

opt
ima

Internet Shutdowns In Bangladesh: *Legal Dimensions and Recourses*

Shahzeb Mahmood

December 2023

Table of Contents

EXECUTIVE SUMMARY	1
1. INTRODUCTION	3
2. SCOPE OF THE REPORT	4
3. CANVASSING GLOBAL INTERNET SHUTDOWNS	4
4. A CLOSER LOOK AT INTERNET SHUTDOWNS IN BANGLADESH	6
5. INTERNATIONAL COMPARATIVE ANALYSES	10
6. LEGAL RESPONSE TO INTERNET SHUTDOWNS IN BANGLADESH	18
7. RECOMMENDATIONS	32
8. CONCLUSION	34
ENDNOTES	35

EXECUTIVE SUMMARY

This report aims to shed light on the issue of internet shutdowns in Bangladesh. It examines the legality of shutdown orders and recommends that the Government of Bangladesh undertake legislative reforms and ensure alignment with applicable human rights standards. Additionally, it outlines the responsibilities of corporations implementing these shutdown measures, along with the legal avenues available to citizens and corporations to challenge unlawful orders.

Parts 1 and 2 of the report focus on government-sanctioned shutdowns and their impact on freedom of expression and access to information in Bangladesh. It does not delve into other forms of interference, such as censorship or attacks by bad actors. It defines “internet shutdown” and outlines circumstances, modalities and methods of implementation of such measures — ranging from complete or partial disconnection of internet connectivity to bandwidth throttling and downgrading mobile internet from 4G to 2G.

In Part 3, the report provides an overview of internet shutdowns implemented in consolidated democracies, hybrid regimes and authoritarian states worldwide, outlining regional and national shutdowns in over 20 countries over the last two decades.

Part 4 examines specific instances of shutdown measures by the national authorities in Bangladesh, the underlying political landscape, and pattern of behaviour of the state agencies. It also considers the role of telecommunication service providers in facilitating these shutdown measures.

Specifically, it highlights the frequent occurrence of internet shutdowns in Bangladesh since 2009, with the country ranking fifth globally for the number of shutdowns in 2022.

Generally, the restrictions range from blocking access to social media and instant messaging services to wholesale internet disruptions and limiting mobile internet bandwidth. Often, the government has denied ordering these restrictions, and sometimes even failed to acknowledge that a disruption has occurred. In cases where shutdown orders are acknowledged, reasons are seldom provided. Furthermore, the report also demonstrates that local telecommunication service providers are key actors in implementing shutdown measures, with their compliance driven by a combination of legal and practical reasons.

Part 5 provides an overview of the international response to state-sanctioned internet shutdowns, analyses of international frameworks and review of lawsuits initiated in four jurisdictions. In the first section, the report highlights opposition to internet shutdown by various international organisations, including the United Nations, the Human Rights Council, the Human Rights Committee, the Council of Europe, the African Commission on Human and Peoples’ Rights and the Freedom Online Coalition, as well as ambassadors, diplomats, special rapporteurs and statesmen worldwide. These stakeholders underscore the importance of the internet as a medium through which individuals can exercise their right to freedom of expression.

The second section elaborates on Article 19 of the International Covenant on Civil and Political Rights, arguing that while general restrictions on the internet and online services are not compatible with the three-part test, a more narrowly targeted restriction (for instance on specific websites or online platforms) could, in certain narrowly defined, highly exceptional cases, be proportionate and justifiable response, provided the measures meets one of the qualified grounds of restrictions.

The final section examines lawsuits against internet shutdown in India, Turkey, Togo and

Russia. Particularly, the decision of the Supreme Court of India in *Anuradha Bhasin v. Union of India* is examined in this section and in other parts of the report.

Part 6 outlines possible legal responses to internet shutdowns in Bangladesh, specifically focusing on utilising the Right to Information Act, 2009 for disclosure of shutdown orders and the filing of public interest litigation under Article 102 of the Constitution of Bangladesh to challenge legality of such orders. Here, the report highlights the duty, and the authority, of the High Court Division of the Supreme Court of Bangladesh in responding to violation of constitutional rights. It argues that an internet shutdown measure can be challenged for contravening Articles 39(2) and/or 27 and 31 of the Constitution of Bangladesh. Additionally, it affirms that the jurisprudential parameters exist for the constitutional courts to consider, albeit in exceptional cases, international laws and cases in domestic proceedings.

Part 7 outlines a list of recommendations to address internet shutdown, including actions that can be taken by the government, corporations, and citizens and civil society organisations.

Part 8 concludes the report, arguing that a human-centric and rights-respecting approach is key to effectively interrogating this space and counteracting the phenomenon, as it not only promotes transparency and accountability but also ensures that focus remains on those most acutely affected — the citizens.

1. INTRODUCTION

Over the course of nearly three decades, the widespread adoption of the world wide web and the rapid advancement of digital technologies has transformed the way society communicates, transacts and stays connected.¹ Yet, internet freedom has increasingly been imperilled by autocratic tools and tactics.² Digital authoritarianism, encompassing wide-ranging policies and practices deployed by governments to exert pressure and exercise pervasive control over people's lives, has manifested in the form of internet shutdown in recent years.³

For the purposes of this report, the term "internet shutdown" means intentional measures taken by or on behalf of a government, often with the assistance of non-state actors operating telecommunication systems and infrastructures, in order to disrupt access to, or the effective use of, the internet or online information and communications tools by a large number of people.⁴

Internet is a kludge — an effective but tangled network grown through spontaneous expansion and shaped by makeshift fixes ossified into structural features⁵ — and, therefore, technically cannot be shut down.⁶ However, it can be restricted within certain geographical locations using a variety of technical mechanisms. Such restrictions may, for instance, affect local areas, an administrative region, several regions or an entire country, with the duration ranging from a few hours to months, or even years.⁷

Generally, internet shutdowns are implemented in two ways: either at the national level, where internet traffic entering or exiting a country faces restrictions through a national gateway or firewall, or through administrative directives or extra-legal pressures on telecommunication and internet service providers.⁸

Outcomes are not homogeneous and exist on a spectrum,⁹ ranging from the hammer of a complete blackout to more targeted screwdriver-style arrangements involving bandwidth throttling and internet access restrictions.¹⁰ Disconnecting broadband and mobile internet connectivity completely is the "nuclear" option and an extreme manifestation of shutdowns.¹¹ However, increasingly, only access to mobile internet is restricted, which can result in complete blackout for a majority of the population in areas where broadband internet is not accessible and mobile devices are the primary means of internet access.¹² It is the totality, the bluntness, the widespread impact and the intentionality of these measures that distinguishes them from more targeted forms of restriction.¹³

On the other end of the scale are bandwidth throttling and downgrading mobile internet services from 4G to 2G, which, while allowing nominal access, hinders the ability to upload, access or share anything beyond simple text-based content, severely limiting the usefulness of the internet as a communication tool.¹⁴ Furthermore, blacklisting — and less commonly, whitelisting — are other tactics of internet shutdown. While the former involves selectively obstructing the availability or accessibility of two-way, or multi-way, real-time communications

platforms, such as internet-based messaging applications and social media services,¹⁵ the latter creates a walled cyberspace where only government-approved platforms are accessible.¹⁶

Ultimately, the objective of each of these measures is to render online channels of communication inaccessible or effectively unusable, in order to exert control over the flow of information on the internet.¹⁷

2. SCOPE OF THE REPORT

If an act of interference does not fit into the broad categories outlined in Part 1 above, it will likely fall into the category of censorship rather than an internet shutdown, and therefore is beyond the scope of this report. For example, restrictions on platforms like WhatsApp, Facebook, Twitter and YouTube would constitute internet shutdowns, as these platforms enable user-to-user communications. However, the blocking or censoring of websites such as Wikipedia or The Washington Post would be considered censorship, as these platforms primarily focus on publishing content.¹⁸

Further, this report does not examine restrictions on adult content websites that facilitates user-to-user communications. It also excludes internet shutdowns during conflict situations between belligerent states, such as in the Gaza Strip since October 2023¹⁹ and in Ukraine throughout 2022.²⁰

Shutdowns can also occur due to various factors, including severe weather conditions, natural disasters, accidental cable severance or prolonged electricity blackout.²¹ Anachronistic methods of internet shutdown include cutting off power grids, powering off cell towers, dismantling internet service infrastructures, initiating distributed denial-of-service attacks or manipulation of network routers and domain name systems. However, this report

concentrates on government-sanctioned internet shutdowns, and, therefore, to the extent these methods are not initiated or sanctioned by the government, they fall outside the scope of this report.

Finally, this report narrowly focuses on the impact of internet shutdowns on the right to freedom of expression and access to information, and the examination of public interest litigations and information access mechanisms as response to internet shutdowns in Bangladesh. Other implications of shutdowns and alternative responses are not explored in this report.

3. CANVASSING GLOBAL INTERNET SHUTDOWNS

Globally, internet freedom has declined for thirteen consecutive years, with evidence indicating an acceleration in this decline.²² Internet shutdowns are a favoured tactic of many governments worldwide to suppress protests, consolidate powers, censor information and isolate conflict areas from the rest of the world. As observed by UN Special Rapporteur Clément Voule, “[s] hutdowns are lasting longer, becoming harder to detect and targeting particular social media and messaging applications and specific localities and communities.”²³

Research indicates that authoritarian regimes are more likely to impose overt restrictions on internet access compared to states with democratic or hybrid regimes.²⁴ Some of the first instances of shutdowns occurred in Nepal in 2005,²⁵ and in Myanmar and Guinea in 2007,²⁶ when the countries were under non-democratic regimes. Despite being miles apart, each regime used similar strategies to restrict

internet access, disrupt communication and control information flow.

Although internet shutdowns are a hallmark of authoritarian regimes, the world's largest democracy, India, has emerged as one of the most active and aggressive implementers of the measure.²⁷ In 2022 alone, India accounted for 84 blackouts, constituting nearly 45% of the 187 shutdowns documented by the #KeepItOn coalition. Since 2016, the country has been responsible for approximately 58% of all shutdowns recorded by Access Now.²⁸ One of the longest internet blackout periods in the country occurred in Jammu and Kashmir, lasting over 550 days from 5 August 2019 to 5 February 2021.²⁹

However, one of the longest shutdowns in Asia occurred in Myanmar. Starting in June 2019, the government disconnected internet services in several towns in Rakhine and Chin states for over 560 days.³⁰ Following the military coup in February 2021, social media and circumvention tools have been blocked, and connections remain unreliable across the country.³¹

Internet shutdowns are common elsewhere in Asia. Pakistan implemented restrictions on mobile internet and social media in a bid to quell protests following the arrest of its former prime minister in May 2023,³² while the residents of the country's federally administered tribal areas have endured intermittent internet restriction since 2016.³³ Iran used a similar strategy during anti-government protests, implementing internet access limitations in 2022 to suppress protests against the death of 22-year-old Mahsa Amini.³⁴ In January 2022, the Kazakhstan government disrupted

internet access nationwide in response to widespread civil unrest.³⁵ During the terrorist attack in Sri Lanka in April 2019, immediate measures were taken to block access to social media and communication services, including Facebook, Instagram, Snapchat, WhatsApp and YouTube.³⁶ Iraq has repeatedly imposed restriction on internet throughout 2023 to curb cheating during high school exams period.³⁷

Guinea mandated amongst the first shutdowns in Sub-Saharan Africa in 2007, at a time where less than 1% of the population had internet access.³⁸ However, the precursor to today's shutdowns can be traced back to the Arab Spring. In January 2011, President Hosni Mubarak took Egypt offline, followed by Colonel Muammar Gaddafi in Libya in March 2011.³⁹ Since then, internet shutdowns have become routine across the continent, especially when the authority of the ruler is threatened.⁴⁰

In 2021, for instance, governments in Uganda and Zambia disabled access to the internet before and after national elections,⁴¹ while the government of Eswatini suspended access to the internet twice in response to mass anti-government protests.⁴² Starting in November 2021, Burkina Faso also intermittently disconnected access to mobile internet.⁴³ Senegal twice imposed shutdown measures in 2023 amid opposition protests and to prevent the spread of subversive messages online.⁴⁴ Ethiopia experienced a two-week internet shutdown in 2020 following mass protests.⁴⁵ In one of the longest running internet shutdowns to date in the region, Ethiopia's northern Tigray region has been facing internet disruptions since November

2020,⁴⁶ and in February and August 2023, the government also blocked access to social media platforms in other areas amid rising tension with leadership of the orthodox church and to quell violence between regional security forces and national army.⁴⁷ In 2020, to avoid conflicts related to the outcome of the presidential elections, a wholesale ban on internet was imposed in the Democratic Republic of Congo,⁴⁸ and in Mali, social media and messaging platforms were restricted.⁴⁹ Meanwhile Zimbabwe witnessed several incidents of internet shutdowns between 2016 and 2019 during anti-government protests, which only ceased after a court ruling deemed the shutdowns measures excessive.⁵⁰ Similarly, Sudan ended a five-week long internet shutdown in 2019 after a court ordered its immediate restoration.⁵¹ In Chad, access to communication platforms, such as Twitter, Facebook and WhatsApp, was restricted for over 470 days since March 2018.⁵² A 230-day internet shutdown covering the northwest and southwest regions of Cameroon took place between January 2017 and March 2018.

