filed under the DSA against 1841 individuals.[89] Most of these cases were filed by LEAs,[90] as section 43 of the DSA empowered them to arrest anyone if they believed that a violation of the DSA had occurred or was likely to occur.[91] While the CSA revokes the authorities' protection from prosecution for actions taken in good faith,[92] section 42

83 Ibid.

84 *Bangladesh v Bangladesh Legal Aid Services Trust* (2008) 8 SCOB 1.

85 Ananya Azad, 'DSA In Bangladesh : The Death Of Dissent And Freedom Of Expression' (2021) <https://www.etd.ceu.edu/2021/azad_ananya.pdft>.

86 Kamal Ahmed, 'Relabelling the DSA Won't Protect Citizens from Cybercrimes' *The Daily Star* (21 August 2023) <https://www.thedailystar.net/opinion/views/news/relabelling-the-dsa-wont-protect-citizens-cybercrimes-3399621>.

87 DSA, 2018, s 43(1).

88 DSA, 2018, s 57. This section has been omitted in the CSA.

89 Ali Riaz, 'How Bangladesh's DSA Is Creating A Culture Of Fear' (*Carnegie Endowment for International Peace*, 2021) <https://carnegieendowment.org/2021/12/09/how-bangladesh-s-digital-security-act-is-creating-culture-of-fear-pub-85951>.

90 Ibid.

91 CSA, 2023 s 43(1).

92 DSA, 2018 s 57 (now repealed).

continues to provide a blanket power to conduct investigations without a warrant.[93] This allows LEAs to conduct ad-hoc search, seizure and arrest without due process rights like a warrant and further exempts them from any judicial review.

4.5 Bangladesh's Approach to Regulating Social Media Platforms

4.5.1 Safe Harbour Protection

Under section 37 of the CSA, Service Providers comprise entities that enable users to communicate through digital means or entities that process user data to provide a digital service.[94] They are exempted from any liability for hosting user-generated content provided that the offence is committed without their knowledge and the service providers have exercised all due diligence to prevent the offence.[95]

Similarly, the ICTA codifies clauses regarding non-liability and due diligence requirements. Section 79 of the ICTA provides that no network service provider shall be liable for any third-party information or data available from them if such provider proves that the flow of information or data falling under an offence or contravention was committed without their knowledge or that they exercised due diligence to prevent the commission of such a crime.[96, 97]

Although both legislations have similar clauses, there are multiple issues with extending these provisions to social media platforms. Neither the provisions under the CSA nor the ICTA define intermediary in a broader sense, and the interpretation of 'addressee',[98] or

93 Tasnim Binte Maksud, 'What Does the Proposed Cyber Security Act Offer?' *The Daily Star* (8 September 2023) <https://www.thedailystar.net/law-our-rights/news/what-does-the-proposed-cyber-security-act-offer-3413691>.

94 CSA, 2023 s(2).

95 CSA 2023, s 37.

96 ICTA 2006, s 79 Network service providers not to be liable in some instances.—For the removal of doubts, it is at this moment declared that no person providing any service as a network service provider should be liable under this Act, or rules and regulations made thereunder, for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised due diligence to prevent the commission of such offence or violation.

97 ICTA 2006, s 79 Explanation. —For the purposes of this section, – (a) "network service provider" means an intermediary; (b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

98 ICTA 2006, s 2(21) "addressee" with reference to data message means a person intended by the originator to receive the electronic record but does not include any intermediary.

'originator',[99] which concerns the data message, does not include intermediaries. Both the legislations are also silent regarding electronic messages.[100]

Furthermore, these Acts, as well as the Rules framed thereunder, do not explain the nature of the due diligence requirements that intermediaries need to follow to qualify for safe harbour protection.

4.5.2 Digital Content Takedown

Chapter III of the CSA, titled '*Preventive Measures*', lays down the power to remove or block any information published on digital media. Section 8 (1) of the CSA gives the Director General discretionary power to request the BTRC to remove or block any published information which creates a threat to cyber security.[101] The terms 'digital security' used in the DSA and 'cyber security' used in the CSA are loosely defined as the "security of a digital device or digital systems"[102] and "security of a digital device, computer or computer system",[103] leaving them open to interpretation and abuse.

Further, section 8(2) of the CSA empowers law and order forces like the Police and Rapid Action Battalion (RAB) to request the BTRC to remove or block any information that "*hampers the solidarity, financial activities, security, defence, religious values or public discipline of the country or any part thereof, or incites racial hostility and hatred*".

Furthermore, the Draft OTT Policy 2021, if passed, would establish due diligence obligations to adhere to content takedowns.[104]

99 ICTA 2006, s 2(23) originator with reference to data message means a person who sends or prepares data message before preservation or causes any date message to be sent, generated, stored, or transmitted but does not include an intermediary.

100 S.M. Shakib and Noor Afrose, 'Intermediary Liability on the Internet: Adequacy of Bangladesh's Legal Framework on Cyber Crime' (2021) SCLS Law Review Vol. 4. No.3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4056523>.

101 CSA 2023, s 8(1).

102 DSA 2018, s 2(1)(k).

103 CSA 2023, s 2(1)(v).

104 'Bangladesh: Freedom on the Net 2023 Country Report' (*Freedom House*, 2023) <https://freedomhouse.org/country/bangladesh/freedom-net/2023>.

In the past, the Bangladesh government has blocked access to hundreds of news websites for publishing "anti-state news."[105] The BTRC has also reported that "over 8000 Bangladeshi social media links were removed by the government in 2022".[106] The BTRC has sent content removal requests to Facebook, Google, TikTok, and Twitter, and it was reported that BTRC had sent Twitter and Facebook requests to takedown posts by whistleblowers and journalists for critiquing the government.[107, 108]

However, there is not much clarity on the legal framework and the procedure followed by the government to block access to content.[109] The lack of transparency also means that there is no clarity on the number of content-blocking orders being issued by the government. This leaves enough scope for censorship and abuse.

4.5.3 Emerging Trends in Social Media Governance

The government is planning to overhaul the internet and social media governance frameworks. To do so it has proposed two laws. These are (i) the Draft OTT Policy 2021(either the Bangla draft by MIB or the English draft by the BTRC) and (ii) proposed amendments to the BTA.

Section 2.01 (k) of the Draft OTT policy (proposed by the BTRC) provides that any content, service, or application provided to an end-user falls under the definition 'OTT'.[110] This vague definition in the proposed draft can also cover different services, notably media, communication, and social media, thus making it applicable to the various services.[111]

105 AFP, 'Bangladesh Orders 191 "anti-State" News Sites Blocked' (The Hindu, 31 January 2023) <https://www.thehindu.com/news/international/bangladesh-orders-191-anti-state-news-sites-blocked/article66454856.ece>.

106 Toggle Desk, 'Govt Removed over 8,000 Social Media Links in 2022: Report' (*The Daily Star*, 14 October 2022) <https://www.thedailystar.net/tech-startup/news/govt-removed-over-8000-social-media-links-2022-report-3142356>.

107 Twitter Correspondence with Users Reveals Bangladesh Government Attempts to Remove Tweets' (*Netra News* — নেত্র নিউজ, 3 December 2022) <https://netra.news/2022/twitter-correspondence-with-users-reveals-bangladesh-government-attempts-to-remove-tweets/>.

108 'Concerted Attacks against Bangladeshi Activists on Facebook' (*Global Voices*, 8 February 2022) <https://globalvoices.org/2022/02/08/concerted-attacks-against-bangladeshi-activists-on-facebook/>.

109 'Bangladesh: Freedom on the Net 2023 Country Report' (*Freedom House*, 2023) <https://freedomhouse.org/country/bangladesh/freedom-net/2023>.

110 Draft Regulation for Digital, Social Media and OTT Platforms, 2021, Section 2.01 (k) defines 'OTT' as content, a service, or an application that is provided to the end-user over the public internet.

111 Asia Internet Coalition (AIC) Comments on Bangladesh Telecommunication Regulatory Commission Regulation for Digital, Social Media and OTT Platforms, 2021 ("Draft Regulation") (Asia Internet Coalition, 4 March 2022) <https://aicasia.org/wp-content/uploads/2022/03/Asia-Internet-Coalition-AIC-Comments-on-Bangladesh-Telecommunication-Regulatory-Commission-Regulation-for-Digital-Social-Media-and-OTT-Platforms-2021-Draft-Regulation.pdf>.

Moreover, an intermediary, including a social media intermediary, has been obliged to discharge a wide range of duties under the draft. As per section 6.01, an intermediary is bound to provide information about its users upon receiving an order from the concerned authority - "to verify the identification, prevent, detect, or address any offences under any law or for cyber security concerns".[112] Intermediaries are required to comply with government orders seeking user data within a 72-hour timeline. Given the above-mentioned obligation, different social media platforms such as Facebook and Twitter will be bound to provide user data to the government.

The aforementioned time limit may lead to arbitrary decision-making and infringement of due process, and intermediaries may engage in over-removal erring on the side of caution.[113] Additionally, under section 7(5), all social media platforms have institutional obligations to set up an office with a physical address in Bangladesh. However, the punishment for refusing registration is not mentioned and allows for government discretion. Thus, the government will also hold unequal power over compliance with these provisions, especially in the case of smaller social media platforms, as they might not be able to afford local offices in Bangladesh.

Furthermore, the proposed draft by the BTRC does not distinguish between 'intermediary' and 'social media intermediary'. This may unintentionally bring OTT platforms such as Bioscope, Bongo, Chiaki, and Binge within the ambit of the regulation.[114] Moreover, unlike the CSA and the ICTA, the proposed draft lacks a safe harbour protection clause, which may pave the way for increased censorship of speech on digital platforms.[115]

Moreover, the power of the registration authority to direct OTT authorities to ban content violates the principle of natural justice. The registration authority, i.e. MIB, has a broad scope for arbitrary treatment.

112 See Draft OTT Policy, s 6.01, "An intermediary, including social media intermediary, shall observe the following activities while discharging its duties, name the intermediary shall, as soon as possible, but not later than seventy two hours of the receipt of an order, provide information under its control or possession, or assistance to the Government or its agency which is lawfully authorised for investigative or protective or cyber security activities, for verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents: Provided that any such order shall be in writing stating clearly the purpose of seeking information or assistance, as the case may be."

113 Letter to the Bangladesh Telecommunication Regulatory Commission: withdraw the Regulation for Digital, Social Media, and OTT Platforms (Access Now, 7 March 2022) <https://www.accessnow.org/bangladesh-digital-social-media-ott-platforms-regulation-letter/>.

114 Draft OTT Policy 2021, s 7.

115 Draft OTT Policy 2021, s 9.

4.6 Institutional and Administrative Landscape

Various bodies work in different sectors in Bangladesh from the perspective of cyberspace, cybersecurity, and social media. For example, the ICT Division supervises the ICTA's requirements. The ICT Division also coordinates with the cybersecurity division of the police under the Ministry of Home Affairs to enforce concerned individuals' privacy rights and data security under the ICTA.

Additionally, there are other authorities and agencies. For example, the CSA 2023 mandates the establishment of various bodies, i.e. The National Cyber Security Council (formed under section 12), the National Cyber Security Agency (formed under section 5), and the National Computer Emergency Response Team (formed under section 9). The CSA also established a Digital Forensic Lab under section 10. In contrast, the ICTA establishes the Office of the Controller of Certifying Authorities (CCA)—a department within the ICT Division.

Several Cyber Tribunals have been established under the ICTA. To date, there are eight tribunals: Cyber Tribunal, Dhaka; Cyber Tribunal, Chattogram; Cyber Tribunal, Rajshahi; Cyber Tribunal, Khulna; Cyber Tribunal, Barishal; Cyber Tribunal, Sylhet; Cyber Tribunal, Rangpur, and Cyber Tribunal, Mymensingh.[116]

The institutional framework of key bodies has been presented in the following table:

Name of the Body	Functions
Bangladesh e-Government Computer Incident Response Team	▪ Manage cyber security in Bangladesh government's e-Government network and related infrastructure. ▪ Serve as a catalyst in organising national cybersecurity resilience initiatives (education, workforce competence, regulation, cyber exercises) among various stakeholders. ▪ Make efforts to establish national cyber security incident management capabilities in Bangladesh.

116 Star Digital Report, 'Cyber Tribunals Set up by Govt in 8 Divisions' (*The Daily Star*, 6 April 2021) <https://www.thedailystar.net/law-our-rights/law-news/news/cyber-tribunals-set-govt-8-divisions-2073209>.

▪ **Cyber Police Centre, CID;**[117] ▪ **Police Cyber Support for Women (PCSW),**[118] **By Police Headquarters** ▪ **CT-Cyber Crime Investigation under the Counter Terrorism and Transnational Crime (CTTC) of DMP**[119]	▪ Counter-terrorism in cyberspace ▪ Patrol, prevent, detect, and investigate cyber-terrorism and cyber-crime.
Cyber Tribunals	Established under Section 68(1) of the ICT Act. They hear offences committed under ICTA and CSA
National Human Rights Commission, Bangladesh	To handle complaints relating to allegations of human rights violations, which include incidents arising from social media usage and in the cyber sphere
Bangladesh Telecommunication Regulatory Commission (BTRC)	▪ BTRC has the responsibilities under the BTA to implement best practices of the online telecommunication platform, address security concerns in terms of customer protection, national security, and regulate online content as mandated in BTA 2001. ▪ BTRC is empowered to block access to content and suspend the internet (see sections 4.2.3 and section 4.5.2)
National Cyber Security Council	▪ National Cyber Security Agency shall be established under the CSA[120] and will comprise of a Director General and two Directors.[121] It is the apex authority tasked with the enforcement of the CSA

117 Cyber Police Centre, CID< https://www.facebook.com/cpccidbdpolice>.

118 Police Cyber Support for Women< https://www.facebook.com/PCSW.PHQ>.

119 CT-Cyber Crime Investigation < https://www.cttcdmp.gov.bd/what-we-do/ct-cyber-crime-investigation>.

120 This shall replace the corresponding Digital Security Agency established under the DSA.

121 Cyber Security Act 2023 s 5.

	▪ The Director General should be an expert in computer or cyber security appointed by the Government, and his employment terms will be decided by the Government.[122] ▪ The Agency is tasked with monitoring and inspection of the safety of CIIs and is permitted to enter, search, examine, or suggest security measures at designated infrastructure, request compliance reports, and perform digital security audits.[123] ▪ The Director General is empowered to request the BTRC to block access to content that violates "cyber security"(earlier "digital security") under preventive measures.[124]
National Cyber Security Agency	▪ National Cyber Security Council shall be established under the CSA[125] and comprises of the Prime Minister as the Chairman and several ministers, departmental secretaries, law enforcement and intelligence officials as its members.[126] ▪ The Council is empowered to provide necessary directions and advice to the National Cyber Security Agency for the implementation of the CSA. To that end, it should fulfil the following:[127] ❐ Provide necessary directions for remedy if digital security is under threat. ❐ Advice on infrastructural development and human resource management for digital security ❐ Formulate inter-institutional policies for digital security

122 Cyber Security Act 2023 s 6.
123 Cyber Security Act 2023 s 16.
124 Cyber Security Act 2023 s 8(1).
125 This shall replace the corresponding National Digital Security Council established under the DSA.
126 Cyber Security Act 2023 s 12.
127 Cyber Security Act 2023 s 13.

Digital Forensic Lab	▪ Digital forensic labs are under the control and supervision of the National Cyber Security Agency (NCSA). ▪ The Digital Forensic Lab offers expert forensic advice used as judicial evidence in court. It also offers forensic support to investigating agencies regarding cybercrime and digital evidence. ▪ The seven BSTI and ISO standards in Section 14(1) of the Digital Security Rules 2020 were mentioned for case management, laboratory analysis, and quality assurance of all digital forensic cases. However, the rules for the Cyber Security Act 2023 have not been enacted yet.
National Computer Emergency Response Team	▪ The CSA mandates the creation of the National Computer Emergency Response Team under the National Cyber Security Agency.[128] ▪ It is tasked with the following functions:[129] ❐ Ensuring the emergency security of critical information infrastructure. ❐ Acting quickly to prevent "cyber or digital attacks" and "cyber or digital security breaches". ❐ Taking the necessary precautions to thwart potential and impending cyber or digital attacks. ❐ Carrying out all cooperative activities, including sharing information with a comparable foreign team or organisation, with the consent of the relevant foreign authority.

128 Cyber Security Act 2023 s 9.

129 Cyber Security Act 2023 s 9(5).

4.7 Legal Remedies

Section 68(1) of the ICTA empowers the government to create cyber courts, also known as tribunals, by gazette notification to prosecute offences swiftly. The Government must create Cyber Appellate Tribunals (CAT) by notification in the Official Gazette, according to section 82(1) of the ICTA. The tribunal must issue its ruling under section 72(1) of the ICTA within ten days following the completion of witness or evidence examination, hearing, or both. The tribunal must provide a written justification if it extends the deadline by less than ten days maximum. The court must issue a ruling within six months of the case's filing, according to section 73(1) of the Act. A written three-month extension can be requested if the judge cannot complete the case by the deadline according to section 73(2) of ICTA. If the judge doesn't finish on time, they can extend the case by explaining the delay in writing to the high court and controller according to section 73(3) of ICTA.

Crimes under section 57 of the ICTA have been incorporated in several areas of the DSA (and now CSA). These concern the publication of propaganda against the liberation war and the national anthem and national flag;[130] false, offensive, threatening information;[131] defamatory information;[132] and deteriorating law and order.[133] Section 57 of ICTA was repealed by section 61(1) of DSA. Section 61(2) of DSA said that section 57 of ICTA would not be deemed repealed if any proceeding is already taken or any case is under trial in the Cyber Tribunal. Now, the DSA is already repealed by the CSA. Nonetheless, trials and investigations of cases under the repealed sections of DSA will continue as per sections 59(2) and 59(3) of CSA as if DSA has not been repealed for the purposes of trials and investigations.