Internet shutdowns also occur in consolidated democracies. For example, the law enforcement agency in England shut down internet access in the London Underground in 2019 to manage protests by climate protesters.⁵³ Although more localised and limited compared to nationwide disruptions, this incident is

noteworthy because the British government utilised this measures whilst advocating for a “no internet shutdown norm”.⁵⁴ Similar measures were implemented earlier in San Francisco in 2011, when mobile-internet and phone services were shut down to control a protest in the subway.⁵⁵

4. A CLOSER LOOK AT INTERNET SHUTDOWNS IN BANGLADESH

A. INTERNET SHUTDOWNS SINCE 2009

Over the last decade, the Government of People’s Republic of Bangladesh (the “Government of Bangladesh”) has increasingly resorted to the use of internet shutdowns as means of controlling communication channels, either unaware of its severe implications, or calculating that the perceived benefits outweigh the harms.⁵⁶ Shutdowns have become increasingly prevalent in Bangladesh in recent years, with the country ranking fifth globally for the number of shutdowns in 2022.⁵⁷ Assessing the level of internet freedom in 70 countries around the world, the Freedom House scored Bangladesh 41 out of 100 for internet freedom and categorised the country as “partly free” in 2023.⁵⁸ Over the last one decade, the country remained “partly free” and, while initially the scores improved, peaking in

<i>Freedom on the Net by Freedom House³³⁷</i>								
2014	2015	2016	2017	2018	2019	2020	2021	2022
49/100	51/100	56/100	54/100	51/100	44/100	42/100	40/100	43/100

2016, it has been in decline since the 2018 elections.

One of the first recorded cases of an internet shutdown in Bangladesh occurred following a paramilitary mutiny in March 2009, when access to YouTube was blocked for a week for hosting content “subversive to the state.”⁵⁹ Since then, the Government of Bangladesh has often resorted to restricting access to social media and instant messaging services.

In January 2015, access to five popular instant messaging services was disabled by the government over national security concerns. Lasting for four days, the restriction was reportedly enforced to address the risk of terrorists using the services to communicate.⁶⁰ Subsequently in November 2015, access to Facebook,⁶¹ Messenger, WhatsApp and Viber were blocked on national security grounds shortly after convicted war criminals lost their final appeal against the death penalty.⁶² After three weeks of restrictions, the services were unblocked.⁶³

Connection to the internet has also been restricted on similar grounds. During a terrorist attack at the Holey Artisan Bakery in July 2016, a geographically targeted restriction on broadband internet connection was enforced in order to prevent the terrorists from communicating outside the café premises.⁶⁴ Close to a million residents of the Rohingya refugee camps in Cox’s Bazar endured a 355-day internet blackout imposed on “security” grounds,⁶⁵ beginning in early September 2019 and continuing for several months even after the first cases of COVID-19 were detected in the camps.⁶⁶ Furthermore, in

August 2018, the mobile internet speed was throttled across the country to prevent image- and video-based content from being uploaded, reportedly in a bid to suppress coverage of student protests as social media became an outlet for an outpouring of public discontent and criticism against the government.⁶⁷

In some instances, the Government of Bangladesh has implemented internet blackouts that extend beyond the scope of public order or national security grounds. Frequently, disruptions are justified by fear of protest during socially and politically sensitive moments.⁶⁸ An example of such overreach occurred ahead of the national election in December 2018, when the country’s telecom regulator, the Bangladesh Telecommunication Regulatory Commission (the “BTRC”), issued directives for the nationwide shutdown of high-speed mobile internet services, purportedly to diffuse risks of rumours and propaganda spreading over social media platforms.⁶⁹

In February 2019, as a part of the anti-pornography drive, somewhereinblog.net, the largest Bengali-language community blogging platform in the world, and TikTok and Bigo were blocked in the country.⁷⁰ A government minister attributed the restriction on the blogging website to anti-government, scandalous and atheistic content,⁷¹ while the telecoms regulator referred to anti-national activities.⁷² After an eight-month-long ban, the social media services and the blogging platform were eventually unblocked for reasons yet undisclosed.⁷³

Often, the Government of Bangladesh denies imposing restrictions, and at times

even the existence of these disruptions.⁷⁴ In 2022, reports surfaced that mobile services were throttled in areas where pro-opposition rallies were organised.⁷⁵ However, the BTRC reportedly denied involvement and instead attributed the disruptions to system overloading caused by mass gatherings, while the responsible minister claimed to have no information about the matter.⁷⁶ Earlier in October 2021, high-speed internet services were disrupted for twelve hours across the country following communal violence instigated by inciteful posts on social media,⁷⁷ and in March 2021, access to Facebook and Messenger was restricted for three days during protests against the visiting Indian Prime Minister Narendra Modi.⁷⁸ However, in these instances, the authorities either refused to comment on the matter or denied issuing directions, instead citing technical issues as the cause of the disruption.⁷⁹ An earlier incident in November 2018 involved restrictions on Skype when the authorities found that an opposition leader was using the videoconferencing platform to interview prospective candidates for the national election from London.⁸⁰ Authorities denied ordering the restriction in this instance as well.⁸¹

B. UNDERSTANDING THE POLITICAL LANDSCAPE

Mustafa Jabbar, the technocrat minister of post and telecommunications, has reportedly expressed opposition to internet shutdowns in the past. According to reports by *The Daily Star*, he has likened the wholesale blocking of the internet in 2010 to forcing people to “live like ostriches with their heads buried in the sand.”⁸² It is

also reported that he called the measures taken in 2015 to block social networking sites and communication applications a “complete failure of the government mechanism.”⁸³ In 2017, he also purportedly said that he is in principle against the blocking or banning of websites for any period of time and irrespective of the reasons, in response to the news that the cabinet division had recommended disabling access to Facebook from midnight for six hours every day.⁸⁴ At the time, he argued that such measures are ineffective because users could easily move to other platforms, and emphasised that restriction on internet access contradicts the principles of a democratic country and commitments to the *Universal Declaration of Human Rights*. His stance appeared to have changed after his appointment as a government minister in 2018. According to reports, he publicly stated that the internet could be shut down and social media sites could be blocked in the interest of the state and its citizens.⁸⁵ It is unclear if the statement by the minister reflects the official position of the Government of Bangladesh, and if so, how it aligns with the *Digital Bangladesh* and *Vision 2041* aspirations.

It is also important to recognise the role of the telecom regulator in internet shutdowns. Officially, the BTRC is an independent regulatory body responsible for overseeing telecommunication services and systems, and serves as the nodal authority for all shutdown requests from the government. In 2021, an amendment to parent legislation was under consideration, which would have authorised the telecommunications ministry to assume direct oversight and control over most of the regulator’s functions.⁸⁶

World Press Freedom Index by Reporters Without Border³³⁸

2014	2015	2016	2017	2018	2019	2020	2021	2022
146/180	146/180	144/180	146/180	146/180	150/180	151/180	152/180	160/180

Although the proposed amendment has not been enacted, the BTRC in reality appears to lack independence.⁸⁷

Network shutdowns have been described as “the most brute force method of internet control.”⁸⁸ Such restrictive measures are emblematic of the illiberal mindset, and are significant precursors to human rights violations.⁸⁹ Over the years, this attitude has also manifested in how government has censored local and foreign news outlets in Bangladesh.

Access to several international online news outlets have also been blocked in Bangladesh in recent years. Between 2017 and 2021, Scroll was blocked in 2021,⁹⁰ *Benar News* in April 2020,⁹¹ *Netra News*⁹² and *Al Jazeera* in 2019,⁹³ and *The Wire* and the *Swedish Radio* in 2017,⁹⁴ for publishing content implicating government officials in corruption, disappearances and military involvement.

Similarly, between 2016 and 2023, Bangladesh witnessed extensive online censorship, with 191 websites blocked in January 2023 for alleged anti-state propaganda,⁹⁵ an immediate blockage of a new online news site in August 2021,⁹⁶ and the abrupt cutoff of two local news outlets in April and May 2019.⁹⁷ Additionally, in December 2018, over 50 online news portals were blocked ahead of national

elections for spreading perceived anti-government propaganda,⁹⁸ and in June of the same year, telecommunications providers were directed to block a link to a report by *The Daily Star*, leading to an 18-hour restriction of access to the entire website.⁹⁹ Around August 2016, approximately 30 news websites faced inaccessibility measures in the country.¹⁰⁰

In the 2023 *World Press Freedom Index*, Bangladesh ranked 163rd out of 180 countries.¹⁰¹ Over the last one decade, while initially the ranking remained static, it declined progressively after the 2018 elections.

C. TELECOM OPERATORS’ ROLE IN NETWORK DISRUPTIONS

Although government functionaries order shutdowns, telecommunication service providers are the ones who implement them. According to official statistics by the BTRC, there are over 130 million internet subscribers in Bangladesh as of October 2023, with approximately 90% of them using mobile internet, and the remaining use broadband.¹⁰² Disabling or throttling mobile internet nationwide will, therefore, effectively result in a near total blackout of internet access throughout the country. Companies implementing the restrictions are often the first, and sometimes the only,

ones with full visibility on the nature of a shutdown and its scope.¹⁰³ Moreover, in situations where the government denies responsibility for restricting access to the internet or specific websites, the operators are exposed to potential charges of creating unlawful obstructions.¹⁰⁴ Given this context, one may justifiably ask why the three private mobile network operators, controlled by multinational corporations like Axiata, Telenor and VEON, and collectively holding over the total 96% of the country's nearly 187.5 million mobile connections, comply with the shutdown orders in the first place.

Simply put, the compliance is largely due to the business continuity risks that non-compliance entails. Failure to comply with the terms and conditions of the licence can result in loss of this licence, or even imprisonment for a maximum term of five years as well as criminal fine of up to BDT 3,000,000,000 (approx. US\$ 26 million).¹⁰⁵ Contravention could also result in a criminal liability on part of its shareholders, directors, employees and other representatives, unless they can demonstrate that the non-compliance occurred without their knowledge or all measures were taken to avoid it.¹⁰⁶ Defending the right to access the internet, on the other hand, will cost the companies in terms of compliance time and legal fees, offering little incentive for them to go the extra mile. All in all, the overall framework incentivises the operators to err on the side of caution and disable internet connections, thereby fostering a culture of overcompliance that ultimately chills free speech.

5. INTERNATIONAL COMPARATIVE ANALYSES

A. GLOBAL APPEALS TO END STATE-SANCTIONED INTERNET SHUTDOWNS

Access to the internet is recognised as an indispensable enabler of a wide range of human rights.¹⁰⁷ In 2011, UN Special Rapporteur Frank La Rue recognised that few developments in the realm of information technologies have had such a profound and transformative impact as the creation of the internet.¹⁰⁸ It serves as a vital medium through which individuals exercise their right to freedom of expression. Echoing similar views, special rapporteurs on freedom of expression from the United Nations, the Organization for Security and Co-operation in Europe, the Organization of American States, and the African Commission on Human and Peoples' Rights (the "Four Special Rapporteurs on Freedom of Expression") affirmed that the global reach, effectiveness, relative power and accessibility of the internet makes it pivotal in the realisation of the universality of freedom of expression.¹⁰⁹

Article 19 of the International Covenant on Civil and Political Rights ("Article 19, ICCPR") (the "ICCPR") protects both the freedom of individuals to form opinions and their right to express those opinions freely. While these freedoms are independent, they coexist as adjuvants: freedom of expression relies on the anterior and inviolable right to hold an opinion, which, in turn, is shaped by others exercising their right to impart information and ideas.¹¹⁰ Advancements in recent years in digitalisation and digitisation, and improvements in

access, mean internet shutdowns most immediately and directly impinge on the fundamental right to freedom of expression — a cornerstone of free and democratic societies and an indispensable condition for the self-development of a person.¹¹¹ Professor Michael O’Flaherty, now director of the European Union Fundamental Rights Agency, referred to freedom of expression as a *meta* right because of its role in enabling enjoyment of so many other rights.¹¹²

Nevertheless, the unparalleled speed and relative anonymity offered by the internet, along with its cost-effectiveness and instantaneous cross-border communication capabilities, have engendered concerns among national authorities about its potential misuse, resulting in a surge in internet restrictions worldwide. Often, these restrictions lack a strong legal foundation or rely on ambiguous laws, with the implementation of shutdown orders lacking transparency and offering vague rationales that largely fail to meet necessity and proportionality requirements.¹¹³