130 CSA 2023, s 21.
131 CSA 2023, s 25.
132 CSA 2023, s 29.
133 CSA 2023, s 31.

4.8 Forthcoming Developments

4.8.1 Draft Regulation for Digital, Social Media and OTT Platforms

The English draft policy authored by the BTRC, is titled the "Regulation for Digital, Social Media and OTT Platforms, 2021" (Draft OTT Policy) contains an extensive list of vaguely worded "prohibited content", which can result in unreasonable restrictions placed on freedom of speech in Bangladesh. Provisions under the policy can be misused to impose discretionary limitations on content creators.

Furthermore, the Draft OTT Policy bans content that goes against the spirit of the "Liberation War", the country's culture and social values, the harmony between groups, the unity of the state, and the law, the Constitution, or other rules. Section 2(5) lists 'banned contents' which go against the 'spirit of the Liberation War', destroy communal harmony, and threaten public order and integrity. These terms have not been defined or clarified further, leaving scope for ambiguity, confusion, and potential misuse.

According to Section 1(3) of the Draft OTT Policy, every organisation relevant to the ecosystem is bound to comply with this policy. This means that every internet service provider has to abide by this policy. Such a blanket policy restricts freedom of thought, conscience, and speech.

Section 14 states that the registration authority can order the OTT authority to remove any banned content from the OTT platform. The OTT authority will be bound to comply with such an order. Moreover, LEAs will provide all kinds of support to the registration authority regarding such orders. However, this section does not afford the OTT platform any opportunity to show cause or to defend itself. This violates the principle of natural justice, and there is a broad scope for arbitrary treatment by the registration authority, i.e. MIB.

Section 17(2) states that foreign organisations can own OTT platforms while foreign individuals are excluded from doing so. On the other hand, Section 17(1) allows Bangladeshi organisations and individuals to gain ownership of OTT platforms. The draft policy imposes more onerous conditions for ownership. Section 17(4) mentions that any individual

or organisation who has been penalised for any criminal offence cannot be eligible to own an OTT platform. However, this section does not mention which criminal offences fall within the scope of this policy. The Draft OTT Policy also requires a foreign platform to get clearance from the MHA and MFA before registering with MIB.

Section 15 of the draft policy provides self-regulation guidelines. However, the long list leaves little scope for actual self-regulation. Instead, the policy controls the ecosystem in the name of self-regulation. Nothing is mentioned about any appellate authority, where an OTT platform can appeal against refusal of registration.

MIB submitted a revised draft titled "Over the Top (OTT) Content-base Service Provide and Operations Policy-2022"(Proposed OTT policy by MIB) Policy to the High Court on January 8, 2023. The revised draft has proposed the following provisions:[134]

- It has increased the earnest money (security deposit) amounts for Bangladeshi platforms from Tk 5 lakh to Tk 15 lakh and foreign platforms from Tk 25 lakh to Tk 45 lakh.[135]
- 50 per cent of the material on foreign platforms must be "local," and they must establish an office in Bangladesh.[136]
- For local platforms, the five-year registration price has increased from TK 5 lakh to TK 10 lakh, while for overseas platforms, it has increased from TK 20 lakh to TK 35 lakh.[137]
- Each piece of content must be rated according to its acceptability for different audiences[138] and the age of the audiences.[139]
- There must be a parental lock to stop children from watching content that receives a mature rating.[140]

134 Ashutosh Sarkar and Mahmudul Hasan, 'OTT Regulation: Revised Draft Bans a Whole Lot of Content' (*The Daily Star*, 9 January 2023) <https://www.thedailystar.net/news/bangladesh/news/ott-regulation-revised-draft-bans-whole-lot-content-3215876>.

135 Section 6(2) of the proposed OTT policy by MIB.

136 Section 6(2) of the proposed OTT policy by MIB.

137 Section 8(1) of the proposed OTT policy by MIB.

138 Section 12(2) of the proposed OTT policy by MIB.

139 Section 12(1) of the proposed OTT policy by MIB.

140 Section 11(4) of the proposed OTT policy by MIB.

- The policy gives a list of forbidden contents. Some of the phrases, such as hurting religious sentiments, destroying social stability, sectarianism, etc., have been mentioned without detailed definitions.[141] These broad terms leaves scope for abuse in future.
- Section 15 of the proposed policy imposes provisions for self-censorship upon the content creators and providers of the OTT platforms

4.8.2 Draft Personal Data Protection Act, 2023 (PDPA)

The Draft of the Personal Data Protection Act 2023 (PDPA) seems to control how data is processed in Bangladesh and aims to protect citizens' privacy. It also grants the government broad authority to oversee the processing of personal data, investigate claims of violations, and impose fines when necessary. The 2020 and 2022 drafts of the bill titled the Data Protection Act (DPA), were examined by several international and national organisations, which made several recommendations to strengthen the regulatory framework for privacy rights and personal data protection. The government updated the DPA by releasing a new version on March 14, 2023. The DPA was finally modified as the Personal Data Protection Act 2023 (PDPA) and got Cabinet approval on 27 September 2023.[142] While the PDPA makes several improvements, it also leaves in place many of the problematic clauses that other organisations had pointed out in their earlier analyses:[143]

- **Overly Broad Scope**

Similar to the DPA, the main goal of the PDPA is regulatory control over personal data processing in general rather than just securing the rights of data subjects regarding their personal information. Still, the definition of "data" is narrow.

The PDPA's enforceability is still a concern if the government wants to regulate all personal data processing with broad exemptions for government officials. Also, the broad scope

141 Section 13(3), 13(4) of the proposed OTT policy by MIB.

142 TBS Report, 'Cabinet gives in-principle approval to draft Personal Data Protection Act,' (*The Business Standard*, November 2023) <https://www.tbsnews.net/bangladesh/cabinet-gives-principle-approval-draft-personal-data-protection-act-747226>.

143 See Christabel Randolph, 'Bangladesh Draft Data Protection Act 2023: Potential and Pitfalls' (Atlantic Council 2023); 'Third Update Analysis: Bangladesh's Draft Data Protection Act' (ICNL 2023); 'The Cross-Border Policy

gives the government much power over personal data and the information economy, which could make it more likely that people will be watched. The PDPA should be revised to ensure clarity regarding its scope and the definition of personal data if the government only wants to regulate the processing of personal data.

The PDPA maintains a strict definition of sensitive data, providing special protections for information that reveals a person's health data, genetic data, biometric data, and information related to any criminal conviction. However, the data related to race, ethnicity, gender, sex etc., have not been included in the sensitive data category.[144] The PDPA also fails to understand the difference between anonymised data and pseudonymised data and gives no definition for anonymised data.[145]

- **Broad exceptions**

The exemptions are too wide and do not include encrypted and pseudonymised data, resulting in a significant gap in the draft legal protections, and marking a departure from the world's best practices for data protection laws. Other broad exemptions continue to be a concern in addition to the exemptions for government authorities mentioned above. As a result, it lessens protections for marginalised communities, such as religious minorities and the lesbian, gay, bisexual, transgender queer, intersex and asexual (LGBTQIA) communities.

- **Data localisation**

Section 50 of the PDPA mandates that classified data be kept in Bangladesh. The definition of "classified data" is not mentioned in section 2, which contains several definitions. Data localisation requirements that are broad in scope and implemented in political contexts that permit censorship and unrestricted surveillance raise concerns about potential abuse. Although keeping classified information is probably justified, no legitimate goal is served by mandating that all user-generated and sensitive data be stored in Bangladesh, especially in cases where the location where the data would otherwise be stored, such as Ireland, has strict privacy and data protection laws. This includes sensitive health information stored in Bangladesh.

144 Section 2(t) of draft PDPA.

145 Section 2(b) of draft PDPA.

- **Discretionary authority over audits**

The draft PDPA imposes a data audit upon whoever retains data.[146] As per section 35 of the draft PDPA, the government will establish a Bangladesh Data Protection Board (BDPB). Sections 40, 41, 45, 48, and 49 of the draft PDPA give the BDPB complete discretion over the timing, scope, and execution of data audits, to form a panel of data auditors, access database, issue orders to provide personal data, impose fine on the Data Protection Officer, issue any order upon the data processor and Data Protection Officer etc. As a result, there is still a chance that it may be used as a means of harassing companies and organisations, including media outlets and human rights organisations.

- **No Fees Limits**

The 2023 Draft permits data fiduciaries to charge fees for data subjects to access their personal information,[147] just like in previous drafts. However, because the fee amount has not been specified, there is a chance that potentially high fees might be imposed. If this happens, only those who can pay the high fees will be able to take advantage of the PDPA's protections.

- **Broad Discretionary Powers to Authorities**

The draft PDPA does not contain any explicit oversight mechanisms or other limitations on the powers of the Bangladesh Data Protection Board or the directors in charge of upholding the PDPA. The Chairman of BDPB can decide administrative penalties and compensation based on the complaint received from the data subject and subject to the rules made for PDPA.[148] Still, the Chairman is not required to specify in detail how such a decision will be made. Therefore, the PDPA must be changed to limit the BDPB's broad discretion and guarantee its political independence.

146 Section 29 of the draft PDPA.
147 Section 13(2) of the draft PDPA
148 Section 56-63 of the draft PDPA

4.9 Regulating the Online Information Ecosystem

The Constitution of Bangladesh guarantees freedom of expression, including the right to receive and access information. However, according to Freedom on the Net 2023, Bangladesh scored 41 out of 100 due to the restrictions imposed on public digital spaces, access to the internet, restrictions on user rights, and limitations on online content.[149]

As seen across the chapter, different mechanisms have been used to regulate the flow of information on the internet. These include (a) internet shutdowns, (b) blocking content on social media, (c) law enforcement access to user data and (d) criminalisation of online speech.

The government has, in some instances, resorted to restraining access to entire social media or communication platforms, as well as, blocking specific pieces of content related to social, political, and religious aspects.[150] There have also been instances of complete or partial Internet shutdowns and disruptions to the speed of the Internet, as seen in previous sections. This is despite several experts warning that such actions were not an effective solution to address concerns related to national security.[151]

In addition to the aforementioned mechanisms that, when applied without effective checks and balances, can create a chilling effect on online expression, the 'Cyber Threat Detection and Response' initiative by the DoT is set to monitor, block, and filter online content on social media networks.[152] This body has been set up with the aim of curbing the spread of rumours on social media. This move was in line with the DSA's provision to constitute such an agency,[153] and now the CSA's mandate too. This has raised several concerns regarding censorship and surveillance, as this initiative will be used for monitoring different sites around the clock, and LEAs will subsequently ask the BTRC to block any content they deem derogatory or harmful.

149 'Bangladesh: Freedom on the Net 2023 Country Report' (*Freedom House*, 2023) <https://freedomhouse.org/country/bangladesh/freedom-net/2023>.

150 Ibid.

151 Arafatul Islam, 'Internet users defy Facebook to ban in Bangladesh' (DW News, 20 November 2015) <https://www.dw.com/en/internet-users-defy-facebook-ban-in-bangladesh/a-18863635>

152 Muhammad Zahidul Islam, 'Govt can now filter online contents' (Dhaka, 20 September 2019) *The Daily Star* <https://www.thedailystar.net/frontpage/bangladesh-govt-can-now-monitor-block-filter-online-facebook-contents-1802497>.

153 Ibid.

Other developments have been visible since 2021, with the government contemplating a law that obliges social media platforms to monitor and store user-generated data domestically.[154]

At this point, it is essential to note that many provisions criminalising speech can also lead to censorship and arrests of individuals under the ICTA, DSA and now the CSA. For instance, under the ICTA 2006, 94% of the cases fell under the contentious section 57, 13% of the cases were found to be false during the investigation stage, and 66% of the cases could not be proven.[155] In 46 cases over the last three years, the police allegedly submitted final reports to the court.[156] Of these, 4 out of 10 cases were filed against journalists, which the investigation reportedly found untrue.[157]

The DSA was passed in response to this legal mistreatment under the ICTA, which has, in turn, repealed Sections 54, 55, 56, 57, and 66 of the ICT Act. However, eliminating these five ICT Act provisions continued oppression; as the DSA 2018 incorporated many of the problematic provisions again, and the pattern has continued in the CSA 2023 (see sections 4.4 and 4.7).

4.9.1 Freedom of Dissent during the COVID-19 Pandemic

It is also important to note how the online information ecosystem was closely regulated during the COVID-19 pandemic. The government-imposed restrictions to curb the upsurge in disinformation.[158]

- In April 2020, the Directorate General of Nursing and Midwifery issued an order restricting all its officials and employees at government hospitals from speaking in public or to the media without prior permission.[159]

154 Syful Islam, 'Bangladesh tightens grip on Facebook, Twitter and other platforms' (*Nikkei Asia*, 09 September, 2021) <https://asia.nikkei.com/Politics/Bangladesh-tightens-grip-on-Facebook-Twitter-and-other-platforms>.

155 Asaduzzaman, 'Cases of cyber crime are on the rise' (The Daily *Prothom Alo*, September 2016) <www.prothomalo.com/bangladesh/crime/সাইবার-অপরাধের-মামলা-হু-হু-করে-বাড়ছে.

156 'No Place for Criticism : Bangladesh Crackdown on Social Media Commentary' (Human Rights Watch 2018) <https://www.hrw.org/report/2018/05/10/no-place-criticism/bangladesh-crackdown-social-media-commentary>.

157 Ibid.

158 'Bangladesh: Alarming Crackdown On Freedom Of Expression During Coronavirus Pandemic – ARTICLE 19' (*ARTICLE 19*, 2020) <https://www.article19.org/resources/bangladesh-alarming-crackdown-on-freedom-of-expression-during-coronavirus-pandemic/>

159 'Nurses Barred From Speaking To Media' (*Dhaka Tribune*, 2020) <https://archive.dhakatribune.com/bangladesh/dhaka/2020/04/17/govt-instruct-nurses-not-to-speak-to-media>.

- Then, on 4 August 2020, the Ministry of Health and Family Welfare passed an order barring all the health directorate officials from speaking in public or to the media without prior permission.[160]
- Furthermore, the government dropped mass media from the list of emergency services, intending to restrict the transmission of information about COVID-19.[161]

On several occasions, the government has blocked several online news agencies and taken down content on social media.[162] During the COVID-19 pandemic, internet bans were also reported in Bangladesh.[163]

Besides, under various provisions of the ICTA and CSA, authorities have filed complaints against citizens. Several people, including academicians,[164] doctors,[165] political opposition members, and activists[166] were arrested for criticising the government in handling the COVID-19 situation on online platforms.[167] In fact, some civil society members have alleged that citizens have been subjected to enforced disappearances, arbitrary detentions, torture, and in one case, even death in prison.[168]

160 'Health Directorate Staff Barred From Speaking To Media' (*The Business Standard*, 2020) < https://www.tbsnews.net/bangladesh/health/health-ministry-bars-dghs-officials-speaking-media-115663 >

161 'New Bangladesh Directives Drop Mass Media From Emergency Service List' (*New Age | The Most Popular Outspoken English Daily in Bangladesh*, 2020) <https://www.newagebd.net/article/104128/new-bangladesh-directives-drop-mass-media-from-emergency-service-list >.

162 See 'Bangladesh Blocks Several Websites amid COVID-19 Crisis' (*Benar News*, 2 April 2020) <https://www.benarnews.org/english/news/bengali/bangladesh-media-04022020173513.html>;Ahmed Shawki and Nurul Amin, 'Govt to Block 50 Websites, 82 Facebook Pages for Spreading Rumours' *The Business Standard* (1 April 2020) <https://www.tbsnews.net/coronavirus-chronicle/covid-19-bangladesh/govt-block-50-websites-82-facebook-pages-spreading-rumours>.

163 See *Human Rights Watch, 'Bangladesh: Internet Ban Risks Rohingya Lives'* (26 March 2020) <https://www.hrw.org/news/2020/03/26/bangladesh-internet-ban-risks-rohingya-lives>

164 'করোনা নিয়ে ফেসবুকে উস্কানিমূলক পোস্ট, দুই কলেজ শিক্ষক বরখাস্ত' (Bangla Tribune, 2020).

165 'Spreading Rumours: Doctor Put On 3-Day Remand' (*The Daily Star*, 2020) https://www.thedailystar.net/city/news/spreading-rumours-doctor-put-3-day-remand-1884649 >; 'Noakhali Doctor Show-Caused For Social Media Post Over PPE 'Shortage' (*Dhaka Tribune*, 2020) https://archive.dhakatribune.com/bangladesh/nation/2020/04/19/noakhali-doctor-show-caused-for-social-media-post-over-ppe-shortage >.

166 'Juba Dal Activist Held For Criticising Ministers' (*New Age | The Most Popular Outspoken English Daily in Bangladesh*, 2020) < https://www.newagebd.net/article/103060/juba-dal-activist-held-for-criticising-ministers >

167 'World Report 2021: Rights Trends In Bangladesh' (Human Rights Watch) https://www.hrw.org/world-report/2021/country-chapters/bangladesh#f6277a >.

168 Reuters, 'In fear of the state: Bangladeshi journalists self-censor as election approaches', 13 December 2018 <https://www.reuters. com/article/us-bangladesh-election-media-insight-idUSKBN1OC08Q>.