Appeals have been made by human rights bodies to cease state-sanctioned shutdowns.¹¹⁴ For instance, the Human Rights Council (the “HRC”) has consistently reaffirmed the principle that the rights individuals enjoy and exercise offline must also be protected online.¹¹⁵ In 2009, the HRC called upon national governments to refrain from using Article 19, ICCPR to impede access to the internet, curtail the free flow of information and ideas, and stifle expressions on government policies, political debates, corruption, elections and human rights.¹¹⁶ In 2016, it also condemned “measures to intentionally prevent or disrupt

access to or dissemination of information online in violation of international human rights law,” and urged state authorities to refrain from employing such restrictive measures.¹¹⁷ Critical of the practice, and recognising the profound adverse impacts of internet shutdowns on human rights, the HRC implored states in 2018, and again in 2021, to ensure that domestic policies and practices align with international human rights obligations regarding freedom of opinion and expression online.¹¹⁸

In 2011, the Four Special Rapporteurs on Freedom of Expression issued a joint declaration on freedom of expression and the internet, reiterating that freedom of expression applies to the internet as well as all means of communication,¹¹⁹ and restrictions on the right must be properly justified according to the recognised three-part test under international law.¹²⁰ Ensuring the effective exercise of this fundamental right creates an obligation on national authorities to promote universal access to the internet, regardless of political, social, economic or cultural differences.¹²¹ Analogising mandatory blocking of entire websites, IP addresses and network protocols to the banning of a newspaper or broadcaster, the declaration unequivocally stated that cutting off or slowing down internet access, even partially, “can never be justified, including on public order or national security grounds.”¹²² Likewise, another declaration in 2015 by the coalition also affirmed that using “kill switches” to shut down communications systems can never be justified under human rights frameworks.¹²³ In 2019, the coalition also called on states to recognise the right to access and use the internet as a human right and refrain from imposing internet or

telecommunications network disruptions and shutdowns.¹²⁴ Subsequently in 2023, they expressed alarm about authoritarian trends, the growing co-optation of public power, erosion of judicial independence and backsliding of human rights in many established and emerging democracies, and called on national authorities to refrain from “imposing internet throttling and/or shutdowns, which prevent access to information, undermine journalistic work, and often abet the perpetration or cover-up of human rights violations.”¹²⁵

In March 2023, Ambassador Michèle Taylor highlighted the concerning trend of governments worldwide acquiring, developing and deploying tools to enforce internet shutdowns, and reaffirmed the priorities of promoting and protecting fundamental freedoms by actively countering network disruptions.¹²⁶ On the World Press Freedom Day in 2021, Secretary of State Antony Blinken also condemned shutdowns in his diplomatic statements.¹²⁷ Assistant Secretary-General for Human Rights Ilze Brands Kehris also notes that deliberately cutting off internet access is a powerful tool of control over what kind of information can be accessed and shared, and is very hard to justify, if at all, under international human rights law.¹²⁸ In June 2021, the G7 leaders—representing over half of the world’s population living in democratic states—recognised freedom of expression online as an enabler of democracy and condemned “politically motivated internet shutdowns” in the open societies statement.¹²⁹ In a cyber declaration issued in 2018, the Commonwealth Heads of Government also committed to “limit the circumstances in which communication networks may be

intentionally disrupted, consistent with applicable international and domestic law.”¹³⁰

The Declaration of Principles on Freedom of Expression and Access to Information in Africa, issued in 2019, requires the national governments to recognise that “universal, equitable, affordable and meaningful access to the internet is necessary for the realisation of freedom of expression, access to information and the exercise of other human rights,” and prohibits engagement in or condonation of “any disruption of access to the internet and other digital technologies for segments of the public or an entire population.”¹³¹ In the same year, the special rapporteur on freedom of expression in Africa condemned shutdowns in several countries and observed that “[i]nternet and social media shutdowns violate the right to freedom of expression and access to information contrary to article 9 of the *African Charter on Human and Peoples’ Rights*.”¹³² Previously, a resolution passed by the African Commission on Human and Peoples’ Rights in 2016 called upon states to “respect and take legislative and other measures to guarantee, respect and protect citizen’s right to freedom of information and expression through access to Internet services.”¹³³

Because of the role of the internet in advancing public policy goals, in 2015, 194 countries of the United Nations General Assembly recognised information and communication technology as a horizontal catalyst to reach the 2030 Agenda. Reaffirming states’ human rights obligations, the 2030 Agenda reinforces the need for national governments to ensure a universally available and accessible internet, free from unjustified restrictions.

Furthermore, states have also committed to ensuring public access to information and protection of fundamental freedoms, in accordance with national legislation and international agreements. Grounded in international human rights instruments and informed by the *United Nations Declaration on the Right to Development*, the 2030 Agenda aims to realise “human rights of all,” making internet shutdowns contradictory to these commitments.¹³⁴

A declaration adopted in 2003 by the Council of Europe outline principles discouraging general blocking, filtering measures and other forms of prior state control that deny the population access to information and communication on the internet.¹³⁵ In the same vein, the Freedom Online Coalition, composed of thirty governments advocating for internet freedom, expressed profound concern regarding the escalating trend of deliberate state-sponsored disruptions to internet access and information dissemination in 2017.¹³⁶ In order to counteract the normalisation of internet shutdowns, it proposed a set of recommended best practices and principles for national authorities, including a public commitment to enact rights-respecting legislations that clearly delineates the limited circumstances in which communication networks can be disrupted in consonance with international human rights standards and improving transparency in regulatory, judicial and law enforcement agencies. In 2020, the coalition implored all governments to immediately end internet shutdowns and ensure the broadest possible access to online services.¹³⁷

B. DECODING ARTICLE 19, ICCPR

Obligations under paragraph (2) of Article 19, ICCPR includes respecting and ensuring the right “to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.”¹³⁸ Freedom of expression facilitates enquiry and the dissemination of information of every kind, through all conceivable media, as well as the propagation of political and other perspectives, and scrutiny and accountability of state. In fact, this right extends even to expressions that may offend, shock or disturb.¹³⁹ It also enables political engagement through freedoms of assembly, association and participation in public affairs and elections under Articles 21, 22 and 25 of the ICCPR.¹⁴⁰

It is therefore incumbent upon the national authorities to ensure that all individuals have meaningful and uninterrupted access to the internet, since they have a positive obligation to actively promote and protect freedom of expression,¹⁴¹ and to interpret this right in a manner that does not condone actions seeking to undermine freedom or interpret the restriction in a manner that enlarges the scope beyond what is outlined in the ICCPR.¹⁴² Hence, restrictions on websites, blogs, search engines or other internet-based information dissemination systems, or generally on access to the internet,¹⁴³ must adhere to the test firmly rooted in the principles of legitimacy, necessity and proportionality in paragraph 3 of Article 19, ICCPR (“Article 19(3), ICCPR”).¹⁴⁴

Article 19(3), ICCPR contains restrictively formulated limitation clauses. It establishes a three-part, cumulative test that serves as a crucial tool for evaluating the legality and legitimacy of restrictive measures pertaining to the right to freedom of expression. Any restrictions imposed on internet access, therefore, must be grounded in clear and accessible laws, pursue one of the permissible purposes of restriction, and represent an absolutely necessary course of action through the least restrictive means to achieve the intended aim.

First and foremost, restrictions on expression must be established by laws that are precise and accessible to the public. Laws should not grant excessive discretion to national authorities but should instead offer clear criteria for differentiating between permissible restrictions and protected expressions to enable individuals to regulate their conducts accordingly.¹⁴⁵ This approach promotes accountability, transparency and predictability, while allowing countervailing considerations to be balanced with right to freedom of expression.¹⁴⁶

Secondly, the restrictions must be firmly rooted in one of the two limitative areas of restrictions articulated in Article 19(3), ICCPR, viz. the rights or reputations of others, or the protection of national security, public order, or public health and morals. According to the *Siracusa Principles*, “[a]ll limitations on a right recognized by the [ICCPR] shall be provided for by law and be compatible with the objects and purposes of the [ICCPR].”¹⁴⁷ This means that not only must restrictions be established by laws, it must also be

compatible with the provisions, aims and objectives of the ICCPR.¹⁴⁸ No limitations can be implemented other than those listed in Article 19(3), ICCPR, and the grounds of limitation shall be interpreted strictly and in favour of the rights at issue.¹⁴⁹

Specifically, the rights of others and national security needs careful construction. The rights of others refer both to the rights contained in the ICCPR and those more generally recognised in human rights law. With respect to the oft-cited ground of national security, the *Siracusa Principles* clarifies that it can only be invoked to “protect the existence of the nation or its territorial integrity or political independence against force or threat of force,” and ought not be used for local or relatively isolated threats to law and order. General Comment 34 cautions that extreme care should be taken against the misuse of national security as a ground of limitation, such as in sedition counter-terrorism and official secret laws, or those which result in the prosecution of journalists, researchers, human rights defenders or others for disseminating information of legitimate public interest.¹⁵⁰ Furthermore, this ground cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exist adequate safeguards and effective remedies against abuse.¹⁵¹

All too often, however, internet shutdowns are enforced based on vague and overly broad legislations that confer unrestrained discretion to authorities.¹⁵² As elaborated above, restrictions are frequently based on unrecognised grounds, and in many cases no reasons are provided. Official justifications, when given, commonly

revolve around public safety and national security, or the need to restrict content deemed illegal or likely to cause harm, without mentioning specific circumstances or any explanations.¹⁵³ In such circumstances, the law may be deemed imprecise or inaccessible, failing to meet the first limb of the requirement set forth in Article 19(3), ICCPR.

Finally, the third component of the test requires an assessment of the necessity and proportionality of the restriction. As General Comment 34 puts it, the state must “demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.” A restriction must only be applied for purposes for which they were prescribed and must be directly related to the specific need on which they are predicated. Undertaking this evaluation entails considering the proportionality of the restrictive measures, by examining whether the measures are appropriate and the least intrusive means available to achieve the intended protective function.¹⁵⁴ Furthermore, the examination also involves weighing the impact and beneficial outcomes of both countenancing and constraining expression relative to the conflicting interests.¹⁵⁵

Disabling access to the internet is inherently disproportionate and can never be justified under Article 19(3), ICCPR,¹⁵⁶ as argued by UN Special Rapporteur Frank La Rue. He also asserted that all national authorities should ensure continuous internet access at all times, including

during times of political unrest.¹⁵⁷ Similarly, the Human Rights Committee observed that general restrictions on internet-based publishing should generally be content-specific, since generic bans on the operation of certain sites and systems are not compatible with Article 19(3), ICCPR.¹⁵⁸ Blanket restrictions on websites predominantly carrying legal content — such as YouTube, Facebook, Wordpress and Twitter — could be disproportionate since, in all likelihood, it will have the unintended consequences of false positives (i.e., resulting in blocking of websites with no prohibited material) and false negatives (i.e., websites with prohibited material will slip through the filter).¹⁵⁹ Other forms of network and communications disruptions, for instance, bandwidth throttling or regional blackouts, are also likely to have indiscriminate adverse effects, rendering them disproportionate.¹⁶⁰

However, a more narrowly targeted restriction on websites and internet-based communication services in highly exceptional circumstances may be deemed proportionate and justifiable under Article 19(3), ICCPR, if the restrictive measure is implemented as a last resort and in consideration of a clear need to protect others’ rights or reputation, or to safeguard national security of the country or maintain public order, whilst demonstrating that no other alternatives are available for effective prevention or mitigation of the underlying harms.¹⁶¹ Importantly, any law restricting the right to freedom of expression must be applied by a body that is independent of any political, commercial or other unwarranted influences, in a non-arbitrary and non-discriminatory manner, and ensures adequate safeguards

against abuse.¹⁶² But expressions cannot be restricted where the very reason that national security or public order has deteriorated is the suppression of human rights.¹⁶³ Onus to demonstrate that the restrictions are evidence-based and comply with the requisite standards is on the state agency seeking to restrict the right.¹⁶⁴

C. LAWSUITS AGAINST INTERNET SHUTDOWNS AROUND THE WORLD

In several jurisdictions around the world, strategic litigation has served as an aid to promote and protect human rights, at times leading to significant legal precedents and legislative reforms.¹⁶⁵ Lawsuits against internet shutdowns have increased in recent years, with the domestic and regional courts in India, Turkey, Togo and Russia having ruled against shutdowns, or, in some cases, made internet shutdown justifications and implementing procedures more transparent.