Initially, from March to 22 June 2020, according to a report of ARTICLE 19, 89 cases were filed against 173 people under the DSA. However, the number of cases and arrests increased dramatically in 2019, to 1135 arrests in 632 cases.[169] Similarly, between January 2020 and February 2022, approximately 2244 individuals faced charges in 890 cases .[170] The report further depicts that 22 cases were filed against 41 journalists from March 1 to May 31, 2022[171] under the DSA. In 2021, 198 cases were brought under the DSA, and 457 persons of different professions were prosecuted and detained.[172]

4.9.2 Right to Information

The Right to Information (RTI) Act was adopted in significant part because of the status of the right to information as a fundamental right. The primary purpose of the RTI Act is to ensure transparency and accountability of the government and private organisations that receive government or international funding, like NGOs.

Section 3 contains a provision for overriding other laws undermining the right to access information. For instance, the Official Secrets Act 1923, the Government Servant (Conduct) Rules 1979, and the Evidence Act 1872 may impede the provision of information; however, those laws shall be superseded by the provisions of the RTI Act.[173]

However, Section 32(1) of the RTI Act contains some exceptions for organisations and institutions dealing with state security and intelligence.[174] Therefore, citizens cannot get information from these stakeholders. The only safeguard is section 32(2), which states that exceptions related to such organisations will not apply to information about corruption and violation of human rights, as there is a public interest override provision for them.

169 Arifur Rahman Rabbi, 'Upsurge In DSA Cases During The Covid-19 Pandemic' (*Dhaka Tribune*, 2020) < https://archive.dhakatribune.com/bangladesh/2020/06/28/upsurge-in-digital-security-act-cases-during-the-covid-19-pandemic>.

170 'Position-Paper-on-Digital-Security-Act-2018-and-Draft-Cyber-Security-Act-2023' <https://www.ti-bangladesh.org/upload/files/position-paper/2023/Position-paper-on-Digital-Security-Act-2018-and-Draft-Cyber-Security-Act-2023.pdf>.

171 Ibid.

172 Zyma Islam and Ashutoush Sarkar, 'DSA: Misused To Muzzle Dissent' (*The Daily Star*, 2021) < https://www.thedailystar.net/frontpage/news/digital-security-act-misused-muzzle-dissent-2048837 > accessed 21 April 2022.

173 MS Siddiqui, 'Is Official Secrets Act Relevant in Bangladesh?' (*The Daily Star*, 25 May 2021) <https://www.thedailystar.net/law-our-rights/news/official-secrets-act-relevant-bangladesh-2098369>.

174 These organisations are the National Security Intelligence (NSI), the Directorate General Forces Intelligence (DGFI), the Defense Intelligence Units, the Criminal Investigation Department (CID) of Bangladesh Police, the Special Security Force (SSF), the Intelligence Cell of the National Board of Revenue, Special Branch of Bangladesh Police, and Intelligence Cell of Rapid Action Battalion (RAB).

The law has additional exemptions. It contains a list of twenty instances (under section 7) in which people cannot claim information.[175] That list is extensive; moreover, the terms used are also vague and grant excessive discretionary power to the government to deny requests for information. For example, terms like "security of Bangladesh" and "security of the people" are not clearly defined.

Such provisions cut against the intention and spirit of the RTI Act. Public bodies are mandated to actively promote open governance and inform the people of their rights. Therefore, adequate resources should be invested to encourage openness and overcome official secrecy. Wide exemptions infringe upon the right to impart information and hinder the right to freedom of expression.[176]

Consequently, the RTI Act has often fallen short of its goal to provide public-facing transparency of government action, as requests are frequently denied on broad national security grounds. There is, for instance, very limited transparency regarding government action against social media platforms. There is a lack of clarity about the legal basis upon which government authorities are suspending internet services, blocking apps, taking down websites, applications, specific content, and so on. Various procedural and substantive frameworks for blocking content are not publicly available, and the reasons for blocking individual pieces of content remain hidden from the public.

4.10 The Online Information Ecosystem in Bangladesh: A Focus on Security Imperatives

In recent years, security imperatives have heavily influenced the regulatory landscape in Bangladesh. Several key factors and developments illustrate the interplay between security concerns and social media governance in the country.

First, the CSA (and formerly DSA) and the ICTA have introduced broad definitions setting the stage for a security-focused approach. The DSA defined digital security as "the security of any digital device or digital system".[177] But this sheds no light on the scope

175 Sohini Paul, 'Right to Information Act 2009 Summary: Bangladesh' <https://www.humanrightsinitiative.org/programs/ai/rti/international/laws_papers/bangladesh/bangladesh_rti_act_2009_summary.pdf>.

176 A S M Sajjad Hossain, 'Right to Information Act and its effectiveness as a tool to fight corruption in Bangladesh' (2020) <https://www.iaca.int/media/attachments/2022/01/20/a_s_m_sajjad_hossain_thesis_final.pdf>.

177 DSA 2018 s 2(k).

of the term "security". However, a close reading of the legislation reveals that security encompasses "cybersecurity" as well as content-based offences and cybercrimes. The CSA includes similar extensive provisions as the DSA, which now fall under the purview of "cybersecurity".

It is also worth noting that the definition of cybersecurity itself is contested across scholarship.[178] It is also subject to political and geopolitical considerations, especially in the context of multilateral negotiations. The conceptions of cybersecurity in China and Russia differ from those in the United States and Europe, where the technical definitions based on the CIA (Confidentiality, Integrity, Accessibility) triad dominate.[179]

The SCO Agreement on the Information Security Area recognises the "use of dominant position in cyberspace to the detriment of interests and security of other states" and "dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of the states" as threats.[180]

This definition of information security with the aim of curbing separatism, extremism, and terrorism often legitimises the use of excessive measures, amounting to surveillance and censorship, in the purview of cyber security.[181] This is because when cybercrimes are constructed through the lens of security, as opposed to user safety, there is a shift from democratic consultation and decision-making to unilateral state-led action.[182]

This is also underscored by the implementation of legal instruments by LEAs. In Bangladesh, such agencies wield significant legal powers concerning lawful interception assistance, the disclosure of communications data,[183] undertaking investigations without

178 Tim Maurer and Robert Morgus, 'Compilation of Existing Cybersecurity and Information Security Related Definitions,' (October 2014) <https://d1y8sb8igg2f8e.cloudfront.net/documents/compilation-of-existing-cybersecurity-and-information-security-related-definitions.pdf>.

179 Worku Gedefa Urgessa, "Multilateral Cybersecurity Governance: Divergent Conceptualizations and Its Origin," *Computer Law & Security Review* 36 (April 1, 2020): 105368, https://doi.org/10.1016/j.clsr.2019.105368.

180 Shanghai Cooperation Organization (SCO), "Agreement between the Governments of State Members of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring the International Information Security," 2009.

181 Bruna Toso de Alcântara, "SCO and Cybersecurity: Eastern Security Vision for Cyberspace," *International Relations* 6, no. 10 (2018): 549–55.

182 Richard J Kilroy, 'Securitization' in Anthony J Masys (ed), Handbook of Security Science (Springer International Publishing 2018) <https://doi.org/10.1007/978-3-319-51761-2_11-1> defines "Securitization as the process through which non politicised (issues are not talked about) or politicised (issues are publicly debated) issues are elevated to security issues that need to be dealt with urgency, and that legitimate the bypassing of public debate and democratic procedures."

183 Bangladesh Telecommunication Act, 2001 s. 97(A).

a warrant and actions taken during times of emergency,[184] and issuing content blocking requests.[185] This has culminated in the centralisation of powers with the LEAs, resulting in executive discretion and a lack of public-facing transparency.

Website blocking and blocking of content on social media without transparency is also key due to the focus on security (see section 4.5.2)[186] The BTRC has intermittently blocked websites, news outlets, and social media posts critical of the government.[187]

Similarly, the crackdown on internet shutdowns and internet restrictions have largely been targeted at opposition party rallies across the country,[188] and at Rohingya refugee camps.[189] During times of unrest, such as the protests of August 2018, the BTRC took drastic measures by ordering ISPs to reduce mobile phone network signals to 2G.[190]

The experience of popular online platforms like Facebook has also been marked by periodic interruptions in Bangladesh. In 2017, Facebook declined to sign a Memorandum of Understanding (MoU) that would have required Bangladeshi users to provide additional identification, including National ID numbers, reflecting tensions between the platform and government authorities.[191] These efforts further emphasise the control of information flows.

In summary, the online information ecosystem in Bangladesh is significantly influenced by security imperatives. This has significant implications for the freedoms and rights of citizens.

184 CSA 2023, s 42.

185 CSA 2023, s 8(2).

186 CSA 2023, s 8.

187 Twitter Correspondence with Users Reveals Bangladesh Government Attempts to Remove Tweets' (*Netra News* — নেত্র নিউজ, 3 December 2022) <https://netra.news/2022/twitter-correspondence-with-users-reveals-bangladesh-government-attempts-to-remove-tweets/>.

188 'BTRC Shuts 3G, 4G Again' *The Daily Star* (30 December 2018) <https://www.thedailystar.net/bangladesh-national-election-2018/3g-4g-mobile-internet-services-speed-restored-in-bangladesh-1680808>.

189 Human Rights Watch, "Bangladesh: Internet Ban Risks Rohingya Lives" (26 March 2020) <https://www.hrw.org/news/2020/03/26/bangladesh-internet-ban-risks-rohingya-lives> accessed on 10 May, 2023

190 Staff Correspondent, 'Mobile Net Slowed Down' *The Daily Star* (5 August 2018) <https://www.thedailystar.net/country/bangladesh-mobile-internet-speed-brought-down-across-for-24hrs-1615909>.

191 Staff Correspondent, 'ID for New Account: FB Refuses to Sign MoU with Police' *The Daily Star* (15 March 2017) <https://www.thedailystar.net/frontpage/id-new-account-fb-refuses-sign-mou-police-1376128>.

4.11 Impact on the Rule of Law:

(a) Avoidance of Arbitrariness and Fairness in the Application of Law:

Article 26 of the Constitution of Bangladesh provides that all laws inconsistent with the fundamental rights outlined in the constitution — to the extent that they are incompatible —become null and void.

While fundamental rights are a cornerstone of any democratic society, it is important to acknowledge that they are not absolute. Article 39(2) illustrates this by establishing justifiable grounds for imposing reasonable restrictions on freedom of speech and expression. These restrictions include, "security of the state, friendly relations with foreign states, public order, decency, morality, contempt of court defamation or, incitement to an offence."[192]

Nonetheless, ensuring the avoidance of arbitrariness and upholding legal transparency and fairness in the application of the law is imperative. Unfortunately, the CSA, as well as the repealed DSA, introduced vague provisions, such as "propaganda" and "image of the nation" which do not fall within the ambit of Article 39 (2) restrictions. They do not qualify as 'reasonable' restrictions given their wide ambit. Consequently, many experts contend that they are unconstitutional.[193] They certainly undermine the principle of supremacy of the Constitution, which necessitates a fair and reasonable application of law.

The following two case studies illustrate this point further:

> On December 2, 2020, a folk singer and her colleagues were alleged to have jeopardised religious harmony by publishing a folk song on YouTube.[194] The report by the Police Bureau of Investigation against which the arrest warrant was issued stated that the song

192 The Constitution of Bangladesh, Article 39(2).

193 'Shrinking Space for Liberty in South Asia: Analysing the DSA, 2018 of Bangladesh – The Leaflet' (11 July 2022) <https://theleaflet.in/shrinking-space-for-liberty-in-south-asia-analysing-the-digital-security-act-2018-of-bangladesh/>.

194 Tribune Desk Arrest warrant against Baul singer Rita Dewan, 2 others for hurting religious sentiment December 02, 2020 *Dhaka Tribune* <https://archive.dhakatribune.com/bangladesh/2020/12/02/arrest-warrants-against-baul-singer-rita-dewan-2-others-for-hurting-religious-sentiment>.

was written and sung with derogatory statements against Islam.[195] Very broad and vague reasons were provided, and she was convicted under the Penal Code, 1860, and the DSA with several other allegations, notably "creating outrage by insulting religious beliefs, provoking a breach of peace, and making statements to conduct public mischief".[196] Later on, on October 25, 2021, she was convicted for hurting religious sentiments.[197]

In another instance, a 25-year-old primary school teacher in a rural area south of Dhaka was arbitrarily arrested by police for spreading 'anti-state' rumours through her Facebook account on 4 August 2018. Her post appealed for peace during the road safety movement. However, a case was filed under Section 57 of the ICTA. The police also seized her mobile phone and laptop.[198]

These case studies highlight key concerns regarding the arbitrary application of DSA that impacts the right to 'freedom of expression' contained in Article 39 of the Constitution.

(b) Participatory Decision Making:

The Constitution grants the Parliament sole authority over all legislative matters. Members of Parliament (MPs) have to send a notice to the Parliamentary Secretary seeking permission to bring a bill before Parliament. The bill then passes through several steps and drawn-out processes before officially being published in the Gazette and becoming law.

Unfortunately, cyber laws in Bangladesh often fail to go through these processes before becoming law. They often involve little democratic deliberation and stakeholder consultation and are often hastily passed. On 11 March 2014, the Ministry of Posts, Telecommunications, and Information Technology approved the "National Cyber

195 BSS, Dhaka DSA: Arrest warrant issued against Baul Rita Dewan December 02, 2020, *The Daily Star* <https://www.thedailystar.net/country/news/digital-security-act-arrest-warrant-issued-against-baul-rita-dewan-2004665>.

196 No space for dissent Bangladesh's crackdown on freedom of expression online *Amnesty International* 13 <https://www.amnesty.ca/wp-content/uploads/2021/07/Amnesty-NO-SPACE-FOR-DISSENT.pdf>.

197 The Daily Prothom Alo English Desk Baul Rita Dewan indicted in DSA case October 05, 2021, *Prothom Alo* <https://en.prothomalo.com/bangladesh/crime-and-law/baul-rita-dewan-indicted-in-dsa-case>.

198 *The Daily Star*, 'Spreading rumours: Patuakhali school teacher released after HC bail' Aug 20, 2018 <https://docs.google.com/document/d/1b5lmboIbvwSQ4Wz8EidaVYqjRFS8oZeZ/edit>.

Security Strategy"[199] in English (in violation of the Bangla Bhasha Procholon Ain, 1987 – which means "Bengali Language Implementation Act, 1987") and sent it to the Global Cyber Security Agenda at the International Telecommunication Union.[200]

According to section 3(1) of the Bengali Language Implementation Act, 1987, "all records and correspondences, laws, court proceedings, and other legal actions shall be written in Bengali in all courts, government or semi-government offices, and autonomous institutions, after the introduction of this Act."

Furthermore, section 3(3) states, "If any government staff or officer breaches this act, he or she will be accused of violating Bangladesh Civil Servant Order and Appeal Rules, and necessary actions will be taken against him or her." Section 3(2) also says, "If someone submits an appeal or petition in a language other than Bengali to one of the offices listed in clause 3(1), the appeal or petition will be considered illegal and will not be heard." As a result, the legality of Bangladesh's National Cyber Security Strategy is still up for debate.

The DSA was approved by a voice vote in Parliament on 18 September 2018.[201] It came into effect on 9 October 2018, despite vigorous objections from journalists, lawyers, teachers, and human rights activists worldwide, regionally, and locally.[202] The ICTD of the Ministry of Posts and Telecommunications released the Digital Security Rules 2020 under the DSA hastily.

Similarly, as seen earlier, while claiming to have some relevance to defending citizens' rights, the Cyber Security Act contains several provisions that can also be used to limit citizens' freedom of expression, privacy, and other civil rights and criminalise pro-people actions. The government enacted the Cyber Security Act in 2023 amid widespread criticism from opposition, civil society and journalists, without adequate stakeholder consultation.[203]

199 National Cyber Security Strategy, 2014 <https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/policies/3e8d0018_757f_4033_8b9c_47ee17e88c2c/Cyber_Security_Guideline-1.pdf>.

200 'Global Cybersecurity Agenda (GCA)' (ITU) <https://www.itu.int:443/en/action/cybersecurity/Pages/gca.aspx>.

201 Rashidul Hasan, 'Digital Security Bill Passed' *The Daily Star* (20 September 2018) <https://www.thedailystar.net/politics/bangladesh-jatiya-sangsad-passes-digital-security-bill-2018-amid-concerns-journalists-1636114>.

202 See Human Rights Watch, 'Bangladesh: Scrap Draconian Elements of Digital Security Act' (22 February 2018) <https://www.hrw.org/news/2018/02/23/bangladesh-scrap-draconian-elements-digital-security-act>;'Appeal & Denial' *The Daily Star* (10 October 2018) <https://www.thedailystar.net/supplements/news/digital-security-act-2018-appeal-and-denial-1645015>.

203 See Rashidul Hasan, 'Cyber Security Bill 2023: JS Passes It amid Strong Protests' (*The Daily Star*, 14 September 2023) <https://www.thedailystar.net/news/bangladesh/news/cyber-security-bill-2023-js-passes-it-amid-strong-protests-3418161>;Ali Asif Shawon, 'Why Was There Such a Rush to Pass the Cyber Security Bill?' *Dhaka Tribune* (16 September 2023) <https://www.dhakatribune.com/bangladesh/325432/why-was-there-such-a-rush-to-pass-the-csa-bill>.

(c) Separation of Powers

The principle of separation of powers, often known as the checks and balances system, provides that after a significant activity has been delegated to one organ of government, consideration should be taken to establish the involvement of other organs as well.[204] It is provided that no one organ may exceed the Constitution's limits, or undermine the authority granted to other organs.[205] However, the BTRA and the CSA allow the government to unilaterally block and remove content on social media by executive order. This has led to censorship without adequate checks and balances.

As discussed above, section 8 of the CSA states that the BTRC can– while informing the government– take urgent measures to remove or block content, upon receiving requests from the Directorate General or LEAs for the removal of any content or any platform where such data or information is disseminated.[206] Additionally, under section 46 of the BTRA, the government may restrict any website, to stop incitement to commit any crime, or on the grounds of state integrity, state security, and public order violations.[207] These provisions enable the executive branch to take actions that bypass judicial review, infringing on the separation of powers principle.

Furthermore, Bangladesh ranked 5th globally in internet shutdowns in 2022. Authorities shut down the internet six times in 2022, deploying their power to do so as "weapons of control", according to a report of global digital rights watchdog Access Now and the #KeepItOn coalition.[208] Many of these shutdowns were authorised during the opposition party (BNP) protest rallies.[209]

204 Mahmudul Islam, *Constitutional Law of Bangladesh* (Third Edition, Mullick Brothers) 90.

205 The Constitution of the Republic of Bangladesh, art 7; Mohammed Shamsuddin v. SS Wijesinha, [1967] 3 WLR 1460 (PC).

206 The DSA 2018, s 8(3).

207 The Bangladesh Telecommunication Act 2001, s 46.

208 Star Digital Report, 'Global report on internet shutdowns: Bangladesh ranked 5th' (*The Daily Star*, 1 March 2023) <https://www.thedailystar.net/tech-startup/science-gadgets-and-tech/tech-news/news/global-report-internet-shutdowns-bangladesh-ranked-5th-3260651?amp> accessed on 4th April 2023

209 'Global Report on Internet Shutdowns: Bangladesh Ranked 5th' (*Asia News Network*, 2 March 2023) <https://asianews.network/global-report-on-internet-shutdowns-bangladesh-ranked-5th/>.

There have been instances where the government abruptly shut down the internet, such as when the BTRC ordered the nation's International Internet Gateway operators to block access to 35 news websites.[210] This order came the day after the "Internet shutdown drill" was announced. It was presented as a security measure whereby internet connectivity in the commercial area of Dhaka was disabled for 3.5 hours.[211] Moreover, internet access has been blocked in the Rohingya refugee camps since September 2019 due to a BTRC directive, which has been justified as a "security measure".[212]

Such extensive communication restrictions were neither necessary nor reasonable. Moreover, the decisions to impose such restrictions were taken solely by the executive branch. Such unilateral acts conflict with the separation of powers principle. They highlight how the executive branch (i) is unconstrained by judicial review procedures, and (ii) prioritises national security while downplaying competing interests based on an individual's right to free expression.

International law mandates applying a three-part cumulative test to restrict speech online and offline.[213] According to this test, restrictions on speech: (1) must be stipulated by law, which is transparent and available to everyone (principles of predictability and transparency); (2) must pursue one of the goals outlined in Article 19, paragraph 3, of the ICCPR, namely: (i) to protect the rights or reputations of others; (ii) to protect the rights of individuals with disabilities (principles of necessity and proportionality); and (3) must be necessary for a democratic society.[214]

210 Zara Rahman, "Bangladesh Shuts Down the Internet, Then Orders Blocking of 35 News Websites" (*Global Voices*, 4 August 2016) <https://globalvoices.org/2016/08/04/bangladesh-shuts-down-the-internet-then-orders-blocking-of-35-news-websites/amp/> accessed on 10 May 2023.

211 Ibid.

212 Human Rights Watch, "Bangladesh: Internet Ban Risks Rohingya Lives" (26 March 2020) <https://www.hrw.org/news/2020/03/26/bangladesh-internet-ban-risks-rohingya-lives> accessed on 10 May, 2023

213 'Global Toolkit for Judicial Actors: International Legal Standards on Freedom of Expression, Access to Information and Safety of Journalists' - (UNESCO Digital Library) <https://unesdoc.unesco.org/ark:/48223/pf0000378755>;Wolfgang Benedek and Matthias C Kettemann, 'Freedom of Expression and the Internet' (Council of Europe Publ 2013).

214 Ibid.

Additionally, any law that limits the freedom of expression must be applied by a body free from political, commercial, or other unjustified influences. Such a body must act fairly and impartially and enable users to access. Also, such laws should contain sufficient safeguards against abuse, including a chance for challenge and redress in the event of abusive application of the law. This three-part test is in consonance with Bangladesh's jurisprudence on restriction of speech and expression, regardless of the medium. Therefore, the application of cyber laws must satisfy the three-part test and place limits on the executive's ability to exercise unchecked discretion. However, the application of cyber laws frequently flouts the three-part test, due to the lack of meaningful oversight over the Directorate General's discretion. As a result, this lack of adequate safeguards, and checks and balances forces users and journalists to exercise self-censorship.

(d) Legal Certainty

According to the principle of legal certainty, laws must be clear, precise, unambiguous, and have foreseeable legal ramifications. Legal certainty encourages legal efficiency, by enabling individuals to comprehend the law to the extent necessary to comply with it. While the right to express oneself and hold opinions without interference is protected, these rights may be restricted only when such restrictions are "provided by law".[215] The definition of a crime provided in any legislation thus must be strictly construed and cannot be broadened by analogy.[216]

In Bangladesh, several of the CSA's provisions must be narrower and more concise to communicate to the general public, and to those enforcing the legislation, what types of expression are prohibited under the law. For example, "any propaganda or campaign against the liberation war of Bangladesh, the spirit of the liberation war, the national anthem, or national flag" constitutes an offence under CSA.[217] However, the phrase "spirit of the liberation war" is not defined anywhere in the CSA, which leaves room for it to be given a broad definition, and to be used to denigrate, demonise, and attack opponents with the claim that they have compromised the spirit of Bangladesh's independence movement.

215 ICCPR (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, Art 19(3).

216 Rome Statute Of The International Criminal Court (adopted on 17 July 1998, entered Into force July 1, 2002) 2187 U.N.T.S. 90, art 22(2).

217 CSA, 2023, s. 21.

Ahmed Kishore, Mushtaq Ahmed, and nine other people, including two journalists, were charged under the DSA in 2020 with having violated this provision for "knowingly posting rumours against the Father of the Nation and the Liberation War."[218] The contentious post read, "So, when and where will the *Iftar Mahfil* of Mujib Borsho be held?" and this was used as evidence against the accused. Petitioners argued that this post was intended to be ironic, about the fact that the coronavirus hinders organising Iftar parties and that some party activists must be affected by that.[219] This provides another instance of how the provisos' lack of detailed definitions and specificity can result in extremely broad interpretation, making it challenging for people to evaluate their conduct online to avoid prosecution, which encourages self-censorship.

In another case, a political science student from Jagannath University was arrested for hosting a webinar wherein one of the guest speakers, a former Bangladeshi army official (now based in Canada), made comments perceived to be critical of the Bangladeshi authorities.[220] The police accessed a recording of the webinar on YouTube and subsequently filed cases under DSA for attempting to 'deteriorate law and order' and for 'defaming' the prime minister, among other charges.[221] The student was subject to fourteen months of jail time and received permanent bail from the Supreme Court in November 2023. While the case is still being heard, it has since been alleged that the student was seventeen years old at the time of trial but was sued as an adult under the DSA in 2020.[222] It is to be noted that a person below eighteen years of age is considered a child as per Section 4 of the Children Act 2013 of Bangladesh.[223]

218 Zyma Islam, Muntakim Saad Case Against 11 under DSA: Charges appear to be puzzling" (*The Daily Star*, 9 May 2020) <https://www.thedailystar.net/frontpage/news/case-against-11-under-dsa-charges-appear-be-puzzling-1900915>.

219 Ibid.

220 'Bangladesh: Authorities must immediately release university student Khadijatul Kubra' (*Amnesty International*, August 2023) <www.amnesty.org/en/latest/news/2023/08/bangladesh-authorities-must-immediately-release-university-student-khadijatul-kubra/>.

221 Ibid.

222 Zyma Islam and Emrul Hasan Bappi, 'Digital security act: Sued at 17, JnU student in jail' (*The Daily Star*, September 2022) <www.thedailystar.net/news/bangladesh/crime-justice/news/digital-security-act-minor-sued-adult-2yrs-ago-languishing-jail-3121741>.

223 Children Act No.24 of 2013 <http://bdlaws.minlaw.gov.bd/act-1119/section-42716.html >.

Furthermore, the CSA continues to give the government a disproportionate amount of punitive power, as the authority can conduct investigations on any citizen's actions that appear to pose a threat.[224] For instance, the Director General and LEAs have the power, to direct the BTRC to remove any content they believe "poses a threat to digital security" or "creates disunity in the country, disrupts economic activities and security, defence, hurts religious values, creates communal hatred or bad feelings" from the platform on which it was published.[225] The provision's ambiguous language allows for a wide interpretation of what constitutes unlawful information. Therefore, the grounds needed to remove or prohibit online information are overly broad in scope and may be subject to different interpretations by different individuals, LEAs and other authorised personnel, undermining the principle of legal certainty.

(e) Equality Before the Law

The principle of equality before the law entitles individuals to equal protection without any discrimination.[226] It is linked to the creation of legal standards, whereas equal protection under the law is concerned with (i) substantive equality concerns and (ii) the application and implementation of the law.[227] In keeping with the pledge made in the Constitution's preamble to uphold the rule of law, a positive provision guaranteeing equality before the law has been incorporated.[228]

Every piece of legislation must adhere to the rule of law, regardless of the subject matter. However, in Bangladesh, vague and broad provisions in the DSA and the Penal Code have been used to stifle free expression. Several times they have been deployed to justify arrests and persecution of dissenters; such arbitrary application has a severe negative effect on the principle of equal protection.

224 Ali Riaz 'How Bangladesh's DSA Is Creating a Culture of Fear' (*Carnegie Endowment for International Peace*, 9 December 2021) <https://carnegieendowment.org/2021/12/09/how-bangladesh-s-digital-security-act-is-creating-culture-of-fear-pub-85951>.

225 The DSA, 2018 s. 8.

226 ICCPR Art 26.

227 Kristin Henrard, 'Equality of Individuals' Max Planck Encyclopedia of Public International Law [MPEPIL] (2008), para 5.

228 The Constitution of the Republic of Bangladesh, Art 27.

Section 29 of the repealed DSA states that if a person commits an offence under Section 499 of the Penal Code (relating to defamation) on a website or any electronic device(s), he shall be punished. This section can be misused to bring charges against individuals who criticise influential figures such as ministers and politicians. As stated earlier, the CSA retains defamation as an offence under section 29.

According to research conducted by the Centre for Governance Studies (CGS), in the 26 months before February 2022, 162 cases were filed under Section 29 of the DSA, wherein 427 people were accused, and 76 people were arrested.[229] A considerable number of the accused were journalists, which shows that the section has often been misused to intimidate, harass, and threaten journalists and human rights advocates, resulting in the stifling of critical voices online.

In the northwest Thakurgaon district, a 17-year-old was arrested for "defaming" the prime ministers of Bangladesh and India and the foreign minister of Bangladesh in an internet video that contained remarks critical of the leaders of Bangladesh and India.[230] This incident occurred during protests against the Indian Prime Minister Narendra Modi's visit to Bangladesh by Muslims and student activists in Dhaka. Another 15-year-old was detained for having "badmouthed our mother-like leader," the Prime Minister, in a Facebook post.[231]

A total of 210 people have been accused, and 115 have been detained in the 140 cases that claim the Prime Minister has been defamed.[232] The statistic indicates how the principle of equality before the law may have been compromised when dissenting opinions are stifled for criticising politicians, members of the ruling party, or other prominent figures.

229 Centre for Governance Studies, 'What's happening: Trends and Patterns of the DSA 2018 in Bangladesh' (Centre for Governance Studies, 25 January 2023) <https://cgs-bd.com/article/11282/What%e2%80%99s-happening--Trends-and-Patterns-of-the-Digital-Security-Act-2018-in-Bangladesh>.

230 SM Najmus Sakib, Bangladesh arrests teen for defaming premiers" (Anadolu Agency, 21 March, 2021) <https://www.aa.com.tr/en/asia-pacific/bangladesh-arrests-teen-for-defaming-premiers/2183493>.

231 Brad Adams, 'Bangladesh Arrests Teenage Child for Criticizing Prime Minister' (Human Rights Watch, 25 June 2020) <https://www.hrw.org/news/2020/06/26/bangladesh-arrests-teenage-child-criticizing-prime-minister> accessed on 5 April 2023

232 Ali Riaz, 'The Unending Nightmare: Impacts of Bangladesh's DSA 2018' (Center for Governance Studies, 2022)

Several Awami League and Jubo Mahila League officials and activists filed a criminal defamation suit against photojournalist and editor Shafiqul Islam Kajol under the DSA. Kajol allegedly wrote "defamatory, offensive, and obscene remarks in his Facebook profile."[233] The situation was particularly suspicious since Kajol mysteriously vanished the day after the complaint was submitted. He was discovered 53 days later in a field, blindfolded with his legs and wrists bound.[234] He was immediately detained for three counts against him under DSA.[235]

(f) Accountability Before the Law

The principle of accountability before the law implies that the executive and administrative bodies must also comply with the law, and in particular, must observe relevant limitations on exercising their powers.[236] Under the rule of law, individuals who wield authoritative power are just as much subject to the law as those who are impacted by it. At its foundation, accountability has four goals:[237] (i) to make an official's actions transparent to the public, (ii) to restrain an official from abusing their position of authority, (iii) to punish the abuse of power, and (iv) to consequently restore any interests that were harmed.

According to section 40 of the DSA, an investigating officer has 60 days to conclude an inquiry, and the higher authority may add 15 days. The cyber tribunal is authorised by law to prolong the inquiry time after this 75-day window expires. This provision has been and continues to be gravely violated. In section 39 of the CSA, this provision of 60 days has been extended to 90 days.[238]

233 Staff Corrospondent, 'Kajol's DSA Plight: Charges in 3 cases framed in 1 day' (*The Daily Star*, 11 November 2021) <https://www.thedailystar.net/news/bangladesh/crime-justice/news/kajols-dsa-plight-charges-3-cases-framed-1-day-2225141>.

234 Kaamil Ahmed, 'Bangladeshi Journalist Is Jailed after Mysterious 53-Day Disappearance' *The Guardian* (8 May 2020) <https://www.theguardian.com/global-development/2020/may/08/bangladeshi-journalist-is-jailed-after-mysterious-53-day-disappearance>.

235 Staff Correspondent, 'Kajol's DSA Plight: Charges in 3 cases framed in 1 day' (*The Daily Star*, 11 November 2021) <https://www.thedailystar.net/news/bangladesh/crime-justice/news/kajols-dsa-plight-charges-3-cases-framed-1-day-2225141>..

236 *Corporation of the City of Enfield v Development Assessment Commission* (2000) 199 CLR 135, 157.

237 Ellen Rock, 'Accountability: a core public law value?' [2018] 24 Australian Journal of Administrative Law 189.

238 CSA 2023, s 39.

The DSA imposed severe penalties upon conviction; bail is unavailable with few exceptions. For example, two individuals– cartoonist Ahmed Kabir Kishore and writer Mushtaq Ahmed were imprisoned in a case under the DSA. They were both denied bail six times in ten months by lower courts, and they filed appeals in the High Court on February 23, 2021.[239] However, Ahmed Kabir Kishore was only given bail after Mushtaq Ahmed died in custody, as massive protests erupted over his death.[240]

In some DSA cases, the victims and human rights defenders in Bangladesh have alleged disappearances and torture to death of individuals.[241] This violates Article 35 of the Constitution, the Torture and Custodial Death (Prevention) Act of 2013, and the guidelines set forth by the High Court in the *Blast v. Bangladesh* case.[242, 243]

The following example also illustrates the failure to uphold legal accountability. Mamunur Rashid Nomani, the editor of Barisal Khabar, a privately held news website, alleged that Serniabat Sadiq Abdullah, the mayor of the Barisal City Corporation, assaulted him for having contributed a report to his news site.[244] Nomani sustained serious injuries, including several broken fingers. A case was filed against Nomani under the DSA.[245] His injuries

239 Faislam Mahmud, 'Bangladeshi cartoonist granted bail after widespread protests' (Aljazeera, 3 March 2021) <https://www.aljazeera.com/news/2021/3/3/cartoonist-gets-bail-in-bangladesh-after-widespread-protests>.

240 Ibid.

241 See 'Bangladesh: Reveal Whereabouts of Disappeared Journalist, End Repression' (*Amnesty International*, 18 March 2020) <https://www.amnesty.org/en/latest/news/2020/03/bangladesh-must-reveal-whereabouts-of-disappeared-journalist-and-end-repression/>;TBS Report, 'Victims of Enforced Disappearances, DSA Seek Justice at BNP's Youth Rally' *The Business Standard* (22 July 2023) <https://www.tbsnews.net/bangladesh/bnp-men-gearing-youth-rally-suhrawardy-669378>; Jyotirmoy Barua, 'A New Trend in Disappearance Cases' *The Daily Star* (30 August 2020) <https://www.thedailystar.net/opinion/news/new-trend-disappearance-cases-1952957>.

242 Human Rights Watch, "Bangladesh: Joint Call for the Release of Journalist Shafiqul Islam Kajol" (11 August 2020) <https://www.hrw.org/news/2020/08/11/bangladesh-joint-call-release-journalist-shafiqul-islam-kajol>.

243 Bangladesh Legal Aid and Services and Trust and others vs. Bangladesh and Others [Section 54 Guidelines Case, or Rubel Killing Case, or Guidelines on Arrest and Remand Case] (Writ Petition No. 3806 of 1998)55 DLR (2003) 363.