In August 2019, a sweeping ban was imposed on the internet and telecommunication services in Jammu and Kashmir due to concerns over potential violence. While affirming that the internet is the most used and accessible medium for disseminating information, the Supreme Court of India in *Anuradha Bhasin v. Union of India* (the “*Anuradha Bhasin case*”) held that the freedom of expression guaranteed under article 19(1)(a) of the country’s constitution includes the right to disseminate information to as wide a section of the population as is possible through the internet.¹⁶⁶ Consequently, any restriction on internet access must be sanctioned by law, align with the permissible grounds of limitation and

adhere to the principles of reasonableness.¹⁶⁷ While the existing laws sanctions internet shutdowns and there are guardrails built into the law (including requirements for restrictions to be temporary and orders to be properly reasoned, issued following due process and reviewed by an independent committee), however, they are susceptible to subjective assessments, misinterpretations and misuse by the authorities. The court concluded that internet shutdown is a drastic measure that should only be employed when absolutely necessary and unavoidable, and only when there are no less intrusive alternatives available.¹⁶⁸ Crucially, the provision enabling shutdown cannot be used as a tool to stifle constitutionally protected expressions of opinion or grievance, or the exercise of democratic rights, unless there is sufficient evidence demonstrating that such expression has been used to incite a situation of emergency.¹⁶⁹ After this decision was delivered in January 2020, access to the internet was partially restored in Jammu and Kashmir, allowing access to whitelisted websites at 2G mobile internet speed but the ban on social media and virtual private networks continued.¹⁷⁰ Full access to 4G internet was restored after 18 months of shutdown in February 2021.¹⁷¹

In December 2015, the European Court of Human Rights (the “ECtHR”) declared that a wholesale ban on YouTube in Turkey, imposed for hosting user-generated content insulting the memory of Mustafa Kemal Atatürk, resulting in the exclusion of the users from accessing the platforms altogether, was incompatible with Article 10 of the *European Convention of Human Rights* (“Article 10, ECHR”).¹⁷² In reaching this decision, the court recognised that

the video-sharing platform is an essential source of information and a vital means of communication, highlighting that restricting access to the platform deprives individuals of a significant avenue for exercising their right to receive and impart information and ideas.¹⁷³ However, the law empowering national authorities to block access to specific content cannot be interpreted to authorise the complete disabling of access to an entire website.¹⁷⁴ Although YouTube was unblocked in 2010 after over two years of restriction, this decision reaffirms the principle that a failure to meet lawfulness requirement could render an administrative decision incompatible with the fundamental right to expression.¹⁷⁵

Earlier in December 2012, in another factually similar but unrelated situation in Turkey, an incidental restriction on all websites hosted on Google domain, aimed at blocking a single website hosting insulting content about Mustafa Kemal Atatürk, was deemed by the ECtHR to be incompatible with Article 10, ECHR.¹⁷⁶ It was argued by the Open Society Justice Initiative that since search engines serve as a repository of vast amounts of information, it is comparable to the online archives of major newspapers or traditional libraries, and the restriction amounted to a prior restraint on expression.¹⁷⁷ In ruling that there is no provision in the law that allows for complete disabling of access to an entire website or domain, the court ruled that the interference was incompatible with freedom of expression due to a lack of legal foreseeability.¹⁷⁸ Notably, the Turkish government did not actively contest the case.

In March 2013, the ECtHR declared the

collateral blocking of access to a website hosted on the same server and sharing the same IP address as another website featuring cannabis-themed folk stories in Russia to be incompatible with freedom of expression protected under Article 10, ECHR.¹⁷⁹ Advocacy organisations, ARTICLE 19 and Electronic Frontier Foundation, contended that the indiscriminate blocking of websites constituted an extreme and disproportionate measure, analogous to banning a newspaper or television station, as it failed to differentiate between lawful and unlawful content.¹⁸⁰ Observing that a legal provision conferring an executive agency broad discretion carries a risk of arbitrary and excessive blocking, the court held that the inclusion of an IP address to the register of blocked materials leading to the incidental blocking of an entire cluster of websites that shared the same IP address, even though they were not unlawful, is not compatible with Article 10, ECHR.¹⁸¹ Additionally, the court also stated that it is incompatible with the principles of the rule of law and the foreseeability requirement if the legal framework fails to establish safeguards capable of protecting individuals from excessive and arbitrary effects of blocking measures. Having failed to meet the requirement of lawfulness, the interference was declared incompatible with Article 10, ECHR.¹⁸²

In June 2020, the Economic Community of West African States Community Court ruled that the intermittent shutdown measures implemented in response to anti-government protests in Togo had violated citizens' freedom of expression, as protected by Article 25 of the country's constitution.¹⁸³ In holding that access to the internet itself is not considered a

fundamental right, the court stated that it serves as a crucial platform for the exercise of freedom of expression, and is, therefore, considered a derivative right inherent to the exercise of this freedom.¹⁸⁴ More importantly, the court found that the interference with internet access was not sanctioned by any specific legislation, and the arguments presented by the government regarding national security were unconvincing to justify the internet shutdown.¹⁸⁵ As a result, the measures taken to disable access to the internet was violative of the right to freedom of expression, and the government was directed to prevent similar occurrences in the future and to enact necessary laws that are consistent with international human rights instruments.¹⁸⁶ Although internet access was disrupted for just seven days and restored in September 2017, this decision establishes a valuable precedent highlighting the significance of uninterrupted internet access as a fundamental precondition to exercise freedom of expression and the importance of compliance with legality requirement to ensure constitutional validity.

6. LEGAL RESPONSE TO INTERNET SHUTDOWNS IN BANGLADESH

A. APPLICATION UNDER THE RIGHT TO INFORMATION ACT, 2009

According to the preamble to the *Right to Information Act, 2009* (the “2009 Act”), the right to information is “an inalienable part of freedom of thought, conscience and speech,” necessary for enhancing

transparency, accountability and good governance within government institutions. In short, this statute enables free flow of information held by the state agencies,¹⁸⁷ including any information or order that may have been issued mandating internet shutdown.

Under the 2009 Act, every citizen has the right to receive information from state agencies by making a formal request.¹⁸⁸ It imposes a corresponding obligation on state agencies to furnish correct and complete information to the citizen within 20 working days of receipt of the request, or a maximum of 30 working days where more than one agency is involved, without necessarily having to obtain prior permission from the higher authority.¹⁸⁹ Obligation to supply requested information and documents — legally a public document¹⁹⁰ — is mandatory and absolute.¹⁹¹ A failure to furnish the information requested, or comply with the statutory timeline, therefore, entitles the applicant to appeal before an appellate authority, and decision of the appellate authority can be challenged before the Information Commission, which is authorised to conduct inquiry into the complaint, compel disclosure, impose civil fine and recommend departmental action for non-compliance.¹⁹² After exhausting the executive appeal process, proceedings can be initiated under article 102 of the Constitution of Bangladesh (“Article 102, Constitution”) (the “Constitution”).

Furthermore, state agencies are also obligated to proactively make available to the public necessary information related to decisions and actions taken by them, annual reports containing information on

the decision-making process and directives and orders issued, and in appropriate cases explanation on the reasons and causes of decisions.¹⁹³

However, information need not be disclosed in two specific cases. First, no disclosure is required where, relevantly, the information may threaten the security, integrity or sovereignty of the country, or it relates to a secret information protected by law.¹⁹⁴ However, in such cases, prior approval must be accorded by the Information Commission for withholding information. Secondly, information is not required to be furnished by eight agencies involved in state security and intelligence.¹⁹⁵

Nevertheless, the publication of an order mandating an internet shutdown issued by the BTRC does not appear to meet these exemptions, since its disclosure is not likely to threaten the security, integrity or sovereignty of the country, and the information contained in the order is not likely a secret information approved by the Information Commission. Furthermore, the telecom regulator is not an enlisted intelligence agency. Significantly, the 2009 Act overrides any conflicting legislation that disallows state agencies from providing information. Hence, any citizen can submit a formal request for the disclosure of the internet shutdown orders issued by the BTRC or any other state agency.

B. INITIATING PUBLIC INTEREST LITIGATION

Article 102, Constitution confers the right to initiate public interest litigation¹⁹⁶ before the High Court Division of the Supreme Court of Bangladesh (the “High Court Division”) in

two distinct manners.

Firstly, any person affected by an action or inaction of a state agency can file a public interest litigation, and the High Court Division can issue directions and orders to any person or authority, including those involved in the service of the republic, for the enforcement of fundamental rights.¹⁹⁷ Secondly, if the High Court Division finds no equally efficacious remedy in the existing laws, it can order a state agency to either cease unlawful activities or perform legal obligations and/or declare government actions as legally unauthorised and void.¹⁹⁸ While the first is rooted in the violation of fundamental rights by state and non-state actors, the latter extends only to actions and inactions of the government agencies,¹⁹⁹ and the courts can exercise both mandates conjunctively.

In Bangladesh, all three branches of the government operate “under a constitutional leash and circumspection,”²⁰⁰ empowering the High Court Division to invalidate laws or administrative actions infringing fundamental rights.²⁰¹ Constitutional courts have long upheld their jurisdiction to declare state actors’ arbitrary, discriminatory or unreasonable actions as invalid, and to rectify any impropriety.²⁰² Enforcement of fundamental rights is considered an obligation, not discretionary, as soon as a violation occurs,²⁰³ as the courts cannot “remain a silent spectator to the inertness on the part of the government or its officials.”²⁰⁴ This should hold true even if the state actors merely encourage interference, or informally direct the shutdown, as the state is still de facto responsible for those measures.

The mandates under Article 102, Constitution is broad enough for the High Court Division to nullify statutes and government actions violating fundamental rights²⁰⁵ and issue mandatory orders to both state and non-state actors. Notably, the right to initiate such judicial review proceedings is in itself a fundamental right,²⁰⁶ allowing for constitutional lawsuits challenging internet shutdowns. Such lawsuits can argue that shutdowns violate the right to freedom of speech and expression, protected under Article 39(2) (a) of the Constitution (“Article 39(2), Constitution”). Additionally, the legality of the shutdown orders can be contested on the grounds that the orders are not sanctioned by any specific law and/or not inadequately reasoned, contravening the requirements of equality of law and equal protection of law under Articles 27 and 31 of the Constitution (“Articles 27 and 31, Constitution”). The lawsuit may also seek specific directions to the BTRC to fulfil its statutory obligations, ensuring access to telecommunication services²⁰⁷ and preventing network shutdowns without clear legal authority, as well as a declaration that past shutdowns were without lawful authority and hold no legal effect.

Government-sanctioned internet shutdowns present a compelling case as a “public interest” concern due to their wide-ranging impact not only on individual’s right to freedom of speech and expression but also the collective right of society to access information and communicate freely. Decision by Mostafa Kamal J clarifies that when a public wrong or invasion of fundamental rights affects an indeterminate number of people — as it does with internet shutdowns — any citizen suffering the

common injury can be considered a “person aggrieved” with the right to invoke the jurisdiction under Article 102, Constitution, so long as the litigants are genuinely espousing a public cause and acting in the interest of the common good.²⁰⁸

It is worth highlighting that the authority under Article 102, Constitution has been instrumental in creating novel remedies and responses to rights violation, to address evolving challenges and shape legal frameworks to safeguard constitutional rights.²⁰⁹ For instance, the High Court Division utilised this authority to formulate guidelines on sexual harassment in 2009 and 2011,²¹⁰ subsequently codified in labour laws in September 2022. In another case, the court embraced the principle of *maxim salus populi suprema lex esto* — i.e., the welfare of the people should be the supreme law — asserting that safeguarding rivers from encroachments is a matter of public interest.²¹¹ Endorsing this view in 2019, the apex court declared all rivers in the country as living entities with legal personhood, placing the National River Conservation Commission in *loco parentis* for their protection.²¹² Currently, there is an ongoing constitutional matter concerning the government’s failure to regulate digital platforms, in which the High Court Division directed concerned authorities to formulate necessary regulations.²¹³ Therefore, the overall jurisdictional parameters exist for the High Court Division to entertain legal actions under Article 102, Constitution, enabling it to direct relevant authorities to establish rules on internet shutdowns and mandate the disclosure of shutdown orders not formally disclosed under the 2009 Act.

Set out below are two substantive grounds

for challenging internet shutdown under Article 102, Constitution.

I. FREEDOM OF EXPRESSION

Article 39(2), Constitution protects the right to freedom of speech and expression, subject to reasonable restrictions imposed by law on specified grounds. Mahmudul Islam highlights that this fundamental freedom encompasses not only a right to freely express and disseminate information through any means of communication but also includes the right to receive information and stay informed.²¹⁴ Implicit within this right, therefore, is the entitlement to access the internet as a medium of communication.

Affirming the sanctity of this fundamental right, the Supreme Court of Bangladesh has emphasised that the right should prevail without hindrance as long as expressions do not contravene legally sanctioned limits.²¹⁵ Freedom of expression and free flow of information are considered crucial liberties in the secular republic, serving as vital vector for open discussions and intellectual advancements.²¹⁶ Consequently, curtailment of this freedom solely on account of the unpopularity, hatefulness or perceived foolishness of an expression is not allowed, nor should restrictions be imposed merely because an expression challenges prevailing orthodoxies.²¹⁷

Citizens' entitlement to access information about the administration of the country and engage in discussions on public affairs and government criticism is foundational in a democratic state.²¹⁸ Embracing a broad spectrum of forms of expression, this fundamental freedom extends to acts of

protest, criticism of the government and its policies, and other political actions.²¹⁹ These forms of expression are vital for the functioning of a democratic society,²²⁰ enabling citizens to effectively participate in representative democracy. Given the importance of this freedom in the formation of public opinion on social, political and economic matters, political expressions are accorded a higher degree of protection compared to other types of expressions.²²¹

However, this fundamental right is not absolute. It is subject to the restrictions imposed by law on specified grounds exhaustively set out in Article 39(2), Constitution. These grounds include state security, friendly relationships with foreign governments, public order, decency, morality, contempt of court, defamation, or incitement of an offence.²²² In its assessment, the court will enquire whether the restriction can be justified as permissible limitations, rather than whether the right can be exercised in the face of the legal prohibition.²²³ Crucially, freedom of expression is the norm, and any limitation to this constitutional right is an exception.

For a restriction to be constitutionally valid, it must satisfy the three-part test inherent in Article 39(2), Constitution — i.e., the action must be based on law, founded on one of the qualified grounds, and reasonable.²²⁴ If one of these components are not met, the offending law or executive action may be deemed unconstitutional.²²⁵ In the following paragraphs are chronological analyses of each of the three components.

a. RESTRICTION IMPOSED BY LAW

In most jurisdictions, the legal bases for internet shutdowns are typically outlined in the legal frameworks and the licensing arrangements governing telecommunications.²²⁶ In Bangladesh, the primary legislation that confers to the regulator a mandate to regulate telecommunication services and systems in the country is the *Bangladesh Telecommunication Regulation Act, 2001* (the “2001 Act”), which is supplemented by the licensing guidelines issued by the BTRC.

Under its statutory authority, the BTRC is responsible for licensing and regulating operators that facilitate internet access within Bangladesh, including those managing mobile networks, internet services, international gateways and national internet exchanges. While neither the 2001 Act nor any secondary enactment contains express provisions empowering governmental agencies to mandate internet shutdowns or obligate operators to disable access to the internet, websites or internet-based communication tools, however, most licensing guidelines include broad clauses that require operators to comply with any directives, instructions or orders issued by the regulator. Failure to comply can result in licence suspension or cancellation, as well as wide-ranging criminal and administrative penalties. As such, in the absence of express provision on internet shutdowns, the BTRC exercises its discretionary power under open-ended compliance clauses to restrict internet access in the country.

Central to the concept of the rule of

law — enshrined in the preamble of the Constitution — is the requirement for reasonable and non-arbitrary laws upheld by the principles of due process, reasonableness and non-discrimination under Articles 27 and 31, Constitution.²²⁷ At a minimum, this entails that laws affecting individual liberty must be reasonably certain and predictable.²²⁸ When the law confers discretionary powers to state actors, there must be adequate safeguards against their abuse, particularly in cases where specific restrictions are not expressly authorised in a statute.²²⁹ Additionally, government agencies are also under an obligation to ensure that the statutory mandates are exercised within predefined limits and in a fair, reasonable, predictable, non-capricious, non-discriminatory and non-arbitrary manner.²³⁰ If a law is overly vague, lacks procedural safeguards against arbitrary exercise of power, or yields outcomes disproportionate to the intended remedy, restrictions can be deemed unconstitutional and voided to the extent of the inconsistency.²³¹ Ultimately, the objective is to provide individuals with a published standard against which they can assess the legality of their actions.²³²

Abuse or improper application of discretion, however, cannot be the sole basis for examining the constitutionality of a law, as it does not necessarily mean that the statute itself is unconstitutional.²³³ Generally, statutes are presumed to be constitutional, and historically, the courts have leaned against interpretations that render a statute unconstitutional.²³⁴ Statutes empowering executive bodies to exercise authority in a manner that encroaches on fundamental rights are narrowly construed to avoid declaration of unconstitutionality.²³⁵

However, it is important to note that interpretation of statutes is guided by the fundamental principles of state policy,²³⁶ which requires consideration of human rights and fundamental freedoms.²³⁷ As a result, if the wording of the statute is so vague that it will inevitably lead to abuse or improper application, or when the plain and literal meaning of a provision confers arbitrary discretion and no alternate interpretation exists, it will attract scrutiny of the constitutional courts.²³⁸

Examples of such scrutiny can be seen in the judgments of *Afzalul Abedin v. Bangladesh* and *Dr. Nurul Islam v. Bangladesh*. In the former case, the *Public Safety (Special Provision) Act, 2000* was declared unconstitutional due to its vagueness and the absence of guidelines and objective standards for enforcement,²³⁹ violating the non-discrimination and substantive due process requirements in Articles 27 and 31, Constitution.²⁴⁰ Dr. Kamal Hossain, a constitutional expert, opined that the fundamental flaw in the statute is that it enables the law enforcement authorities to choose individuals arbitrarily, inconsistently, whimsically and discriminatorily.²⁴¹ In the latter case, section 9(2) of the *Public Servants (Retirement) Act, 1974* was declared unconstitutional because it granted arbitrary discretion to force compulsory retirement of public servants.²⁴² Legal expert Syed Ishtiaq Ahmed argued that the statutory provision, in the absence of guidelines, confers unchecked and uncontrolled discretion to the state authorities to issue orders without assigning any reasons, leading to discriminatory outcomes.²⁴³

To understand the shortcomings of the legal framework on internet shutdowns in Bangladesh, it is useful to examine laws in comparable jurisdictions, and India is an excellent case study. Under the *Temporary Suspension of Telecom Services (Public Emergency or Public Service) Rules, 2017*, a delegated legislation created under the *Telegraph Act, 1885* of India, state agencies are expressly empowered to restrict internet access.²⁴⁴ There are some guardrails built into the rules, including requirements for restrictions to be temporary and orders to be properly reasoned, issued by a specified competent authority and notified to the telecommunication service providers by a senior officer. More importantly, a suspension order must be sent to a review committee by next working day, and the committee will then have to convene within five days to review the order and record its findings on the legality of the order. However, a report on internet shutdowns, prepared by a parliamentary standing committee led by Shashi Tharoor, noted that the rules still lack adequate safeguards and allows subjective assessments, misinterpretations and misuse by the authorities.²⁴⁵

Before 2017, internet shutdowns were generally imposed in India under section 144 of the *Code of Criminal Procedure, 1973*, which grants wide discretionary powers to specially empowered magistrates to issue written orders in situations posing imminent threats to human life or public peace.²⁴⁶ According to the standing committee report mentioned above, powers were exercised under this provision in “an arbitrary manner without an adequate safety valve.”²⁴⁷ However, a constitutional court earlier held that the provision does

not confer unfettered power on the magistrate, since it can only be exercised in the immediate prevention of sudden emergency situations, preceded by an inquiry with the material facts for exercising the power clearly set out, and the option to alter or rescind the order when the situation so warrants.²⁴⁸ Nevertheless, this provision cannot be used to suppress expressions unless evidence links them to incitement to an imminent state of emergency.²⁴⁹

In contrast with India, there are no enactments in Bangladesh that expressly empower state actors to impose internet shutdowns, define the circumstances in which restrictions may be imposed, specify the nature of restrictions, or establish the procedures to be followed when exercising such authority. While the BTRC has a statutory obligation to enact secondary legislations to address matters not sufficiently covered by the 2001 Act,²⁵⁰ as well as the authority to conduct public hearings on matters related to the exercise of its power and the regulation of the telecommunication industry,²⁵¹ there is no evidence of any initiative to comply with these requirements. Absent an express mandate, the BTRC has routinely enforced restrictions on internet access and internet-based communication tools, presumably on the basis of its undefined discretionary powers, often without issuing sufficiently reasoned order and reportedly at times without issuing written orders at all.²⁵² Such actions contradict the principles of legal certainty and predictability, as well as the need for adequate safeguards against potential abuse, potentially violating the constitutional requirement that restrictions be anchored on laws.

Thus, the constitutionality of using vague provisions of the 2001 Act or secondary legislations and licensing guidelines as the legal basis for issuing shutdown orders, and/or the inaction of relevant ministries in preventing such overreach, may be challenged under Articles 27 and 31, Constitution, and the executive orders mandating internet shutdowns may be challenged under Article 39(2), Constitution.

b. PUBLIC ORDER AND STATE SECURITY

Governments worldwide assert their sovereign authority and argue that shutting down the internet is necessary to counteract threats to public order and national security — the two most cited grounds of restrictions.²⁵³ This position aligns with the constitutive documents of the International Telecommunication Union, which grant countries the right to cut off telecommunication services in accordance with their national law, if it endangers state security or contravenes public order.²⁵⁴

In recent years, the Government of Bangladesh too has used the rhetoric of “public order” and “security of the state” to justify the implementation of restrictions on internet communication. While “public order” denotes an aggravated disturbance of public peace impacting the general public, “security of the state” signifies a situation where the disturbance has escalated to a point where the security of the country is at stake.²⁵⁵ Distinction between these terms is illustrated in the *Anuradha Bhasin* case using three concentric circles: “law and order” represents the largest circle, within which is the next circle representing “public order,”

and the smallest circle representing “state security.” It is then easy to see that an act may impact law and order but not public order just as an act may affect public order but not security of the state. Illustratively, a violent protest can qualify as contrary to public order, while calls for mutiny or coordinated acts of terrorism can be seen as threats to state security.²⁵⁶

However, several instances of internet shutdowns in Bangladesh raise questions about their relevance in maintaining public order and state security. For instance, the internet shutdown imposed between September 2019 and August 2020 in the refugee camps based on “security” grounds (as opposed to public order ground) may not withstand constitutional scrutiny, as there is no credible evidence indicating that the disturbances in the camps had escalated to a level where the security of the country was genuinely at stake. Considering the measures in place to isolate the refugees from the general population, it is arguable whether their activities could in reality ever have caused a disruption to public peace of such magnitude to warrant such a restriction. Underscoring the adverse effects of internet disruptions (along with seizures of mobile phones) on the right to freedom of opinion and expression, the UN Special Rapporteurs stressed that such network shutdowns not only fail to meet the standard of necessity, on the contrary, it interferes with other fundamental rights given the wide range of essential activities and services the restrictions affect.²⁵⁷

Sweeping restrictions on internet access can be seen as collective punishment on the citizens rather than a pragmatic

response to a real risk.²⁵⁸ Crucially, the security of the state is distinguishable from the security of the government, as peaceful and orderly opposition to the government, aimed at bringing about changes in policies or leadership, cannot be suppressed.²⁵⁹ Mere expressions of discontent towards the government, without incitement to violence, do not pose a direct threat to public order or state security.²⁶⁰ Therefore, the measures taken to throttle mobile internet service during student protests in August 2018 and restrictions on mobile internet during opposition rallies in 2022 may not be defensible on the grounds of public order, let alone national security. In December 2022, the #KeepItOn coalition appealed to the Government of Bangladesh to maintain “unfettered access to the internet for all, and to protect people’s fundamental rights and freedoms especially in times of protest.”²⁶¹

When it is not invoking the public order or state security grounds, the government is known to have relied on vague, and often impermissible, grounds of restriction. For example, orders to slow down internet speed to prevent academic misconduct during school examinations in February 2018,²⁶² and the proposal to do so again during medical examinations in 2023,²⁶³ do not clearly fall within the permissible grounds of restriction.²⁶⁴ Moreover, a geographically localised suspension of mobile internet access in the capital amid fighting between students of a college and local traders in April 2022 is also hard to rationalise.²⁶⁵ Constitutional basis of the restriction on the blogging site in 2019 also remains unclear. Restrictions on access to Facebook for a week and on YouTube for eight months in May 2010 and September

2012, respectively, for hosting content relating to Prophet Mohammed cannot readily be reconciled with constitutionally allowable grounds of limitation.²⁶⁶ Each of these instances demonstrate that restrictions on internet access are often based on undisclosed subjective criteria.