244 Staff Correspondent, "DSA: Three including editor of online portal sent to jail"(*The Daily Star*, 15 September 2020)<https://www.thedailystar.net/city/news/three-including-editor-online-portal-sent-jail-1961477>; Committee to Protect Journalists (CPJ), "Bangladeshi journalist Mamunur Rashid Nomani harassed following 2020 assault, detention" (2 February, 2022) <https://cpj.org/2022/02/bangladeshi-journalist-mamunur-rashid-nomani-harassed-following-2020-assault-detention/>.

245 Staff Correspondent, "DSA: Three including editor of online portal sent to jail"(*The Daily Star*, 15 September 2020)<https://www.thedailystar.net/city/news/three-including-editor-online-portal-sent-jail-1961477>.

were untreated for the whole of his 17-day detention; it was not until the journalist was released on temporary bail that his fractured fingers and other wounds were attended to.[246]

Such cases raise concerns about a pattern of abuse of authority, a lack of recourse for individuals who suffer from such violations, and a failure to uphold legal accountability.

4.12 Conclusion

It would not be wrong to say that the social media governance in Bangladesh is driven by security interests to a large extent. Thus, it appears that social media governance often manifests in regulating the flow of online information through internet shutdowns, blocking content on social media, criminalising speech, arresting individuals, and interception and monitoring communication.

The lack of procedural and substantive safeguards, and the vague and ambiguous drafting of laws, vests the executive and LEAs with immense discretionary power. This is magnified by the lack of independent oversight and accountability. Such executive overreach points to shortcomings in adhering to the principles of the democratic rule of law when it comes to social media regulation.

246 Committee to Protect Journalists (CPJ), "Bangladeshi journalist Mamunur Rashid Nomani harassed following 2020 assault, detention" (2 February, 2022) <https://cpj.org/2022/02/bangladeshi-journalist-mamunur-rashid-nomani-harassed-following-2020-assault-detention/>.

5. CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

As seen across chapters 2, 3 and 4 ("country profiles"), governments across Sri Lanka, India, and Bangladesh are increasingly regulating[1] social media through existing ICT regulation and penal provisions (directed at users), as well as novel statutes, subordinate legislation and policies. We observe that (a) ICT regulation comprising of cybersecurity, data protection, and telecommunication regulation; (b) intermediary liability frameworks;[2] and (c) key speech laws (mostly penal) are employed to regulate the flow of online information and have a definitive impact on how social media is governed across the three countries.

We further identify four key mechanisms through which the information ecosystem is regulated across the three jurisdictions: (a) internet shutdowns, (b) blocking content on social media,[3] (c) criminalisation of online speech, and (d) law enforcement access to user data.

It was observed that state security[4] imperatives often drive this regulation of the online information ecosystem. This has implications on rule of law and we observe through case studies and examples of implementation that all three countries grapple with some

1 As noted earlier, we use the term "regulate" to broadly mean any actions taken to govern or influence the way in which social media platforms are operated as well as, used and accessed. It consists of regulation that is directed at (a) social media platforms as intermediaries; (b) other intermediaries like ISPs; and (c) end users.

2 While India and Bangladesh provide conditional exemption from liability for third-party content hosted by intermediaries, Sri Lanka lacks such an exemption framework at the time of writing. However, this can change with the proposed Online Safety Bill 2023.

3 As noted in chapter 2, Sri Lanka does not have a legal framework to issue blocking orders for specific pieces of content on social media platforms at the time of writing. However, this could change if the Online Safety Bill 2023 becomes law.

4 As noted earlier, for the purposes of this report, we do not draw distinctions between internal and external security. Instead, we use the term "state security" to broadly encompass concepts such as "sovereignty and integrity", "security of the state", "defence of the state", "*national security*" as well as "*public order*", "*public security*", "*public tranquillity*", "*public emergency*" employed across the three jurisdictions.

shortcomings when it comes to separation of powers, procedural and legal transparency and fairness in application.[5] A discernible trend towards excessive executive control and the centralisation of powers is evident across all three jurisdictions, particularly when it pertains to the 'security' imperatives of the state.

The first part of this chapter systematically maps the emerging trends in the governance of social media. Key areas of convergence become apparent, notably in mechanisms for regulating the flow of online information and the dominance of state security concerns, as well as in the exercise of executive discretion and the limited transparency surrounding these processes.

The second part of the chapter provides recommendations to limit the scope of security exceptions and institute checks and balances in social media regulation to safeguard against misuse of state power. It becomes essential that security imperatives should be applied to public digital spaces by employing reliable, efficacious, efficient, proportionate and rights-respecting tactics.[6] Coercive action that places limits on individual and collective rights must be legitimate, necessary and proportional, follow established standards and undergo independent review.

5.2 Mechanisms to Regulate the Flow of Online Information and the Dominance of State Security Concerns

It is evident from the analysis in the country profiles that security concerns play a significant role in regulating the information ecosystem. In this section we outline the trends that illustrate how security imperatives manifest across: (a) internet shutdowns, (b) blocking content on social media, (c) criminalisation of online speech, and (d) law enforcement access to user data

5 See sections 2.8,3.9 and 4.11.

6 Michael Skerker, 'A Two-Level Account of Executive Authority' (2018) Oxford University Press <https://philpapers.org/archive/SKEATL.pdf>.

5.2.1 Internet Shutdowns

Shutdowns are employed by all three countries under study. India has consistently recorded the most number of internet shutdowns in the world since 2018.[7] It has recorded 764 total internet shutdowns to date, including 77 in 2022 and 101 in 2021.[8] Bangladesh also featured among the top 5 countries in internet shutdowns per the 2022 Internet Shutdown report by Access Now.[9] Bangladesh recorded at least six shutdowns (slowing of internet speed) during six separate rallies by the opposition party. Sri Lanka has also experienced partial internet shutdowns in the form of social media platforms being blocked.[10]

As seen in the country profiles, security concerns have underlined the legal provisions governing internet shutdowns across all three countries.[11]

It has also been observed that in practice, all three countries cite security concerns to restrict access to the internet or parts of it during public protests. India, for instance, has used internet suspension as a tool to curb access to social media during mass protests like the 2020-21 farmer's protests ,[12] the Citizenship Amendment Bill protests,[13] and most recently, the protests against the Agneepath Scheme for recruitment in the armed forces.[14] India also explicitly used whitelisting of websites to curb access to social media in Kashmir (see section 3.5.2).

---

7 Access Now, 'Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022' (2023).

8 'Internet Shutdowns Tracker' (*SFLC.in*) <https://internetshutdowns.in/>.

9 Access Now, 'The Return of Digital Authoritarianism: Internet Shutdowns in 2021' (*Access Now*, 2022) <https://www.accessnow.org/wp-content/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf>.

10 'Authorities, telcos in Sri Lanka must ensure internet access throughout crisis' (*Access Now*, 3 May 2022) <https://www.accessnow.org/press-release/sri-lanka-internet-access-crisis/>.

11 In India, the Telegraph Act of 1885 lays down grounds for suspending internet access, including "*interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence*." In Bangladesh, the Telecommunication Regulation Commission issues internet suspension orders on the basis of "national security" and "public order" under section 97(A) of the Bangladesh Telecommunication Act, 2001 (BTA). While in Sri Lanka the Telecommunications Act empowers the TRCSL to issue directions in times of "*public emergency*" or in the interest of "*public safety and tranquillity*".

See sections 2.2.2, 3.5.2 and 4.2.4 for more detail.

12 'India Protests: Internet Cut to Hunger-Striking Farmers in Delhi' (*BBC News*, 30 January 2021) <https://www.bbc.com/news/world-asia-india-55872480>.

13 Neha Alawadhi, 'Going Offline: Anti-CAA Protests Led to Large Scale Internet Shutdowns' (*Business Standard India*, 21 December 2019) <https://www.business-standard.com/article/economy-policy/going-offline-anti-caa-protests-led-to-large-scale-internet-shutdowns-119122100077_1.html>.

14 Harshit Sabarwal, 'Agnipath Protests: Internet Suspended in 12 Bihar Districts till June 19' (*Hindustan Times*, 17 June 2022). <https://www.hindustantimes.com/cities/patna-news/agnipath-protests-internet-suspended-in-12-bihar-districts-till-june-19-101655474597679.html>.

In Bangladesh, too, complete or partial internet suspension, blocking of social media platforms and restricting the speed of the internet have been used in the face of protests[15] and elections.[16] In 2015, social media was blocked by Bangladesh to prevent any disruption to public order following the death sentence of a war convict.[17]

Sri Lanka has out-right banned public access to social media platforms in situations of violence or public protest, as has been seen in the social media blackout following the 2018 Easter Bombings[18] and the protests in the wake of the 2022 economic crisis.[19] It is significant that Sri Lanka's Ministry of Defence is reported to have played an active role in the recent social media bans.[20]

5.2.2 Blocking Content on Social Media

India[21] and Bangladesh[22] often resort to blocking access to specific pieces of content on social media on grounds of security (see sections 3.5.3 and 4.3.2, respectively). In Sri Lanka, however, there is no legal framework to issue blocking orders for specific pieces

15 Khtisad Ahmed, 'Opinion: Bangladesh Has Damaged Its Democratic Credentials with the Latest Crackdown' (*Scroll.in*, 11 August 2018) <https://scroll.in/article/889870/opinion-bangladesh-has-damaged-its-democratic-credentials-with-the-latest-crackdown>.

16 Press Trust of India, 'Bangladesh Election: Internet Services Suspended, Restored 10 Hours Later' (*Business Standard India*, 28 December 2018) <https://www.business-standard.com/article/international/bangladesh-election-internet-services-suspended-restored-10-hours-later-118122800257_1.html> .

17 'Bangladesh death sentences lead to Facebook ban' *BBC News* (London, 18 November 2015) <https://www.bbc.com/news/world-asia-34860667>.

18 *NetBlocks*, (*Twitter*, 22 April 2019) <https://twitter.com/netblocks/status/1120297427871903744>;'Sri Lanka blocks social media for third time in a month' (*NetBlocks*, 13 May 2019) <https://netblocks.org/reports/sri-lanka-blocks-social-media-for-third-time-in-one-month-M8JRjg80>.

19 'Social media restricted in Sri Lanka as emergency declared amid protests,' (*NetBlocks*, 2 April 2022) <https://netblocks.org/reports/social-media-restricted-in-sri-lanka-as-emergency-declared-amid-protests-JA6ROrAQ>; 'Sri Lanka blocks social media, arrests economic crisis protestors,' (*EconomyNext*, 3 April 2022) <https://economynext.com/sri-lanka-blocks-social-media-arrests-economic-crisis-protestors-92443/>.

20 Zulfick Farzan, 'Imposing Social Media Ban a violation of Human Rights – SL Human Rights Chief' (*News 1st*, 3 April 2022) <https://www.newsfirst.lk/2022/04/03/imposing-social-media-ban-a-violation-of-human-rights-sl-human-rights-chief/ >.

21 Section 69A of the IT Act 2000 provides for blocking on the following grounds: "*interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to them*".

22 Section 8(1) of the CSA in Bangladesh grants discretionary powers to block or remove any content that is seen as a threat to "digital security".The Director General of the Digital Security Agency (now Cyber Security Agency) may, at their discretion, request that the Bangladesh Telecommunication and Regulatory Commission (BTRC) remove or block *any* information that poses a risk to digital security. Further, law enforcement agencies have the authority to ask the BTRC to block or remove any data/information that (i) is published or spread through digital media and (ii) undermines the country's or any part of its "public discipline" or incites racial hostility and hatred. Further, Bangladesh's Draft Regulation for Digital, Social Media and OTT Platforms, 2021 bans content that is against the "spirit of the Liberation War", or poses a threat to communal harmony or public order and integrity.

of content on social media platforms. On the contrary, the government exercises control over its ISPs through licensing and mandates them to block access to entire social media platforms (see section 2.3). This would, however, change if the Online Safety Bill 2023, comes into force in Sri Lanka (see section 2.6.1). As seen through multiple examples across the report, in both India[23] and Bangladesh[24] such content blocking has often resulted in state censorship of dissent.

5.2.3 Criminalisation of Online Speech

All three countries have criminal penalties for citizens for publishing online content that endangers state security.

The CSA (and earlier the DSA) in Bangladesh contain a number of content-based offences that are unique to online communication (sections 21, 24, 28, 29, 31), and some even impose different penalties for similar speech offences offline (see section 29 of the CSA).[25] These content-based offences include criminalising any content which is "*false or a part of the propaganda intended to cause harm to the reputation of the country*"[26] and "*any propaganda or campaign against the liberation war of Bangladesh, the spirit of the liberation war, the national anthem or national flag*"[27] (see section 4.4).

23 See Shirin Ghaffary, 'A Major Battle over Free Speech on Social Media Is Playing out in India during the Pandemic' (Vox, 1 May 2021) <https://www.vox.com/recode/22410931/india-pandemic-facebook-twitter-free-speech-modi-covid-19-censorship-free-speech-takedown>; 'India: Activists Detained for Peaceful Dissent' (*Human Rights Watch*, 15 April 2020) <https://www.hrw.org/news/2020/04/15/india-activists-detained-peaceful-dissent>;Sameer Yasir, 'Climate Activist Jailed in India as Government Clamps Down on Dissent' *The New York Times* (15 February 2021) <https://www.nytimes.com/2021/02/15/world/asia/climate-activist-jailed-india.html>;Katy Migiro, 'India Blocks Journalists' Tweets about Violence against Muslims' (Committee to Protect Journalists, 12 September 2023) <https://cpj.org/2023/09/india-blocks-journalists-tweets-about-violence-against-muslims/>; Vakasha Sachdev, 'Is the Ban on Twitter Accounts of Caravan, Farm Activists Legal?' (*TheQuint*, 1 February 2021) <https://www.thequint.com/news/law/legal-basis-twitter-accounts-caravan-withheld-69a-it-act-blocking-rules-review-and-challenges>;Avi Asher-Schapiro and Ahmed Zidan, 'India Uses Opaque Legal Process to Suppress Kashmiri Journalism, Commentary on Twitter' (Committee to Protect Journalists, 24 October 2019) <https://cpj.org/2019/10/india-opaque-legal-process-suppress-kashmir-twitter/>;Aroon Deep, "Indian government censors tweets critical of Indian internet censorship," *Entrackr*, June 27, 2022, <https://entrackr.com/2022/06/indian-government-censors-tweets-critical-of-indian-internet-censorship/>.

24 See 'Govt Removed over 8,000 Social Media Links in 2022: Report' (*The Daily Star*, 14 October 2022) <https://www.thedailystar.net/tech-startup/news/govt-removed-over-8000-social-media-links-2022-report-3142356>; Twitter Correspondence with Users Reveals Bangladesh Government Attempts to Remove Tweets' (*Netra News*, 3 December 2022) <https://netra.news/2022/twitter-correspondence-with-users-reveals-bangladesh-government-attempts-to-remove-tweets/>; 'Bangladesh: Freedom on the Net 2023 Country Report' (*Freedom House*, 2023) <https://freedomhouse.org/country/bangladesh/freedom-net/2023>.

25 Nowzin Khan, 'From DSA to CSA: The Same Two Bottles of Agony' *The Daily Star* (26 August 2023) <https://www.thedailystar.net/opinion/views/news/dsa-csa-the-same-two-bottles-agony-3403566>.

26 Cyber Security Act 2023, s 25.

27 Cyber Security Act 2023, s 21.

In Sri Lanka, an emergency regulation[28] at one point criminalised digital content, including content on social media, if it spreads "*any rumour or false statement or any information or image or message which is likely to cause public alarm, public disorder or racial violence or which is likely to incite the committing of an offence*."[29] The Online Safety Bill 2023 also introduces vague and overbroad offences, including the prohibition of communications of false statements.[30] It lays several offences like the prohibition of a false statement of fact, which is "a threat to national security, public health or public order or promotes feelings of ill-will and hostility between different classes of people, by communicating a false statement",[31] false statement with the intent to provoke a breach of peace ,[32] to cause mutiny or offence against the state[33] among others (see section 2.6.1)

It is important to note that in India, there are no specialised regulations criminalising online speech detrimental to state security. Online content-based offences mostly contain provisions criminalising non-consensual intimate imagery (NCII) and child sexual abuse material (CSAM).[34] However, penal provisions pertaining to sedition[35] and assertions prejudicial to national integration[36] are invoked against social media users.[37] (see

28 Emergency regulations are made when the President declares an emergency under the public security ordinance. Such regulations are made to maintain "*public security, preservation of public order, suppression of mutiny, riot or civil commotion*".

29 Emergency (Miscellaneous Provisions and Powers) Regulations, No. 1 of 2022, Gazette Extraordinary No. 2278/23.

30 It defines false statements ambiguously as "a statement that is known or believed by its maker to be incorrect or untrue and is made especially with intent to deceive or mislead but does not include a caution, an opinion or imputation made in good faith"

31 Online Safety Bill 2023, s 12(a).

32 Online Safety Bill 2023, s 20.

33 Online Safety Bill 2023, s 21.

34 See Section 66E, 67, 67B of the IT Act.

35 The Indian Penal Code 1860, s 124A.

36 The Indian Penal Code 1860, s 153B.

37 See Mohit Rao, 'Karnataka Has More Sedition Cases Based On Social-Media Posts Than Any State. Most Are Illegal —' *Article 14* (13 July 2021) <https://article-14.com/post/karnataka-has-more-sedition-cases-based-on-social-media-posts-than-any-state-most-are-illegal-60ecf64da7945>; Mohd Dilshad, 'Five Men Arrested in 24 Hrs for Objectionable Posts on Social Media' *The Times of India* (Muzaffarnagar, 16 November 2019) <https://timesofindia.indiatimes.com/city/meerut/five-men-arrested-in-24-hrs-for-objectionable-posts-on-social-media/articleshow/72076928.cms>; Apurva Vishwanath, 'Pawan Khera Arrest | Section 153A: Its Use and Misuse' *The Indian Express* (25 February 2023) <https://indianexpress.com/article/explained/explained-law/section-153a-its-use-and-misuse-pawan-khera-arrest-supreme-court-8465400/>.

section 3.5.1) This trend of invoking penal provisions for online content is also visible in the sedition provisions in Bangladesh[38] and Sri Lanka's use of ICCPR Act[39] and penal provisions pertaining to exciting or attempting to excite disaffection[40, 41]

Overbroad restrictions on speech based on ambiguous terms such as – "*any kind of propaganda or campaign against liberation war, spirit of liberation war, father of the nation, national anthem or national flag*", "*interests of security*" or "*public order*" – risks criminalising legitimate expression. Such vagueness is amplified by the absence of adequate checks and balances. As a result, such provisions are easily misused by the executive to censor dissenting opinions and create a chilling effect on free speech and expression.