Orders to impose internet restrictions ahead of elections merit some elaboration. In December 2018, high-speed mobile internet services were shut down nationwide, purportedly to prevent the spread of rumours and propaganda on social media platforms.²⁶⁷ Such a measure is problematic for a number of reasons. Firstly, the order was not based on constitutionally permissible grounds of restriction. Secondly, it has a negative impact on democracy. Restricting access to the internet in the lead-up to an election means that the opposition will be less able to coordinate, canvas and campaign, during an election means that irregularities will not be immediately reported, and in the aftermath of a controversial election makes it harder for citizens to voice their discontent.²⁶⁸ Observers consider the national election, in which the ruling party won for a third consecutive five-year term with 96% of the parliamentary seats, was “neither free nor fair and marred by irregularities including ballot-box stuffing and intimidation of opposition polling agents and voters.”²⁶⁹

Thirdly, there is no evidence of effectiveness of shutdowns in the prevention of misinformation spreading during elections. Shutdowns do not curb the flow of information, as people continue to receive information over other mediums (such as over phone calls and text messages, or simply through word of

mouth). Contrarily, such measures amplify distrust and create conditions where fact-checking using digital tools is in many cases impossible, resulting in circulation of half-baked news and inauthentic information. Operating in the opposite direction, internet shutdown can in fact increase the spread of misinformation and reduce the agency to counteract it.²⁷⁰

Fourthly, shutdowns during contentious elections can create circumstances contrary to public order, and in extreme cases, state security. Studies indicate that information blackouts resulting from internet shutdowns can actually result in increased violence, with non-violent protests that rely on the internet for organisation substituted with aggressive tactics that are less reliant on effective communication and coordination.²⁷¹ Expressing similar views, the Internet Freedom Foundation observed that the perceived trade-off of internet shutdowns leading to better law and order outcomes with reduced risk of violence is dubious in its assumption at best.²⁷² Rather, the smokescreen that network restrictions offer can be used to conceal violence and human rights violations by state and non-state actors. Studies indicate that not only are shutdowns ineffective in pacifying protests, they often have the unintended consequence of incentivising violent forms of collective action and state-sanctioned human rights abuses during internet shutdowns.²⁷³ For instance, violence had increased substantially when the internet access was disrupted during the Syrian civil war in 2012 and widespread protests in Iran in 2019, suggesting the strategy has become part of a playbook to mask heavy-handed tactics by armed forces.²⁷⁴

c. REASONABLENESS OF RESTRICTIONS

The internet serves as an essential medium for mass communication, enabling citizens to actively participate in debates, disseminate alternative views, and express dissenting opinions.²⁷⁵ Occasionally, however, individual liberty and right to access the internet will be subordinate to the larger societal interests, warranting reasonable restrictions on fundamental rights and liberties.²⁷⁶

Assessing the reasonableness of such restrictions requires a delicate balance between protecting constitutional rights and preventing disorder and destabilisation in the country.²⁷⁷ Given the fact-sensitive nature of the assessment, the legislative view on what qualifies as reasonable is not conclusive, making it incumbent upon the court to conduct a thorough review and evaluate the reasonableness of the restriction.²⁷⁸ This principle of unreasonableness test was propounded in the case of *Associated Provincial Picture House Ltd vs Wednesbury Corporation*²⁷⁹ and severally invoked in several domestic cases.²⁸⁰ A decision is *Wednesbury* unreasonable (or irrational) if it is so unreasonable that no reasonable person acting reasonably could have made it.

Central to this assessment is determining whether the imposed restrictions have a nexus with the legislative objective and whether restriction exceeds what is necessary to achieve that objective.²⁸¹ Restrictions that are general, abstract or indefinite in duration are unlikely to be deemed reasonable.²⁸² Similarly, reflexive exercise of discretionary powers, even if

conferred by the parliament in absolute terms, can also result in unreasonableness.²⁸³ Lord Diplock's aphorism — "you must not use a steam hammer to crack a nut if a nutcracker would do" — captures the essence of the requirement that all state action should be reasonable and commensurate with the objectives it intends to achieve.²⁸⁴

In the *Anuradha Bhasin* case, the court emphasised that while the government can legally impose a wholesale ban on internet access, it must ensure that the restriction is not excessive, as the principles of proportionality requires the government to be able to justify the restriction and explain why less severe alternatives are inadequate.²⁸⁵ Doctrinally, proportionality is a subset of the concept of reasonableness. Reasonableness of a restriction should be determined objectively, considering the interests of the general public rather than focusing solely on the individuals subjected to the restrictions, or abstract considerations.²⁸⁶ Disabling access to the internet, a drastic measure, should only be considered when absolutely necessary and unavoidable, and when no less intrusive alternatives are available.²⁸⁷ Moreover, the territorial and temporal scope of the restriction should be reasonable relative to a genuine need required to address the emergent situation.²⁸⁸

Several shutdown measures in Bangladesh do not demonstrate sufficient reasonableness. For instance, the restrictions on instant messaging services in January 2015 and broadband internet in July 2016, driven by concerns about potential misuse by terrorists, do not appear to be reasonable for three

distinct reasons. Firstly, these restrictions assume that such services are the sole or primary means of communication for criminal actors. While it is well accepted that modern terrorism relies heavily on the internet for raising funding, recruitment and spreading propaganda and ideologies,²⁸⁹ there is no conclusive evidence that blanket restrictions on the internet, or social media intermediaries, effectively mitigate those risks. Alternative communication channels (ranging from cellular network connections to alternative messaging and voice-over-internet-protocol services) were accessible at all material times during the incidents, weakening the argument for the necessity and reasonableness of the restrictions. Secondly, decisions to block access to these services were based on speculative prognostication of future events and perceived risks. While an anticipatory measure to address foreseeable risks to public order or national security will not necessarily amount to an unreasonable restriction,²⁹⁰ in these cases there was no concrete proof of the extent to which these services can be, or has been, used for unlawful activities. Finally, where specific websites or mobile applications are disabled, it is easy to bypass the restriction, for instance, using virtual private networks, even for technically unskilled individuals.²⁹¹

It is also questionable whether the restriction on internet access in the refugee camps was reasonable. Even if the internet shutdown and disruption to mobile network services in the refugee camps are presumed to be reasonable in normal circumstances, it can hardly be justified on public order or national security grounds during the COVID-19 pandemic, when access to information was of critical

importance and the non-derogable right to life was at risk.²⁹² Disabling access to online information and communications not only isolated the refugees from the rest of the world, it also prevented them from accessing vital health information during an unprecedented health crisis and disallowed aid workers and humanitarian actors from coordinating emergency services.²⁹³ Disruption in the already fragile information and communication ecosystem perpetuated misinformation and mistrust and exacerbated the vulnerabilities and challenges already faced by the refugees and is therefore likely to be deemed unreasonable.²⁹⁴

Of the over 130 million internet users recorded by the BTRC in November 2023 in Bangladesh, over 90% use mobile internet, while the remaining 10% of connections are through broadband.²⁹⁵ Disabling or throttling access to mobile internet has a sweeping effect on the majority of internet users, rendering the measure unreasonable. Unlike measures to block specific websites or content, disabling access to the internet as a whole treats all internet traffic as unlawful, making such restrictions on mobile internet unreasonable in most situations.²⁹⁶

When restrictions are implemented during elections or peaceful protests, they excessively impede citizens' ability to engage in political discourse, form peaceful assemblies online, access essential services and make informed decisions, thereby limiting the diversity of voices and perspectives in the public sphere. An internet shutdown ahead of the national election in 2018 was enforced in order to prevent rumours circulating on social

media platforms, despite international calls to ensure stability and openness of the internet during the elections, as “free and open internet expands political discourse and is an indicator of a legitimate election” and there is no evidence that “measures like shutdowns and throttling will stop the spread of disinformation and propaganda online.”²⁹⁷ While social networking and instant communication services could serve as the primary conduits of false information, neither the government nor any independent research provides a correlation between internet restrictions and more accurate electoral outcomes or peaceful elections. Limiting access to internet and important websites dissuades democratic practices and undermines the integrity of elections, thereby diminishing the democratic fabric of the nation,²⁹⁸ and is, therefore, unreasonable.

Furthermore, if internet shutdowns are used to block access to specific websites and applications, access to other unrelated services may also be impacted as collateral damage. For instance, shutting down internet access to block certain social media services will also limit access to internet-enabled ride sharing applications, messaging platforms, online banking and mobile financial services and e-commerce, creating a disproportionate and unreasonable disruption to the lives of the citizens.²⁹⁹ As an illustration, in Kashmir, thousands travelled on a train known as the “Internet Express” to towns unaffected by internet restrictions, simply to fill out online job applications and check business emails.³⁰⁰

Unreasonableness of an internet shutdown can also be argued in terms of

its economic costs. Given the increasing reliance of businesses and trade on digital technologies and the internet, disruptions to internet and communications services are highly detrimental to all sectors of the economy. According to a 2016 Deloitte study, the impacts of a temporary shutdown of the internet grow larger as a country develops and as a more mature online ecosystem emerges.³⁰¹ It is estimated that for a low (internet penetration <49%) and medium (internet penetration 49-79%) internet connectivity economies, the per day impact of a temporary shutdown of the internet and all of its services would on average be US\$ 0.6 million and US\$ 6.6 million for every 10 million population, respectively.³⁰²

Other studies have also indicated the staggering financial implications of such shutdowns. For instance, a study by the Brookings Institution revealed that internet shutdowns across 19 countries between July 1, 2015 and June 30, 2016 resulted in a global loss of US\$ 2.4 billion in gross domestic product.³⁰³ Another study by Top10VPN indicates that shutdowns in 46 countries between 2019 and 2021 led to economic losses amounting to US\$ 20.5 billion.³⁰⁴ Notably, the World Bank calculated that internet shutdowns in Myanmar alone had cost nearly US\$ 2.8 billion between February and December 2021,³⁰⁵ reversing economic progress made over the previous decade.³⁰⁶ In 2019, the internet shutdowns in Indian-administered Kashmir and in Sudan had cost their economies more than US\$ 2.4 billion and US\$ 1 billion, respectively.³⁰⁷ Estimates from NetBlocks, which track and document internet disruptions worldwide, indicate an estimated loss of approximately US\$

78 million per day for nationwide internet shutdown and around US\$ 10 million daily for country-wide restriction in Bangladesh on Facebook and WhatsApp.³⁰⁸ Indirect economic impact includes factors such as the loss of domestic and international investor confidence as well as increased cost of doing business.³⁰⁹ However, no impact assessment study has been done in Bangladesh to assess the economic implications of shutdown measures. Considering the extraordinary economic costs associated with internet shutdowns, it is more likely than not that such measures will be deemed unreasonable.

II. DISCLOSURE OF DULY REASONED ORDERS

Every citizen is entitled to receive a reasoned order from government authorities.³¹⁰ A fundamental principle of the rule of law, and indeed Articles 27 and 31, Constitution, requires establishment of a polity where state functionaries must justify their actions with reference to clear legislative mandate and executive actions operating to the prejudice of an individual must be adequately and logically reasoned.³¹¹ As government actions have a public element, they must be guided by public interest and reason.³¹² In order for an administrative order to be valid and effective, it must be accurately recorded, adequately reasoned and appropriately communicated to the affected individuals, in line with the rules of natural justice.³¹³

Of note, the administrative law requirement to issue a duly reasoned order is supplemented by statutory obligations under the 2001 Act to ensure that decisions are made in an open, fair and transparent

manner³¹⁴ and under the 2009 Act to publish administrative orders and other information related to actions taken, along with necessary explanations. However, executive orders sanctioning internet shutdowns are not publicly disclosed. Government representatives have often refused to acknowledge the existence of disruptions or denied ordering the interference, attributing the shutdowns to system overloading or technical glitches.³¹⁵ In cases where internet shutdowns are acknowledged, the reasons are vague at best.

Access Now has aptly highlighted the challenges with vague explanations provided by the regulator regarding internet shutdown: they “are often issued to telecommunications companies behind closed doors, and provide only general information about justification, reach, duration, or underlying legal authority.”³¹⁶ Simply disclosing the fact that shutdown was imposed does not justify it or account for the rights implications of failure to issue a reasoned order.³¹⁷ Rather, it creates confusion.

Difficulty in producing administrative orders mandating internet shutdown in the Jammu and Kashmir was declared as invalid ground for failure to produce the orders before the court in the *Anuradha Bhasin* case, as effective enforcement of fundamental rights cannot be realised without meaningful access to information in the possession of the state.³¹⁸ Although a parent or subsidiary statute may not explicitly require publication and notification of the orders, it is a settled principle of law and natural justice that an order affecting lives, liberty and property of individuals must be

made freely available through appropriate mechanism, irrespective of whether the statutes prescribe it or not.³¹⁹ Even in cases where there are some overriding grounds of privilege or countervailing public interest is to be balanced, a redacted version of the orders must be adduced.³²⁰ In that case, the court directed the state to publish all existing and future orders for suspension of internet services to enable the affected persons to challenge it before the court, which prompted the government to amend the rules in November 2020 to ensure that a suspension order is not in operation for more than fifteen days and all such orders are made publicly available.

As such, after exhausting the statutory procedure under the 2009 Act, a public interest litigation can be filed under Article 102, Constitution to challenge the failure of the government to issue duly reasoned administrative orders mandating shutdown and to compel disclosure of all such orders, as failure to do so may constitute violation of Articles 27 and 31, Constitution.

Can the domestic courts rely on international human rights law?