Cyberterrorism

In each of the three countries, laws governing information and communication technologies explicitly criminalise the use of computer resources to threaten national security.

Bangladesh and India have cyberterrorism laws. In Bangladesh, section 27 of the CSA defines 'cyber terrorism' which includes disruption or unauthorised access to computer resources that threaten the integrity, security and sovereignty of the state (see section 4.3). Similarly, in India, section 66F of the IT Act underlines the cyberterrorism provisions which aim to thwart unauthorised access to information impacting "state security" among other things (see section 3.2.4).

38 See Meenakshi Ganguly, 'Dispatches: Bangladesh's Machete Attacks On Free Speech | Human Rights Watch' (18 August 2015) <https://www.hrw.org/news/2015/08/18/dispatches-bangladeshs-machete-attacks-free-speech>; HT Correspondent, 'Student Faces Sedition Charges over FB Post' *Hindustan Times* (Dhaka, 3 June 2012) <https://www.hindustantimes.com/world/student-faces-sedition-charges-over-fb-post/story-yKGAnLvDNUtCWqQWFVCMyL.html>;Star Digital Report, 'JS Body for Sedition Charges against Those Spreading Propaganda through Social Media' *The Daily Star* (10 February 2021) <https://www.thedailystar.net/bangladesh/news/js-body-sedition-charges-against-those-spreading-propaganda-through-social-media-2042581>.

39 See 'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*, 2021) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>; Colombo Telegraph, 'Friends In High Places Saving Columnist Kusal Perera: Unequal And Arbitrary Application Of ICCPR' (Colombo Telegraph, 2019) <https://www.colombotelegraph.com/index.php/friends-in-high-places-saving-columnist-kusal-perera-unequal-and-arbitrary-application-of-iccpr/>;'Sri Lanka: Due Process Concerns in Arrests of Muslims' (*Human Rights Watch*, 23 April 2020) <https://www.hrw.org/node/341285/printable/print>.

40 See 'Youth Activist behind #GoHomeGota Facebook Campaign Arrested and Produced in Court' The Sunday Times, Sri Lanka (3 April 2022) <http://www.sundaytimes.lk/220403/news/youth-activist-behind-gohomegota-facebook-campaign-arrested-and-produced-in-court-479036.html>.

41 Penal Code Ordinance No 11 1887, s 120.

Although Sri Lanka does not have explicit cyber terrorism provisions, Section 6 of the CCA criminalises the use of computer resources to commit offences that endanger "national security or public order".[42] Even though the above-mentioned provisions in Sri Lanka and India do not explicitly target online user content, broad interpretations of the law have led to arrests of social media users for sharing content.[43, 44, 45]

5.2.4 Law Enforcement Access to User Data

All three countries have laws requiring intermediaries to assist relevant state authorities in intercepting and monitoring citizen data on grounds of state security.

India's IT Act grants expansive monitoring and interception powers to the government on grounds like sovereignty and integrity or security of the state or defence of India or investigation of any offence.[46] (see section 3.5.5) Bangladesh's interception and monitoring provisions are similar and the BTA empowers the state to monitor and intercept citizen data on grounds of "*security of the state and public tranquillity*".[47] (see section 4.2.2) The Sri Lankan Telecommunications Act, too, provides a broad range of powers to the Minister in charge to issue interception orders in the event of "*occurrence of any public emergency or in the interest of public safety and tranquillity*".[48] (see section 2.2.2) The executive wields considerable discretion in the absence of judicial oversight in all three countries. Such concentration of power heightens concerns about unbridled surveillance being justified due to state security.

42 Computer Crime Act No 24 2007< https://www.lawnet.gov.lk/act-no-24-of-2007/>.

43 Amani Nilar, 'Police arrests man for posting fake photos of COVID-19 deceased' *News 1st* (Colombo, 24 August 2021) <https://www.newsfirst.lk/2021/08/24/police-arrests-man-for-posting-fake-photos-of-covid-19-deceased/>

44 PTI, 'Haryana: Journalist Booked For "Cyber-Terrorism" Over Social Media Post' (*The Wire*, 11 April 2021) <https://thewire.in/media/haryana-journalist-booked-for-cyber-terrorism-over-social-media-post>.

45 Safwat Zargar, 'Kashmiri Students Charged with Cyberterrorism, Sedition for Allegedly Cheering Pakistan Cricket Team' (*The Scroll*, 29 January 2022) <https://amp.scroll.in/article/1016166/illegal-custody-says-lawyer-of-three-kashmiri-students-held-in-an-agra-jail-for-three-months>.

46 Section 69 of the IT Act deals with interception, monitoring or decryption of information transmitted, received or stored through any computer resource. Further, as discussed in section 3.3.4, Rule 4(2) of the Intermediary Guidelines 2021, requires significant social media intermediaries (SSMIs) primarily providing messaging services to identify the "first originator" of a message upon receiving an order from a court or other competent body under Section 69 of the IT Act. Section 91 of the CrPC has also been used by LEAs to request data from intermediaries for investigations(see 3.5.5).

47 Bangladesh Telecommunication Regulatory Act 2001, s 97A.

48 Sri Lanka Telecommunications Act No 25 1991.

5.2.5 Conclusion

It is clear from the above discussion that social media regulation in all three countries relies on governing the information ecosystem through security imperatives. We also observe that security concerns are often dealt with by countries in a way that does not comply with democratic principles of accountability and transparency.[49] This security lens to regulation can result in the reduced scope of democratic debate and political dissent.

As seen across the report, states have attempted to censor political speech on social media in the interest of state security. This trend was also witnessed during the pandemic when arresting citizens and content-blocking orders to platforms were sent in the context of posts critical of the State.[50]

5.3 Executive Discretion and Limited Transparency

It is evident from the analysis of the country profiles that the executive in all three countries exercises excessive discretionary powers, with limited judicial and parliamentary oversight over several aspects of social media regulation. Further, state orders for content takedown or requests for user data to platforms are not disclosed publicly. This can be attributed to either legally mandated confidentiality provisions or due to the absence of procedural safeguards mandating such disclosures.[51] This secrecy[52] further empowers the executive

49 Jason Gratl and Andrew Irvine, 'National Security, State Secrecy and Public Accountability' (2005) 54 UNBLJ 251.

50 In Sri Lanka, arrests were made under the Quarantine Act, Penal Code, Computer Crime Act and ICCPR with the ostensible goal to curb misinformation (see section 2.3).

51 In India, the Disaster Management Act was deployed to criminalise online speech and blocking notices for content critical of the government's handling of the pandemic were issued. See Karan Deep Singh and Paul Mozur, 'As Outbreak Rages, India Orders Critical Social Media Posts to Be Taken Down' (*The New York Times*, 25 April 2021) <https://www.nytimes.com/2021/04/25/business/india-covid19-twitter-facebook.html>; (see section 3.5.1)

In Bangladesh, internet shutdowns, and arrests and arbitrary detentions were made under various provisions of the ICT and DSA to curb dissent during the pandemic. (see section 4.9.1)

The orders received under section 69A of the IT Act are governed by the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. Rule 16 outlines strict confidentiality of the content takedown orders issued by the government and the response of the intermediary to such requests. Similarly, with regards to requests for user data, Rule 25(4) of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 mandates confidentiality.Although similar confidentiality provisions do not exist in Sri Lanka and Bangladesh, there is an absence of procedural safeguards that mandate such disclosures. Refer to 5.3.4 for more details.

52 Secrecy of executive action refers to orders, directions and guidelines that are not officially available to the general public.

to exercise its regulatory powers with limited judicial and legislative[53] oversight. This lack of checks and balances also diminishes public oversight and accountability.

It is important to note at this point that states across the globe often grant greater executive discretion in addressing security imperatives,[54] with some degree of secrecy being a regular part of national security governance.[55] Secrecy, in such contexts, is often exercised to maintain the confidentiality of sensitive government programs, prevent circumvention or otherwise increase a program's effectiveness, or avoidance of public opposition.[56] The security standard takes precedence over public oversight in cases when disclosure would diminish the efficacy of such actions.

As social media platforms become increasingly relevant to states' security apparatus, social media regulation will in some way reflect the security imperatives of states.[57] For instance, interception and monitoring are important mechanisms that assist in ongoing investigations, enable the gathering of actionable intelligence and secure national security and public order imperatives of the executive. However, the clandestine nature of interception and monitoring capabilities of the state, along with the lack of adequate procedural safeguards (transparency of issued orders) and checks and balances (such as judicial oversight) can negatively impact the fundamental freedoms of individuals.[58, 59]

53 Sanjana Nayak, "Administrative Law and Doctrine of Excessive Delegation," (2020) International Journal of Legal Science and Innovation <https://www.ijlsi.com/wp-content/uploads/Administrative-Law-and-Doctrine-of-Excessive-Delegation.pdf>.

54 See Thierry Balzacq, *A Theory of Securitization: Origins, Core Assumptions, and Variants* (Routledge 2010).

55 Marlen Heide and Jean-Patrick Villeneuve, 'Framing National Security Secrecy: A Conceptual Review' (2021) 76 International Journal: Canada's Journal of Global Policy Analysis 238.

56 Jonathan Manes, "Secret Law" (2018) Georgetown Law Journal 106 <https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2018/06/Secret-Law.pdf>.

57 Elena Chachko, 'National Security by Platform' (2021) 25 Stanford Technology Law Review.

58 Regina Mihindukulasuriya, 'Who Legally Authorises Data Interception & on What Grounds: A Study of 5 Democracies' (*ThePrint*, 30 January 2022) <https://theprint.in/india/who-legally-authorises-data-interception-on-what-grounds-a-study-of-5-democracies/816613/>.

59 PTI, 'Point out Law and Procedure for Monitoring, Interception of Phones: HC to Centre' (*The Economic Times*, 31 August 2021) <https://economictimes.indiatimes.com/news/india/point-out-law-and-procedure-for-monitoring-interception-of-phones-hc-to-centre/articleshow/85799356.cms?from=mdr>.

Thus, while the state may have legitimate security interests in social media governance, safeguards against executive discretion are imperative to ensure democratic accountability.[60] When left unchecked, executive control has the propensity to negatively impact democratic values and undermine procedural and substantive safeguards that preserve individual liberty.[61]

The subsequent sections, trace how executive discretion and limited accountability play out in the three jurisdictions:

5.3.1 Limited Parliamentary Oversight

The executive in India and Sri Lanka plays a central role in enforcing and formulating laws through delegated legislation[62] and ordinances.[63] Such law-making mechanisms limit parliamentary oversight and grant excessive discretionary power to the executive. Another important trend noted across the country chapters is the absence of or ineffectiveness of a consultative process in drafting legislation, which limits the scope of public oversight from independent technical experts, Civil Society Organisations, academia etc.[64]

60 Elonnai Hickok, 'Policy Brief: Oversight Mechanisms for Surveillance — *The Centre for Internet and Society*' (CIS, 2015) <https://cis-india.org/internet-governance/blog/policy-brief-oversight-mechanisms-for-surveillance#fn2>.

61 CM(2008)170, The Council of Europe and the Rule of Law, s 46, <https://www.coe.int/t/dc/files/Ministerial_Conferences/2009_justice/CM%20170_en.pdf>.

62 MeitY has imposed due diligence obligations on social media platforms through delegated legislation in the form of Intermediary Guidelines 2021 (see section 3.3).

63 The power to issue an '*ordinance*' highlights the legislative role performed by the executive in case of an emergency. The ordinance is a temporary but legally binding order that can introduce legislative changes. However, it can be enforced for a specific period and subsequently needs to be either re-introduced or embedded into the legal framework. In Sri Lanka, the issuing of emergency ordinances has been noted in section 2.2.2.

64 For instance, in India, the Intermediary Guidelines 2021 were passed without any meaningful public consultation. See Torsha Sarkar, 'New Intermediary Guidelines: The Good and the Bad' [2021] *Down To Earth* <https://www.downtoearth.org.in/blog/governance/new-intermediary-guidelines-the-good-and-the-bad-75693>.In Sri Lanka, the Online Safety Bill 2023 has been criticised for being introduced without any public consultation. See *Niresh Eliatamby, 'BASL Demands Withdrawal of Anti-Terrorism and Online Safety Bills'* (23 September 2023) <https://english.newsfirst.lk/2023/9/23/basl-demands-withdrawal-of-anti-terrorism-and-online-safety-bills>.

In Bangladesh, the recent passing of the CSA has been criticized for lack of public consultation.

See Nowzin Khan, 'From DSA to CSA: The Same Two Bottles of Agony' *The Daily Star* (26 August 2023) <https://www.thedailystar.net/opinion/views/news/dsa-csa-the-same-two-bottles-agony-3403566>.

5.3.2 Limited Judicial Oversight

In India, the executive can issue content takedown orders under section 69A of the IT Act, and there is no requirement to obtain judicial sanction for such orders.[65] Similarly, broad executive discretion and the absence of judicial oversight prevails in section 69 of the IT Act, which regulates government access to user data via monitoring and interception.[66]

Similarly, in Bangladesh, the Director General under the CSA can request the BTRC to issue takedowns or blocking orders against any information that "creates threat to digital security".[67] Further, the BTA enables interception and monitoring on broad grounds of national security and public order without any judicial sanction.[68] No procedural safeguards mandate the disclosure of monitoring orders or place limits on the duration of interception in Bangladesh.[69] This law provides overbroad power to the executive, to authorise intelligence agencies, investigation agencies, or any officer of law enforcement agencies to prohibit the transmission, record, or collection of user information.[70] The Digital Security Agency (now Cyber Security Agency) has been given absolute power to (i) initiate investigations, (ii) order the BTRC to remove and block any information or data on the internet and (iii) arrest anyone without any warrant or court order.[71] Due to no ex-ante judicial sanction and a lack of basic safeguards such as requirement of warrants before arrests, there is scope for gross misuse of this power.[72]

65 Revathi Krishnan Mihindukulasuriya Regina, 'Accounts of Prasar Bharati CEO, Caravan, Actor Sushant Singh among Those "withheld" by Twitter' (*ThePrint*, 1 February 2021) <https://theprint.in/india/accounts-of-prasar-bharati-ceo-caravan-actor-sushant-singh-among-those-withheld-by-twitter/596638/>.

66 In the past, the Supreme Court of India upheld the constitutional validity of section 69A of the IT Act and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules), although it did introduce some procedural safeguards for content blocking. However, recently two cases have brought questions of due process back to the forefront.

The petitioners in *Tanul Thakur v Union of India and X v. Union of India* have challenged the validity of the content blocking process. They contend that the procedural safeguards introduced by the Supreme Court are no longer being followed. For instance, one of the major grounds of challenge is that users/originators (those who post content) are not furnished with the blocking orders. It is essential to provide them with the same, so that they can, if they wish to, seek judicial oversight by challenging the blocking orders before a High Court.

67 Cyber Security Act 2023, s 8(1).

68 Bangladesh Telecommunication Regulatory Act 2001, s 97 (A).

69 'Bangladesh Country Report' (*Telenor*, 2017) <https://www.telenor.com/binaries/sustainability/responsible-business/handling-access-requests-from-authorities/Authority-Request-Legal-Overview_March-2017-bangladesh.pdf >.

70 Bangladesh Country Report' (*Telenor*, 2017) <https://www.telenor.com/binaries/sustainability/responsible-business/handling-access-requests-from-authorities/Authority-Request-Legal-Overview_March-2017-bangladesh.pdf >

71 'Bangladesh: New Digital Security Act is attack on freedom of expression'(*Amnesty International*, 2018) <https://www.amnesty.org/en/latest/press-release/2018/11/bangladesh-muzzling-dissent-online/>.

72 Ibid.

In Sri Lanka, social media regulation is yet to be codified. This lacuna is highlighted through the non-standardised method of restricting social media access[73] and website blocking mechanism.[74] Although the Sri Lanka Telecommunications Act empowers the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) to issue blocking orders to Internet Service Providers (ISPs), the procedure and safeguards for the same are not known publicly.[75] The case studies in the Sri Lanka chapter highlighted that the President exercises discretion through various executive authorities on broad grounds such as "damaging the President's reputation."[76] (see section 2.7)

5.3.3 Lack of Independent Regulators

The absence of independent regulators across the three jurisdictions also contributes to the centralisation of power in the hands of the executive. India lacks a specialised independent regulator for online platforms. Instead, various ministries (MeitY, MIB, and MHA) are the key institutions for social media regulation in India (see section 3.4.2).

In Sri Lanka, TRCSL, the telecom regulator, wields significant power over platforms (see sections 2.3 and 2.5). While the TRCSL was established as an autonomous regulatory body, this has not been translated into practice. It has faced criticism due to allegations of partisanship and corruption, particularly in relation to undue influence exerted by the President.[77]

73 'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*, 2021) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>.