Domestic statutes are generally presumed to be in conformity with international law and should be interpreted accordingly, unless the wording of the statute clearly contradicts international provisions. If the language of the statute is clear and unambiguous, it should be applied even if it conflicts with international law. However, in cases where the legislation is unclear and open to multiple interpretations, the relevant treaty comes into play, as there is a presumption that parliament did not intend to violate international law. In such cases,

an interpretation that aligns with treaty obligations should be preferred.³²¹

In *Bangladesh v. Abdul Quader Molla*, several amici curiae shared their insights on this matter.³²² Tafazzal Hossain Khan opined that when national law is incomplete, vague or undefined, and international jurisprudence has developed on the specific issue, national courts have an obligation to follow those principles to address any gaps or omissions.³²³ Aligned with this view, Mahmudul Islam stated that while the domestic courts do not enforce treaties and conventions unless incorporated into municipal legislation, they can still be considered as an aid for interpretation.³²⁴ Expressing similar views, Rokanuddin Mahmud and Ajmalul Hussain KC averred that international law cannot intrude on matters covered by domestic legislation but can only apply to areas unaddressed within domestic legislation.³²⁵ Hassan Arif emphasised that the Constitution mandates respect for international law and the principles enunciated in the Charter of the United Nations as one of the fundamental state policies of the nation, allowing domestic courts to consider international law and evolve their domestic jurisprudence.³²⁶

Concurring with these submissions, the apex court affirmed that although international human rights norms are not part of the *corpus juris* of the state and directly enforceable in domestic courts unless specifically incorporated into national law, they can be considered as persuasive authorities.³²⁷ International instruments serve as aids to interpretation of fundamental rights when domestic laws are not sufficiently clear or silent on

a matter.³²⁸ Indeed, the courts should “forever remain alive to the international instruments and conventions and apply the same to a given case when there is no inconsistency between international norms and the domestic law occupying the field.”³²⁹ While inconsistencies between national and international laws should be ruled in favour of national laws, the court has the responsibility to draw the attention of the lawmakers to such inconsistencies.³³⁰

Accordingly, the High Court Division may refer to the text of Article 19, ICCPR, as well as associated general comments and concluding observations issued by the HRC, the 2030 Agenda, and resolutions and declarations of the United Nations, the Council of Europe, and the Four Delegates on Freedom of Expression, in assessing the constitutionality of internet shutdowns. Additionally, foreign judgments on internet shutdowns can also be relied upon as persuasive authority, to the extent they are consistent with domestic jurisprudence.

7. RECOMMENDATIONS

A. LEGISLATIVE REFORMS

As mentioned above, the BTRC has a statutory obligation to enact secondary legislations to address matters not sufficiently covered by the 2001 Act,³³¹ as well as the authority to conduct public hearings on issues related to the exercise of its power and the regulation of the telecommunication industry.³³² As such, if the Government of Bangladesh does not amend the 2001 Act, secondary enactments should be formulated under sections 98 or 99 of the 2001 Act to explicitly mandate internet shutdowns. In pursuing legislative reforms, it is crucial to

consult the relevant ministries. Any rules or regulations drafted should be subject to public consultation in accordance with article 31A of the *Rules of Business* and section 87 of the 2001 Act.³³³

B. LEGALITY OF SHUTDOWN ORDERS

Consistent with the recommendations by the HRC, internet shutdowns should strictly adhere to the essential requirements of legality in all cases. Orders to disable or throttle internet connection, or impede accessibility and usability of online interactive communications tools such as social media and messaging services, should be:

- i. grounded in publicly available law that expressly confers powers to specified state agency. The exercise of powers under the law should be guided by sufficient guidelines and objective standards for enforcement, and subject to adequate safeguards against abuse.
- ii. necessary to achieve one of the specified grounds of restrictions, as set out in Article 39(2), Constitution.
- iii. reasonable and the least intrusive means to achieve the intended restrictions. Accordingly, the order should be as narrow as possible, in terms of duration, geographical scope and the networks and services affected, and precision tools should be opted over blanket restrictions.
- iv. accurately recorded, appropriately substantiated, adequately reasoned and communicated in advance to the affected individuals and telecommunications service providers, along with a clear explanation of the

legal basis and factual circumstances surrounding the shutdown and details regarding its scope and duration.

- v. published and publicised in compliance with the 2009 Act and constitutional requirements.
- vi. subject to prior authorisation by a court or other independent adjudicatory body, in order to avoid any political, commercial or other unwarranted influence.
- vii. subject to meaningful and timely redress mechanisms accessible to those whose rights have been affected by the shutdowns, including through judicial proceedings under Article 102, Constitution, even after the end of the shutdown. To be considered as effective, the remedies must be capable of restoring the violated rights as much as is possible, cease ongoing violations, and prevent the repetition of similar violations in future.

C. COMPLIANCE BY CORPORATIONS

According to the *UN Guiding Principles on Business and Human Rights*,³³⁴ commercial enterprises — including mobile network operators and internet service providers — should have policies and processes:

- i. affirming their commitment to respect fundamental rights under the Constitution and international human rights framework;
- ii. setting out procedure for human rights due diligence, aimed at identifying, preventing, mitigating and accounting

for how impacts on human rights are addressed; and

- iii. enabling the remediation of adverse human rights impacts caused or contributed by their activities.

Additionally, enterprises should refrain from imposing internet restrictions that are not sanctioned by law and/or unnecessary, unreasonable or lacking proper reasoning. If faced with unlawful orders, companies should take measures to protect consumer interest, including by refusing to comply with the unlawful orders and challenging the orders in judicial forums in appropriate cases.³³⁵ Companies must also be transparent and disclose to the public when they receive unlawful orders to impose internet restrictions. Article 102, Constitution entitles the High Court Division to issue directions and orders to “any person or authority” for the enforcement of the fundamental rights, and this discretion could extend to issuing directions on private enterprises.

D. FREEDOM OF INFORMATION REQUESTS

An application for disclosure of shutdown orders can be filed with the BTRC and other appropriate authority by any citizen, and the state agency must furnish requested information within statutorily prescribed timeline. A failure to provide information requested, or comply with the statutory timeline, can be challenged before an appellate authority, and then before the Information Commission if the decision of the appellate authority is unsatisfactory. After exhausting executive appeal process, proceedings can be initiated under Article 102, Constitution.

E. PUBLIC INTEREST LITIGATION

A public interest litigation can be filed under Article 102, Constitution by individuals as well as industry associations and rights organisation with sufficient standing to challenge the legality of internet shutdowns, on the grounds that such measures infringe Article 39(2), Constitution and/or Articles 27 and 31, Constitution. In this lawsuit, the petitioner can seek specific directions from the High Court Division to direct the BTRC as well as the telecommunication service providers to ensure uninterrupted internet access and to refrain from imposing unlawful restrictions. Furthermore, direction may also be sought for the disclosure of the shutdown orders and the formulation of rules on internet shutdowns. Even if the litigation formally fails, it will have created a legal precedent and provided vital transparency on the origins, duration and impact of shutdowns.

8. CONCLUSION

Disconnecting access to the internet and online communications tools not only hinders the free flow of information, rather, given their indiscriminate reach and adverse impacts, also fails to meet the constitutional criteria for restrictions, even in the face of legitimate threats. Internet shutdowns undermine individuals' ability to participate in shaping their own lives and contributing to the development of secure and prosperous societies, and further entrenches digital divides between and within countries. It is imperative, therefore, for the Government of Bangladesh to reassess its reliance on internet shutdowns and explore more effec-

tive, human-centric and rights-respecting alternatives for addressing security and public order concerns. Efforts should focus on promoting transparency, accountability, and adherence to human rights standards, ensuring that the benefits of the internet are accessible to all individuals without unnecessary and disproportionate restrictions.

Stopping internet shutdowns is a moon-shot problem, but there are multiple moons and a thousand trajectories.³³⁶ Strategies for controlling information flows online, and resisting such control, are amorphous, evolving and multifaceted. As technology advances and the digital landscape continues to transform, internet shutdowns, as defined in this report, will vary along dimensions such as duration, breadth, depth, speed, frequency and tactics. Confronting this challenge requires a concerted effort, as there is no one-size-fits-all solution or universal strategy. It is crucial to explore diverse approaches, employing a balanced mix of carrots and sticks, in consideration of the unique social, economic and political contexts of Bangladesh. The recommendations presented in this report serve as a starting point for initiating meaningful change and fostering a rights-respecting approach that ensures equal access to the benefits of the internet for all individuals in the country.

ENDNOTES

- 1 [‘Public Acceptance of Internet Censorship in Indonesia’](#), *Australasian Conference on Information Systems* (2021).
- 2 [‘Advancing Strategic Litigation on Internet Shutdowns cases in Africa: Promises and Pitfalls’](#), *Collaboration on International ICT Policy for East and Southern Africa* (2022).
- 3 [‘Digital dictatorship: authoritarian tactics and resistance in Eastern Europe and Central Asia’](#), *Access Now* (2023).
- 4 Access Now defines “internet shutdown” as “an interference with electronic systems primarily used for person-to-person communications, intended to render them inaccessible or effectively unusable, to exert control over the flow of information.” According to the #KeptOn coalition, the term refers to “an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.” However, these definitions, including the one proposed in this report, are not exhaustive. With advancements in technologies and technical capabilities, governments worldwide are adopting suite of more finely honed control tools to enforce network shutdowns, which may not fall squarely within these existing definitions. See also [‘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 Rights’](#), *Human Rights Council* (A/HRC/50/55, 2022), [4] (A/HRC/50/55); [‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression’](#), *Human Rights Council* (A/HRC/35/22, 2017), [8]; [‘Ending internet shutdowns: a path forward - Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association’](#), *Human Rights Council* (A/HRC/47/24/Add.2, 2021), [7] (A/HRC/47/24/Add.2).
- 5 [‘The draconian rise of internet shutdowns’](#), *Wired* (2021) (‘2021 Wired Report’).
- 6 [‘The right to development and internet shutdowns: Assessing the role of information and communications technology in democratic development in Africa’](#), *Global Campus Human Rights Journal* (2019).
- 7 For example, in Myanmar, communications services have been disrupted since the military coup in February 2021, with several townships in conflict- and violence-affected areas without any internet or, in some cases, fixed or mobile telephone lines. In the English-speaking part of Cameroon and India-administered Kashmir experienced shutdowns that lasted many months. See [‘Situation of human rights in Myanmar since 1 February 2021 - Report of the United Nations High Commissioner for Human Rights’](#), *Human Rights Council* (A/HRC/49/72, 2022), [48]-[49]; [‘Concluding observations on the fifth periodic report of Cameroon’](#), *Human Rights Committee* (CCPR/C/CMR/CO/5, 2017), [41]; [‘UN expert urges Cameroon to restore internet services cut off in rights violation - Internet cut off’](#), *United Nations Human Rights Office of the High Commissioner* (2017); [‘UN rights experts urge India to end communications shutdown in Kashmir’](#), *United Nations Human Rights Office of the High Commissioner* (2019); [‘Disconnected: A Human-Rights Based Approach to Network Disruption’](#), *The Global Network Initiative* (2019) (Jan Rydzak Report 1).
- 8 [‘Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?’](#), *Carnegie Endowment for International Peace* (2022). See also A/HRC/50/55 (n 4) [30], [47].
- 9 [‘Africa’s Internet Shutdowns: A report on the Johannesburg Workshop’](#), *University of Oxford* (2019) 2 (Marchant and Stremlau Report).
- 10 [‘How to shut down the internet – and how to fight back’](#), *The Guardian* (2022); [‘The Internet Shutdowns Issue’](#), *The Current* (2021).
- 11 Jan Rydzak Report 1 (n 7) 6; Marchant and Stremlau Report (n 9) 7.
- 12 According to a survey by the BRAC Institute of Governance & Development, approximately 96% of the rural population in Bangladesh with access to the internet uses mobile internet. See [‘Digital Literacy in Rural Bangladesh: Survey 2019’](#), *BRAC Institute of Governance & Development* (2020).
- 13 Marchant and Stremlau Report (n 9) 3.
- 14 A/HRC/50/55 (n 4) [5].
- 15 [‘Legal Guidance on Internet Restrictions and Shutdowns in Africa’](#), *International Commission of Jurists* (2022) 2-4; [‘United Nations Office of the High Commissioner for Human Rights Call for Input: U.N. Human Rights Council 50th Session report on Internet Shutdowns and Human Rights’](#), *Access Now* (2022) 2.
- 16 [‘How to shut down the internet – and how to fight back’](#), *The Guardian* (2022).
- 17 Jan Rydzak Report 1 (n 7) 26.
- 18 [‘A Taxonomy of Internet Shutdowns: The Technologies Behind Network Interference’](#) *Access Now* (2022) 6.
- 19 [‘Palestine unplugged: how Israel disrupts Gaza’s internet’](#), *Access Now* (2023); [‘How Israel is shutting down the internet in Gaza’](#), *Access Now* (2023).
- 20 [‘How Russia Took Over Ukraine’s Internet in Occupied Territories’](#), *The New York Times* (2022)
- 21 [‘Parts of country plunge into the long dark over ‘technical glitch’](#), *The Business Standard* (2022); [‘Mobile users suffer as towers go down in Sylhet’](#), *The Daily Star* (2022).
- 22 [‘Freedom on the Net 2023: The Repressive Power of Artificial Intelligence’](#), *Freedom House* (2023).
- 23 A/HRC/47/24/Add.2 (n 4) [4].
- 24 Jan Rydzak Report 1 (n 7) [8]-[9].
- 25 [‘Nepal: Out of the Silence’](#), *Committee to Protect Journalists* (2005).
- 26 [‘Internet access cut off in Burma’](#), *The Guardian* (2007).
- 27 [‘Shutting Down the Internet to Shut Up Critics’](#), *Human Rights Watch* (2020).
- 28 [‘Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022’](#) *Access Now* (2023) 4 (‘Access Now Report 2022’).
- 29 [‘“No Internet Means No Work, No Pay, No Food”: Internet Shutdowns Deny Access to Basic Rights in “Digital India”](#), *Human Rights Watch* (2023) (‘2023 HRW India Article’).
- 30 2021 Wired Report (n 5).
- 31 [‘Internet Shutdowns Myanmar’](#), *Internet Society Pulse* (2021).
- 32 [‘Ruined my livelihood: Pakistan internet shutdown hits millions’](#), *Al Jazeera* (2023).