74 Raisa Wickremetunge, 'Blocked: RTI Requests Reveal Process behind Blocking of Websites in Sri Lanka' (*Groundviews*, 8 December 2017) <https://groundviews.org/2017/12/08/blocked-rti-requests-reveal-process-behind-blocking-of-websites-in-sri-lanka/>.

75 As observed in the case study on protest against the 2022 Economic Crisis (see section 2.2.5), the Ministry of Defence (MOD) issued a request to the TRCSL to ask service providers to restrict access to social media platforms. The request to restrict access to social media was criticised by the Human Rights Commission of Sri Lanka (HRCSL), which observed that the TRCSL had "no authority" to ask service providers to restrict access to social media, on the basis of a "request from the Ministry of Defense". The exercise of discretion by the government was widely criticised by opposition political parties, journalists, and lawyers resulting in the rollback of the social media ban.Website blocking requests can also originate from the Mass Media Ministry and the Presidential Secretariat. However, due to the lack of an effective oversight mechanism, such executive-actions cannot be brought to the public forum for scrutiny.

76 Raisa Wickremetunge, 'Blocked: RTI Requests Reveal Process behind Blocking of Websites in Sri Lanka' (Groundviews, 8 December 2017) <https://groundviews.org/2017/12/08/blocked-rti-requests-reveal-process-behind-blocking-of-websites-in-sri-lanka/>.

77 Malathy Knight-John, 'Telecom Regulatory and Policy Environment in Sri Lanka: Results and Analysis of the 2008 TRE Survey' [2008] SSRN Electronic Journal <http://www.ssrn.com/abstract=1555595>.

In Bangladesh too, the telecom regulator, BTRC, exercises considerable influence over platforms through measures such as internet suspensions, blocking, and interception; however, its independence has been called into question.[78] Additionally, the Digital Security Agency (to be reconstituted as the National Cyber Security Agency)[79] holds significant powers with respect to enforcing the CSA and safeguarding "digital security". It also has the power to advise BTRC to block specific content online.[80] However, the influence of the executive on the Cyber Security Agency ("Agency") cannot be underestimated, given that the members of the agency are appointed by the government.[81] Further, the agency is advised by the National Cyber Security Council which is comprised of the Prime Minister as the Chairman and several ministers, departmental secretaries, law enforcement and intelligence officials as its members.[82]

5.3.4 Confidentiality Provisions and Opaque Executive Action

In India, the state takedown orders are enforced with "strict confidentiality" and platforms in India are not allowed to make any information public about the orders so received.[83] Procedural safeguards do require the government to make "all reasonable efforts" to identify the originator of the information or intermediary and provide a 48-hour window for them to respond and clarify.[84] But this has not been followed in practice and has recently come under judicial scrutiny.[85] This practice of confidential takedown orders has prevented the aggrieved end-users from exercising their right to challenge executive blocking orders in court. This also leads to the executive unilaterally deciding what speech breaches the constitutionally demarcated free speech.

78 'Bangladesh: Freedom on the Net 2023 Country Report' (*Freedom House*) <https://freedomhouse.org/country/bangladesh/freedom-net/2023>.

79 Zahidur Rabbi, 'Bangladesh Govt. Forms "National Cyber Security Agency"' *The Daily Star* (21 November 2023) <https://www.thedailystar.net/tech-startup/news/bangladesh-govt-forms-national-cyber-security-agency-3475501>.

80 Section 8(1) of the CSA in Bangladesh grants discretionary powers to block or remove any content that is seen as a threat to "digital security".

81 Cyber Security Act 2023 s 6.

82 Cyber Security Act 2023 s 12.

83 The orders received under section 69A of the IT Act are governed by the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. Rule 16 outlines strict confidentiality of the content takedown orders issued by the government and the response of the intermediary to such requests. Similarly, with regards to requests for user data, Rule 25(4) of the Information Technology ((Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 mandates confidentiality.

84 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009, Rule 8.

85 Vasudev Devadasan, 'The Phantom Constitutionality of Section 69A: Part I' (*Indian Constitutional Law and Philosophy*, 22 October 2022) <https://indconlawphil.wordpress.com/2022/10/22/the-phantom-constitutionality-of-section-69a-part-i/>.

Even when there are no confidentiality provisions and safeguards mandate public disclosure, as in the case of internet suspensions, there is still a level of opacity when it comes to implementation and often orders are not made public.[86] India has codified the law for internet suspension[87] and notified procedural safeguards .[88] In the *Anuradha Bhasin* case,[89] the Supreme Court of India highlighted the need for publishing internet suspension orders. The court opined that "*a democracy, which is sworn to transparency and accountability, necessarily mandates the production of orders as it is the right of an individual to know*." The court held that the suspension orders must pass the test of proportionality and necessity by compulsorily publishing and allowing judicial oversight over such orders that restrict fundamental freedoms. However, in practice, internet suspension orders are often not made public.[90]

Further, the executive review committees for blocking, interception and internet suspension fail to entrench any accountability given their workings are non-transparent with little information in the public domain.

When it comes to Sri Lanka[91] and Bangladesh,[92] although the law does not place any limits on the extent or disclosure of such orders, there do not exist any procedural safeguards to entrench transparency either. This discourages transparency of executive action in practice.

86 *Internet Freedom Foundation*, '6 Months after Anuradha Bhasin v. UoI, State Governments Are Still Not Publishing Internet Shutdown Orders #KeepUsOnline' (*Internet Freedom Foundation*, 14 July 2020) <https://internetfreedom.in/publication-internet-shutdown-orders/>.

87 The Indian Telegraph Act 1885, s 5(2).

88 The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017.

89 *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.

90 *Internet Freedom Foundation*, '6 Months after *Anuradha Bhasin v. UoI, State Governments* Are Still Not Publishing Internet Shutdown Orders #KeepUsOnline' (*Internet Freedom Foundation*, 14 July 2020) <https://internetfreedom.in/publication-internet-shutdown-orders/>.

91 Sri Lanka Telecommunications Act 1991, section 54(3) lays down the conditions for lawful interception.However, there are no procedural safeguards mandated for the same.

92 Bangladesh Telecommunication Regulatory Act 2001, Section 97(A) gives the government of Bangladesh the powers to conduct interception, monitoring and censorship of information on the grounds of national security and public order. However, there are no procedural safeguards mandated for the same.

5.3.5 Limitations of the Right to Information

The codified transparency mandates have often proven ineffective. This can be observed across Bangladesh,[93] India[94] and Sri Lanka[95] through the refusal of '*right to information*' (RTI) requests that seek information about governmental blocking orders.

In Bangladesh, RTIs can be denied on twenty-two vague grounds under the RTI Act.[96] The RTI act also allows eight intelligence and security agencies to be exempted from the purview of information requests.[97] (see section 4.9.2)

The TRCSL in Sri Lanka also refused to furnish social media suspension orders or any communication from the suspension request by MOD.[98] The request was rejected on the grounds that "disclosure of such information would undermine the defence of the state or national security."[99] TRCSL also denied RTI requests in 2018, on the grounds of national security and suggesting that it has no recorded interactions with ISPs challenging its blocking orders.[100]

In India, the RTI requests have met a similar fate of denial on grounds of national security. One such example is an RTI on the surveillance capabilities of the state.[101] The RTI requested information on the total number of surveillance orders, the number of surveillance requests by law enforcement agencies, etc.[102] The RTIs were denied on the

93 Sohini Paul, 'Right to Information Act 2009 Summary: Bangladesh' (*Human Rights Initiative*) <https://www.humanrightsinitiative.org/programs/ai/rti/international/laws_papers/bangladesh/bangladesh_rti_act_2009_summary.pdf>.

94 See Saurav Das, 'The Court Case That Could Change the Way Government Blocks Info on Censorship' (*The Wire*, 14 June 2023) <https://thewire.in/rights/dowry-calculator-censorship-information-india>; Livemint, 'RTI Applications Rejected over National Security up 83% in 2020-21: Report' (*Mint*, 5 March 2022) <https://www.livemint.com/news/india/rti-applications-rejected-over-national-security-up-83-in-2020-21-report-11646472679235.html>.

95 'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>.

96 Right to Information Act 2009, s 7.

97 Right to Information Act 2009, s 31.

98 Hashtag Generation, 'Our Right to Information Request to the…' (Twitter, 27 April 2022) <https://twitter.com/generation_sl/status/1519272806533693440?cxt=HHwWgIDQ5a2kxZUqAAAA>.

99 Right to Information Act 2016, s 5 (1) b (i).

100 'Sri Lanka: Freedom on the Net 2021 Country Report' (*Freedom House*) <https://freedomhouse.org/country/sri-lanka/freedom-net/2021>.

101 List of RTIs Applications Filed in the Appeals <https://docs.google.com/document/d/1fu_q9HK83a-HrxLjPB-8lo5BKvRcjjkwxYtZT5E84aI/edit>

102 Yashaswini, Krishnesh Bapat, and Tanmay Singh, '„Information Sought Is Not Available": MHA Claims to Have Destroyed All Records When Asked Total Number of Surveillance Orders' (*Internet Freedom Foundation*, 6 August 2021)<https://internetfreedom.in/information-sought-is-not-available-mha-claims-to-have-destroyed-all-records-when-asked-total-number-of-surveillance-orders/>.

grounds of national security, interference with ongoing investigations, and endangering the life and safety of persons.[103] RTI requests seeking copies of blocking orders have been denied, citing the confidentiality clause in the blocking rules.[104]

5.3.6 Overbroad and Vague Security Exemptions in All Three Countries

Across all three jurisdictions, security imperatives of the state are defined in overbroad and vague terms which are open to executive interpretation. For instance, the executive can issue orders to block content[105] or initiate interception and monitoring[106] orders on various grounds, such as "*sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order*" in India, internet suspensions can also be ordered on similar grounds in cases of "public emergency" or in the interest of "public safety".[107] Similarly in Bangladesh, content can be blocked if it creates a threat to "*digital security*"[108] or "*solidarity*", "*security*", "*defence*", "*public discipline of the country or any part thereof*" among others.[109] The state can initiate interception on the grounds of "*security of the state and public tranquillity*" in Bangladesh.[110] In Sri Lanka, interception can be invoked on vague grounds like "*occurrence of any public emergency or in the interest of public safety and tranquillity*.[111]

103 Ibid.

104 Saurav Das, 'The Court Case That Could Change the Way Government Blocks Info on Censorship' (*The Wire*, 14 June 2023) <https://thewire.in/rights/dowry-calculator-censorship-information-india>

105 IT Act 2000, s 69A.

106 IT Act 2000, s 69.

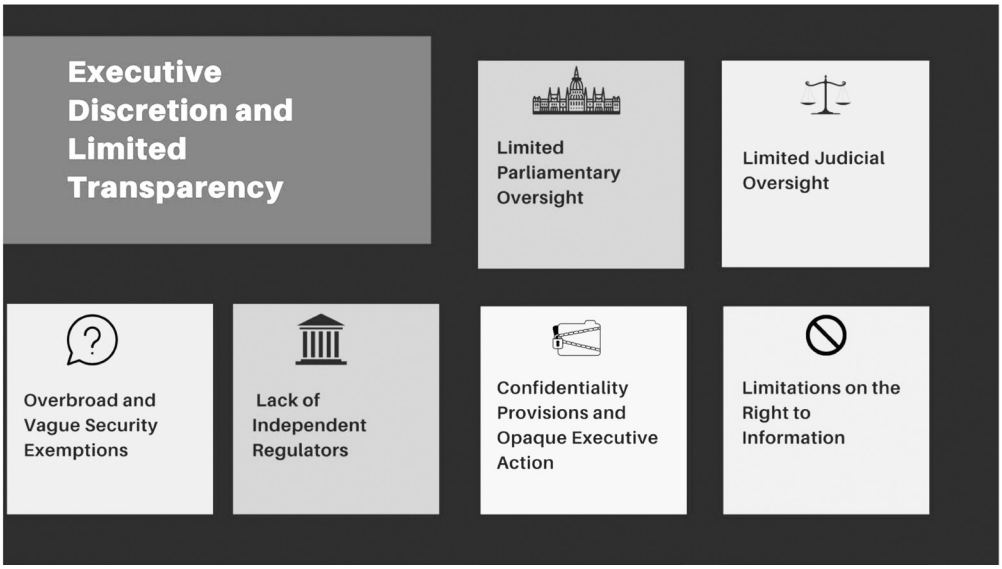
107 The Indian Telegraph Act, 1885, s 5(2) lays down that internet can be suspended by the state or the centre if it is necessary or expedient so to do in the interests of the internet as in the *interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence* for reasons to be recorded in writing.

108 CSA 2023, s8(1) empowers the Director General of the Digital Security Agency to request the BTRC to remove content.

109 CSA 2023, s8(2) empowers LEA to request the BTRC to remove content that that hampers "*solidarity, financial activities, security, defence, religious values or public discipline of the country or any part thereof, or incites racial hostility and hatred*" .

110 Bangladesh Telecommunication Act, 2001 s 97(A).

111 Sri Lanka Telecommunications Act No 25 1991.



5.4 Recommendations

There is a growing tendency of the State across the three countries to exert control over the online information ecosystem through various legislative developments. It is observed that inadequate substantive and procedural safeguards lead to (a) discretionary interpretation of legal provisions and (b) selective/abrupt implementation by executive authorities. The absence of sufficient safeguards can also perpetuate discriminatory outcomes and negatively impact end-users, especially historically marginalised or vulnerable groups, as seen across the three country chapters.

Some of the key rule of law concerns highlighted in the previous sections include wide and ambiguous penal provisions; overbroad and vague security exceptions, lack of adequate procedural safeguards such as the right to a hearing, reasoning and notice; lack of judicial and parliamentary oversight; excessive executive discretion and centralisation of power; and overcriminalisation of online speech and expression.

This section provides recommendations to strengthen the rule of law and engender greater accountability in social media governance:

5.4.1 Limiting the Scope of National Security Exceptions

States' pursuit of national security objectives and citizens' civil liberties have historically been at odds with one another. This juxtaposition of national security and human rights has also translated to social media regulation, where states often use national security imperatives to control the flow of information. Since national security crises are associated with an existential threat to the state and society, they enable the executive to suspend ordinary due process considerations and wield exceptional power.[112] This comes with the risk of abuse of these provisions, especially in the absence of proper checks and balances.

Overbroad, unclear and ambiguous definitions of key terms and offences in legislation and/or regulations leave room for discretion in interpretation, which could lead to discriminatory and unfair enforcement. States often abuse such provisions to curb dissent and impose censorship and surveillance, as seen in the previous chapters. These also have a chilling effect and lead to self-censorship and collateral private censorship. Thus, precise and narrow definitions can be the first step towards preventing state overreach.

From a rule of law perspective, in a democracy, an independent judiciary performs the balancing of competing interests of national security and individual rights. Here, the onus lies on the executive to establish the necessity of an exceptional action based on national security considerations. The three-part test[113] has been used across jurisprudence to evaluate when freedom of expression can be legitimately restricted, "(i) the restriction is provided by law; (ii) the grounds for the restriction are specific: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order or of public health or morals' (iii) the restriction is necessary to a democratic society and proportionate".

States can also take a cue from international developments to determine what can be considered legitimate, necessary and proportional national security exceptions. The Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR, for instance, state that national security exceptions can only be invoked when there are effective safeguards and remedies against abuse in place. National security exceptions cannot be used by states to suppress opposition to its human rights violations or repression of its citizens.[114]

112 See Thierry Balzacq, *A Theory of Securitization: Origins, Core Assumptions, and Variants* (Routledge 2010).

113 Agnes Callamard, 'Freedom of Expression and National Security: Balancing for Protection' [2015] Columbia Global Freedom of Expression.

114 The principles state, "*The systematic violation of human rights undermines true national security and may jeopardize international peace and security. A state responsible for such violation shall not invoke national security as a justification for measures aimed at suppressing opposition to such violation or at perpetrating repressive practices against its population*."

See UN Commission on Human Rights, 'The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights' [1984] E/CN.4/1985/4 .

The Johannesburg Principles on National Security, Freedom of Expression and Access to Information[115] put together by independent experts built on the foundational Siracusa principles. These elaborate that a restriction on grounds of national security is not legitimate "unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government".[116]

It also states that measures taken to suppress industrial unrest, uphold an ideology, and prevent embarrassment to the government or public institutions do not constitute a national security interest. The principles also prohibit any form of discriminatory action on the grounds of national security.[117] The principles enumerate the categories of peaceful expression that cannot be restricted based on national security, including advocacy of change in government or government policy; criticism/ insult of state, nation, its symbols and institutions; or bringing to light international human rights violations.[118]

The Johannesburg Principles also lay down the grounds for ascertaining that an expression constitutes a threat to national security such that "(a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence".[119]

Thus, applying national security exceptions requires careful deliberation and judicial oversight to balance competing rights. However, given the speed and scale of online information flows, case-by-case judicial scrutiny might not always be feasible. Hence, overbroad exceptions on national security become even more risky, especially if decisions are taken by a powerful executive, or are delegated to private platforms under strict timeframes. As a result, having targeted and narrow definitions becomes even more crucial.

As seen through the report, national security exceptions are mobilised to regulate information flows through certain mechanisms. It is thus crucial to strengthen procedural safeguards and checks and balances for them as seen in the following section.

115 Article 19, 'Johannesburg Principles on National Security, Freedom of Expression and Access to Information' (1996).

116 Article 19, 'Johannesburg Principles on National Security, Freedom of Expression and Access to Information' (1996) principle 8.

117 Article 19, 'Johannesburg Principles on National Security, Freedom of Expression and Access to Information' (1996), principle 4.

118 Article 19, 'Johannesburg Principles on National Security, Freedom of Expression and Access to Information' (1996), principle 7.

119 Article 19, 'Johannesburg Principles on National Security, Freedom of Expression and Access to Information' (1996), principle 6.

5.4.2 Checks and Balances for Social Media Regulation

It is evident from the discussion in the chapter that the regulation of the online information ecosystem can result in overbroad censorship or surveillance without adequate checks and balances against misuse of state power. This section provides recommendations to strengthen the rule of law and engender greater accountability in legislation pertaining to the above.

5.4.2.1 Criminalisation of Online Speech

The impact of employing often overly broad and vague criminal laws to counter harmful content can result in overcriminalisation of speech. Such laws impose disproportionate restrictions on users through misuse and arbitrary enforcement. Laws that criminalise vague categories of speech, such as content that is "grossly offensive or has menacing character"[120] or "propaganda against national symbols",[121] can lead to discriminatory enforcement and censorship, as seen across the report.

Similarly, when harmful speech like violent and extremist content is defined in ambiguous terms, it vests discretionary power in the hands of both platforms and the State, especially in the absence of adequate checks and balances.[122] Thus, online harms, like CSAM, NCII, extremist and violent speech, necessitate a clear and targeted set of definitions that articulate the key elements of what constitutes harmful speech online. Further, it is important that similar speech harms are treated uniformly across all forms of media and higher penalties are not imposed for online speech. Several States are bringing provisions to criminalise disinformation.[123] This leads to States and platforms to assume the position

120 In India, section 66A of the IT Act criminalised sending information through a computer resource or communication device:(a) information that is "grossly offensive or has menacing character"; (b) information known to be false but shared with the aim of causing "annoyance, inconvenience, danger , obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently"; (c)any email or message for causing annoyance or inconvenience or to deceive or mislead about the origin of such messages..It was declared unconstitutional in the *Shreya Singhal v Union of India*.

121 In Bangladesh, section 25 of the CSA considers the transmission of offensive, false, or threatening online information, with the aim of humiliating or harming a person's reputation or engaging in propaganda to damage the country's image, as an offence. prohibition of "communication of false statements"

122 Evelyn Douek, 'Australia's" Abhorrent Violent Material" Law: Shouting" Nerd Harder" and Drowning Out Speech'(2020)' 94 ALJ 41; Daphne Keller, 'Internet Platforms: Observations on Speech, Danger, and Money' [2018] Hoover Institution's Aegis Paper Series.

123 In Bangladesh, section 25 of the CSA considers the transmission of offensive, false, or threatening online information, with the aim of humiliating or harming a person's reputation or engaging in propaganda to damage the country's image, as an offence. In Sri Lanka, the Online Safety Bill 2023, prohibits the "communication of false statements". Similar regulatory interventions exist across several jurisdictions. See International Center for Not-for-profit Law, *Legal Responses to Disinformation* (ICNL 2021); Ric Neo, 'The Securitisation of Fake News in Singapore' (2020) 57 International Politics 724 <https://www.researchgate.net/profile/Ric-Neo/publication/336270460_The_securitisation_of_fake_news_in_Singapore/links/5f15544692851c1eff2183bb/The-securitisation-of-fake-news-in-Singapore.pdf>.

of "arbiters of truth", which can result in censorship and over removal of legitimate political speech and dissent.[124] Criminalisation is not the best step to tackle speech harms like dis/misinformation.[125]

In this context, it must also be pointed out that overreliance on criminalisation measures does not address the systemic issues associated with harmful content.[126] It is essential that an attempt to understand the context of the online information-sharing ecosystem is made in future frameworks. This becomes particularly important in understanding disinformation and hate speech amplification.

When criminal laws that were originally designed to address physical or offline harms are applied to online speech, they focus solely on the content of individual posts and the identity of a particular user posting them instead of understanding the networks of amplification and consequent virality associated with such harmful content online. The criminalisation of online content must deal with multiple actors and networks of individuals re-sharing or interacting with illegal online content which necessitates careful consideration.

5.4.2.2 Law Enforcement Access to Citizen Information

State access to citizen data is always fraught with risks of overreach and surveillance. It is evident from the previous chapters, that in the South Asian context, judicial oversight is essential to prevent abuse.[127] Some form of legislative, judicial or independent oversight for interception exists across most democratic countries.[128]

124 Amnesty International, *A Human Rights Approach to Tackle Disinformation:Submission to the Office of the High Commissioner for Human Rights* (*Amnesty International* 2022);International Center for Not-for-profit Law, *Legal Responses to Disinformation* (ICNL 2021);

Kakkar and Desai,'Voting out Election Misinformation in India:How should we regulate Big Tech?' in Kritika Bhardwaj, Sangh Rakshita and Shrutanjaya Bhardwaj (eds), The Future of Democracy in the Shadow of Big and Emerging Tech (National Law University Delhi Press 2021).

125 Kakkar and Desai,'Voting out Election Misinformation in India:How should we regulate Big Tech?' in Kritika Bhardwaj, Sangh Rakshita and Shrutanjaya Bhardwaj (eds), The Future of Democracy in the Shadow of Big and Emerging Tech (National Law University Delhi Press 2021).

126 Evelyn Douek, 'Content Moderation as Systems Thinking' (2022) Harvard Law Review Vol 136

127 Vrinda Bhandari and Karan Lahiri, 'The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World' [2020] U Oxford Hum Rts Hub J 15.

128 Committee of Experts under Chairmanship of Justice B.N Srikrishna Submitted to Ministry of Electronics and Information Technology, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians (2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> , p125.

Consequently, across the three jurisdictions, an effective safeguard could be mandating ex-ante judicial authorisation for each interception order or user data request by law enforcement and intelligence agencies. This will ensure that the rights of the citizens are balanced against the state's interests by an independent judicial body, which tests the proportionality of the state orders on a case–by–case basis.[129]

Alternatively, there could be an option of *ex post* judicial review after the cessation of the surveillance for the aggrieved citizens. This requires that citizens whose data has been accessed by LEAs or who have been put under interception be informed about the same, and provided with a fair chance to challenge it in the court of law.

To strengthen the rule of law, evidence obtained through unconstitutional or illegal surveillance must not be deemed admissible in court.[130] Further, the threshold of offence to allow for an interception order must be set reasonably. Currently, in India, Sri Lanka and Bangladesh, the overbroad ground of "investigation of any offence" can be grounds for an interception order.

It is also important that intelligence agencies authorised to conduct surveillance be accountable to the legislature through parliamentary committees. Intelligence agencies, LEAs, executive actors, and ISPs must mandatorily provide periodic public reports on interception statistics.[131]

5.4.2.3 Internet Shutdowns

It is hard to justify the use of internet shutdowns in democracies, given the blanket unencumbered power it provides to the state.[132] Internet shutdowns have widespread and long-term economic, social and political implications that cannot be properly accounted for at the time of decision-making and consequently, it is thus challenging to justify the

129 As per the Puttaswamy judgement the measures limiting the right to privacy must be (a) be provided by law; (b) pursue a legitimate aim and be necessary in a democratic society; (c) be proportionate to the need for the interference with the right to privacy; and (d) contain procedural safeguards to prevent against abuse.

130 Bhandari and Lahiri (n 127).

131 Albert Gidari, 'Wiretap Reports Not So Transparent' (*The Centre for Internet and Society*, 26 January 2017) <https://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent> .

132 Human Rights Council, 'Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights Report of the Office of the United Nations High Commissioner for Human Right'(2022) A/HRC/50/55 <https://www.ohchr.org/en/documents/thematic-reports/ahrc5055-internet-shutdowns-trends-causes-legal-implications-and-impacts >.

necessity and proportionality of such measures, given their far-reaching and indiscriminate impact on human rights.[133]

Nonetheless, if such shutdowns are being deployed by states, they must only be operationalised under the most exceptional circumstances, where the states can provide evidence that no other less restrictive option can suffice. This must ideally be subject to ex-ante, or at least ex-post, scrutiny by an independent judiciary or any other adjudicatory authority.[134] All such orders by the state must be publically available, and citizens must be free to challenge such orders in a court of law.[135]

5.4.2.4 Limiting Arbitrary Blocking of Online Content

Any restriction on online content must be provided by law, and be necessary and proportional to fulfil a legitimate purpose. These restrictions must meet the thresholds laid down in international human rights law, and protect the freedom of expression, access to information, privacy and other fundamental rights of users.[136]

Blocking access to content or taking down content is employed across the three countries to restrict online content. This involves significant determination of the speech rights of individuals, and as seen in the previous chapters, the concentration of such powers with the executive without adequate checks and balances can lead to state censorship.

Thus, with respect to government requests for content takedown, the executive must obtain court orders before issuing a blocking direction to the intermediaries. There can be certain exceptions provided for cases where blocking of access is time-sensitive for a narrowly-defined category of content (e.g. extremist and violent content). Here, the executive may issue a blocking direction without a court order, on the condition that such an order is limited in duration, and will be subject to judicial scrutiny for its continuation.

133 Ibid.

134 Ibid.

135 *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

136 UNESCO, 'Guidelines for Regulating Digital Platforms: A Multistakeholder Approach to Safeguarding Freedom of Expression and Access to Information' (2022) CI-FEJ/FOEO/3 Rev. <https://unesdoc.unesco.org/ark:/48223/pf0000384031.locale=en> pt27.

Users whose content is subject to such blocking orders must have access to judicial remedies and other independent grievance redressal mechanisms. Thus, users must be notified and provided with the blocking order, the action taken, and information on relevant redressal options available to them. The state's blocking order must include information on the issuing authority, the legal basis for the order, and reasons why a specific piece of content is illegal.[137] Apart from ex-post grievance redressal options, users must also be granted an opportunity to be heard before such an order is passed by the executive .[138] Respective countries must be transparent about the aggregate numbers, categories, legal basis and purpose of blocking orders issued to intermediaries.[139]

5.4.3 Other Recommendations

Multistakeholder Approach to Policy-Making

As a starting point, legislation should be drafted following due processes of democratic deliberation and transparent public consultation processes. It should involve open and transparent consultations with diverse stakeholders and ensure meaningful representation of all interests. Engaging with end-users, judges, lawyers, technical experts, independent researchers, civil society organisations, and academic institutions can serve as an integral part of making the regulatory framework inclusive and effective. The public consultation processes should be regular, provide adequate time for response, and be user-friendly and transparent in dispensing its functions.

Lawmakers should also be mindful that excessive delegation of rule-making to administrative bodies or executive bodies can undermine democratic debate built into parliamentary legislative procedures.[140] Similarly, shadow regulations entered into by

137 Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1, art 9(2)(a).

138 In the Indian context, the Supreme Court in the Shreya Singhal vs U.O.I read such pre-decisional hearings to the intermediary as well as concerned user into the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009 as a necessary procedural safeguard while upholding blocking under section 69A. However, this practice has not been followed by the executive and has recently been challenged in the Delhi High Court in the *Tanul Thakur v Union of India* case.

139 UNESCO, 'Guidelines for Regulating Digital Platforms: A Multistakeholder Approach to Safeguarding Freedom of Expression and Access to Information' (Internet for Trust, Paris, February 2022) <https://unesdoc.unesco.org/ark:/48223/pf0000384031.locale=en> pt27(d).

140 'Content Regulation and Human Rights Analysis and Recommendations' (*Global Network Initiative*, 2020) <https://globalnetworkinitiative.org/wp-content/uploads/2020/10/GNI-Content-Regulation-HR-Policy-Brief.pdf>.

corporations are also fraught with opaqueness and can delegate significant free speech decisions to platforms.[141]

Capacity Building for all Stakeholders

Regulatory frameworks that aim to counter the impact of online harms must be carefully curated and based on empirical evidence. The government should also support independent research to improve the quality of policymaking. This can also aid the government's ability to address the complex challenges unique to the South Asian or local online ecosystem.[142]

Governments must invest in efforts to upscale the quality of education about the internet, emerging technologies, and online harms for all users. Digital education can empower citizens to hold both platforms and states more accountable.[143]

Safe Harbour Protection

With respect to social media regulation, a well-defined and predictable intermediary liability framework is essential to protect the rights of citizens.[144] Its absence leaves platforms vulnerable to state coercion, especially when penal provisions for third-party content are directed at employees of social media platforms/ intermediaries.[145] Further, such regulation should not impose a 'one size fits all' approach; rather, they must codify specific governance frameworks for different classes of intermediaries.[146] It is also important to note at this point that legislation that imposes short takedown timeframes to judge the unlawfulness of content incentivises over-censorship by platforms that seek to avoid liability at all costs.[147]

141 Association for Progressive Communications, *Content Regulation in the Digital Age Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression* (2018) <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/ContentRegulation/APC.pdf>.

142 For instance, research can help understand the limitations of social media platforms in dealing with harmful content online proliferating in regional languages.

143 See Don Passey and others, 'Digital Agency: Empowering Equity in and through Education' (2018) 23 Technology, Knowledge and Learning 425 <https://doi.org/10.1007/s10758-018-9384-x>; Anita Gurumurthy, Nandini Chami and Deepti Bharthur, 'Democratic Accountability in the Digital Age' [2016] Available at SSRN 3875297.

144 Joris van Hoboken and Daphne Keller, 'Design Principles for Intermediary Liability Laws' [2020] Algorithms.

145 UNESCO, 'Guidelines for Regulating Digital Platforms: A Multistakeholder Approach to Safeguarding Freedom of Expression and Access to Information' (Internet for Trust, Paris, February 2022) <https://unesdoc.unesco.org/ark:/48223/pf0000384031.locale=en> pt27(g).

146 UNESCO, 'Guidelines for Regulating Digital Platforms: A Multistakeholder Approach to Safeguarding Freedom of Expression and Access to Information' (Internet for Trust, Paris, February 2022) <https://unesdoc.unesco.org/ark:/48223/pf0000384031.locale=en> pts 66,67.

147 Rishabh Dara, 'Intermediary Liability in India: Chilling Effects on Free Expression on the Internet' (2011) SSRN <http://dx.doi.org/10.2139/ssrn.2038214>.

Platform Accountability

Finally, punitive legislation focusing on unlawful content should be complemented with preventive public policy that increases accountability and incentivises systemic changes in how platforms operate.[148] In recent times, transparency has become a predominant mechanism to facilitate platform accountability.[149] Along with transparency on the platform's internal processes, including content moderation decisions, recommender systems, advertising models etc., there should be greater accountability on state-platform interactions.[150]

5.5 Conclusion

Regulating the online information ecosystem is an important component of social media governance across all three jurisdictions. While internet shutdowns, criminalisation of online speech and law enforcement access to citizen information are being employed across the three countries, Bangladesh and India have additionally developed mechanisms to block access to targeted content on social media through blocking orders to social media intermediaries. These mechanisms are absent in Sri Lanka at the time of writing.[151]

The mechanisms to control the flow of online information manifest as regulations directed to (a) users and (b) social media platforms and other internet intermediaries. These consist of (a) ICT regulation, including cybersecurity, data protection, and telecommunication regulation; (b) intermediary liability frameworks; (c) key speech laws (mostly penal) are used to regulate the flow of information in the three jurisdictions.

All three countries regulate users through existing penal provisions and online content-based offences.[152] However, when it comes to regulating social media platforms, while India and Bangladesh provide conditional exemption from liability for third-party content

148 Government of France, *Creating a French framework to make social media platforms more accountable: Acting in France with a European vision* (Mission report Second Edition Version 1.1, 2019) <https://www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf>.

149 Robert Gorwa and Timothy Garton Ash, 'Democratic Transparency in the Platform Society'.

150 Caitlin Vogus and Emma Llansó, 'Making Transparency Meaningful: A Framework for Policymakers' (Center for Democracy & Technology 2021).

151 However, as noted earlier this could change with the passage of the Online Safety Bill 2023 in Sri Lanka.

152 See 5.2.3 for more details.

hosted by intermediaries, Sri Lanka lacks such an exemption framework. It relies on licensing agreements with ISPs to block social media platforms in emergency cases. However, this can change with the proposed Online Safety Bill 2023.

It is also worth noting that in both India and Bangladesh, the safe harbour protections afforded to intermediaries is witnessing a trend of dilution over time. Although India imposes more extensive due diligence obligations at the moment, Sri Lanka and Bangladesh are also likely to follow a similar trend as being witnessed in the draft OTT Policy and the Online Safety Bill.

Overall, an important trend witnessed in the regulation across the three jurisdictions is the centralisation of power with the executive. The regulatory frameworks lack the necessary judicial and parliamentary oversight mechanisms while issuing content takedown orders, internet suspensions, and user data requests. Overbroad and vague language is used to codify speech-related offences and grounds for security exceptions. These factors contribute to a lack of transparency and accountability for government actions.

We note that social media platforms play a critical role across several national security and geopolitical fronts.[153] However, indiscriminate use of security exceptions can lead to overstepping critical human rights, including free speech and privacy. This subordination of individual rights to security can manifest in states exerting control on the flow of information through coercive regulation or informal cooperation with platforms while neglecting meaningful platform accountability.

As seen throughout the report, security exceptions can be misused by states to curb the legitimate expression of dissent through censorship and surveillance. Thus, it becomes imperative to institute procedural and substantive safeguards when balancing security imperative against the fundamental rights of citizens.

The scale, speed and reach of social media content is unprecedented and has placed current regulatory regimes at a crossroads. It is a good opportunity for South Asian states to gear their focus towards how upcoming regulations could enhance platform accountability and facilitate systemic changes in platform design and operation. An effective and democratic platform governance model should place the rights of citizens at the centre.

153 Elena Chachko, 'National Security by Platform' (2021) 25 Stanford Technology Law Review.