- 33 [‘Pakistanis have long suffered from internet shutdowns. At last, their voices are being heard’](#), *Access Now* (2023); [‘Internet Shutdowns in Asia: Locating the Right to the Internet a Human Right Under International Human Rights Law’](#), *Cambridge Core Blog* (2023)
- 34 [‘Multiple Internet Disruptions Observed in Iran’](#), *Internet Society Pulse* (2022); [‘Iran blocks capital’s internet access as Amini protests grow’](#), *The Guardian* (2022).
- 35 [‘Kazakhstan’s internet shutdown is the latest episode in an ominous trend: digital authoritarianism’](#), *The Conversation* (2022).
- 36 Marchant and Stremlau Report (n 9) 4.
- 37 [‘Iraq: Exam Season 2023 Internet Shutdowns’](#), *Internet Society Pulse* (2023).
- 38 [‘Study on Internet Shutdowns in Africa’](#), *The African Internet Rights Alliance* (2021).
- 39 2021 Wired Report (n 5).
- 40 [‘Walking Through Firewalls: Circumventing Censorship of Social Media and Online Content in a Networked Authoritarian Context’](#) *Social Media + Society* (2022).
- 41 [‘How Weaponization of Network Disruptions During Elections Threatens Democracy’](#), *Collaboration on International ICT Policy for East and Southern Africa* (2021).
- 42 [‘#KeepItOn: Eswatini authorities shut down internet to quell protests, ask people to email grievances’](#), *Access Now* (2023)
- 43 [‘Burkina Faso Must Immediately End Its Internet Shutdown, Not Extend It’](#), *Access Now* (2023); [‘Internet Shutdowns Burkina Faso’](#), *Internet Society Pulse* (2021).
- 44 [‘Internet Shutdowns Senegal’](#), *Internet Society Pulse* (2023).
- 45 [‘Back in the dark: Ethiopia shuts down internet once again’](#), *Access Now* (2023).
- 46 [‘Six million silenced: A two-year internet outage in Ethiopia’](#), *Reuters* (2022).
- 47 [‘Open letter to the Ethiopian Government: urgently end ongoing internet shutdowns in all regions across the country’](#) *Access Now* (2023); [‘Authorities in Ethiopia must restore internet access in Amhara’](#), *Access Now* (2023)
- 48 [‘DR Congo internet restored after 20-day suspension over elections’](#), *Al Jazeera* (2019).
- 49 [‘Social media restricted in Mali amid protests against president’](#), *Netblocks* (2020).
- 50 [‘Zimbabwe imposes internet shutdown amid crackdown on protests’](#), *Al Jazeera* (2019).
- 51 [‘Judges raise the gavel to #KeepItOn around the world’](#), *Access Now* (2023).
- 52 [‘Internet Shutdowns Chad’](#), *Internet Society Pulse* (2023).
- 53 [‘Extinction Rebellion: London Tube Wifi Shut Down By Police In Attempt To Disrupt Climate Change Protesters’](#), *The Independent* (2019).
- 54 Marchant and Stremlau Report (n 9) 4.
- 55 [‘San Francisco Subway Shuts Cell Service to Foil Protest; Legal Debate Ignites’](#), *Wired* (2011).
- 56 A/HRC/50/55 (n 4) [1].
- 57 Access Now Report 2022 (n 28).
- 58 [‘Freedom on the Net 2023: Bangladesh’](#), *Freedom House* (2023).
- 59 [‘YouTube blocked’](#), *The Daily Star* (2009). Subsequently, in September 2012, YouTube was blocked again for hosting a movie trailer that denigrated the Prophet Mohammad, only to be restored over eight months later as inaccessibility was inconducive. See [‘Bangladesh lifts ban on YouTube, blocked after anti-Islam film’](#), *Reuters* (2013).
- 60 [‘Networking sites to be reopened in couple of days: Minister’](#), *Prothom Alo* (2015).
- 61 Access to Facebook has been blocked on at least three occasions since 2010. In late May 2010, access to the social media services was blocked for a week for hosting offensive caricatures of the Prophet Mohammed and satirical images of political leaders. See [‘Access to Facebook restored in Bangladesh’](#), *Reporters Without Borders* [‘facebook blocked’](#), *The Daily Star* (2010).
- 62 [‘Bangladesh Bans Facebook and Chat Apps on ‘Security Grounds’](#), *Global Voices Advox* (2015).
- 63 [‘Govt blocks Twitter, Skype, lmo’](#), *The Daily Star* (2015); [‘Bangladesh lifts ban on all social media’](#), *The Express Tribune* (2015).
- 64 [‘Bangladesh holds internet blackout drill to deal with emergencies like Dhaka terror attack’](#), *BDNews24* (2016).
- 65 [‘Internet shutdowns now ‘entrenched’ in certain regions, rights council hears’](#), *United Nations* (2021); [‘Bangladesh To Restore Phone, Internet At Rohingya Camps’](#), *Anadolu Agency* (2020).
- 66 [‘#Keepiton: Internet Shutdowns Put Lives At Risk During Covid-19’](#), *Access Now* (2023).
- 67 [‘Mobile net slowed down’](#), *The Daily Star* (2018); [‘Unrest in Bangladesh as student road safety protests turn violent’](#), *The Guardian* (2018).
- 68 Jan Ryzdak Report 1 (n 7) 12.
- 69 [‘Bangladesh slows down mobile internet speeds ahead of election - Daily Star’](#), *Reuters* (2018).
- 70 [‘Minister: Govt permanently blocked 22,000 porn sites and 6,000 gambling sites’](#), *Dhaka Tribune* (2022).
- 71 [‘Bangladesh blocks sites in anti-porn crusade’](#), *DW* (2019).
- 72 [‘Bangladesh’s moral police turn the screw’](#), *UCA News* (2019).
- 73 [‘Govt unblock Tiktok, Somewhereinblog’](#) *The Business Standard* (2019).
- 74 Similar strategy has been adopted elsewhere around the world. On more than one occasion, the Zimbabwean government, for example, attributed an internet or social media blackout to technical problems, sabotage, or third-party involvement, removing themselves from responsibility for the block.
- 75 On 23 July 2023, the Information and Technology Affairs Secretary of the Bangladesh Nationalist Party issued a [statement](#) protesting the internet shutdown during

rallies. See also [‘Mobile internet to slow down in Golapbagh’](#), *The Daily Star* (2022); [‘Mobile internet ‘slows down’ in Cumilla’](#) *The Daily Star* (2022); [‘Mobile internet services slowed down in Khulna amid BNP rally’](#), *New Age Bangladesh* (2022); [‘Mobile internet slowed amid BNP rally in Sylhet’](#), *Prothom Alo* (2022); [‘Why internet speed slows down during BNP rallies’](#), *Prothom Alo* (2022).

76 See (n 76).

77 [‘Bangladesh: Deadly Attacks on Hindu Festival’](#), *Human Rights Watch* (2021).

78 [‘Facebook says services restricted in Bangladesh’](#), *Prothom Alo* (2021); [‘Freedom on the Net 2022: Bangladesh’](#), *Freedom House* (2022).

79 [‘Facebook, Messenger still down in Bangladesh’](#), *The Business Standard* (2021); [‘Mobile users across Bangladesh hit by high-speed internet blackout’](#), *bdnews24* (2021).

80 [‘BTRC blocks Skype’](#) *The Daily Star* (2018); [‘BTRC unblocks Skype’](#), *The Daily Star* (2018).

81 [‘Skype ‘blocked’ across country’](#), *Prothom Alo* (2018).

82 [‘facebook blocked’](#), *The Daily Star* (2010).

83 [‘Sudden shutdown follows verdict’](#), *The Daily Star* (2015).

84 [‘The irony of restricting access to internet in “Digital Bangladesh”’](#), *The Daily Star* (2017); [‘Govt may keep FB inaccessible for 6hrs from midnight’](#), *Prothom Alo* (2017).

85 [‘Facebook might be blocked again for saving the state: Jabbar’](#), *The Daily Star* (2018).

86 [‘Amendment To Telecom Act: Govt set to clip BTRC wings’](#), *The Daily Star* (2021).

87 [‘Freedom on the Net 2022: Bangladesh’](#), *Freedom House* (2022).

88 [‘Blocking The Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa’](#) *International Journal of Communication* (2018).

89 A/HRC/50/55 (n 4) [24]; [‘Bangladesh and the U.S.: Internet shutdowns are the wrong response to national security threats’](#), *Access Now* (2023)

90 [‘Indian news website Scroll forced off-line over article on Bangladesh prime minister adviser, Gowher Rizvi’](#), *Medium* (2021).

91 [‘Bangladesh Govt Acknowledges Blocking BenarNews Websites’](#), *Benar News* (2020); Saad Hammadi, [‘World Press Freedom Day: COVID-19 must not be a pathogen of repression’](#), *Amnesty International* (2020).

92 [‘Bangladesh blocks news website accusing minister of corruption’](#), *Al Jazeera* (2020); [‘A wrist of luxury’](#), *Netra News* (2019).

93 [‘Bangladesh blocks access to Al Jazeera news website’](#), *Al Jazeera* (2019); [‘Bangladesh top security adviser accused of abductions’](#), *Al Jazeera* (2019).

94 [‘Bangladesh Government Blocks The Wire’](#), *The Wire* (2017); [‘Bangladesh Academic Mubashar Hasan “Held by Military Intelligence Agency”’](#), *The Wire* (2017).

95 [‘Bangladesh orders 191 ‘anti-State’ news sites blocked’](#), *The Hindu* (2023).

96 [‘Freedom is met with rigorous governmental control and violent attacks by people having impunity’](#), *Asian Human Rights Commission* (2020).

97 [‘Bangladesh government blocks news website in fresh blow to media’](#), *Digital Journal* (2019); [‘Bangladesh blocks news websites in press freedom gag’](#), *Al Jazeera* (2019)

98 [‘Mandates of the Special Rapporteur in the field of cultural rights; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the situation of human rights defenders; the Special Rapporteur on the human rights of internally displaced persons; the Special Rapporteur on minority issues and the Special Rapporteur on freedom of religion or belief’](#) (2018); [‘RSF decries blocking of 54 Bangladeshi news sites before election’](#), *Reporters Without Borders* (2019).

99 [‘Murder’ it was’](#), *The Daily Star* (2018); [‘Star blocked, unblocked’](#), *The Daily Star* (2018).

100 [‘Bangladesh Shuts Down the Internet, Then Orders Blocking of 35 News Websites’](#), *Global Voices* (2016).

101 [‘Bangladesh’](#), *Reporters without Borders*. 3

102 [‘Internet Subscriber’](#), *Bangladesh Telecommunication Regulatory Commission*.

103 A/HRC/50/55 (n 4) [48].

104 [Bangladesh Telecommunication Regulation Act, 2001](#), s 67 (‘2001 Act’).

105 *Ibid* s 73.

106 *Ibid* s 76.

107 A/HRC/50/55 (n 4) [7].

108 [‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue’](#), *Human Rights Council* (A/HRC/17/27, 2011) 19 (A/HRC/17/27).

109 [‘Joint Declaration on Universality and the Right to Freedom of Expression’](#), *United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights Special Rapporteur on Freedom of Expression and Access to Information* (2014) (‘2014 Joint Declaration’).

110 [‘A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee’s Monitoring of ICCPR Rights’](#), *Cambridge University Press* (2020) 538 (Taylor’s Commentary on ICCPR).

111 A/HRC/50/55 (n 4) [9].

112 [‘Human Rights and the 2030 Agenda: Empowering people and ensuring inclusiveness and equality’](#), *European Union Agency for Fundamental Rights* (2019).

113 A/HRC/17/27 (n 120) [23], [26], [29], [67].

114 [‘Kashmir’s Internet Siege an ongoing assault on digital rights’](#), *Jammu Kashmir Coalition of Civil Society* (2020); [‘Of Blackouts and Bandhs: The Strategy and Structure](#)

Internet Shutdowns in Bangladesh:

[of-Dist-0nected-Protest-in-India](#); *Stanford Global Digital Policy Incubator* (2019) (Jan Rydzak Report 2’).

- 115 For example, see [‘38/7. The promotion, protection and enjoyment of human rights on the Internet’](#), *Human Rights Council* (A/HRC/RES/38/7, 2018) (A/HRC/RES/38/7); [‘26/13 The promotion, protection and enjoyment of human rights on the Internet’](#), *Human Rights Council* (A/HRC/RES/26/13, 2014); [‘28/16. The right to privacy in the digital age’](#), *Human Rights Council* (A/HRC/RES/28/16, 2015); [‘20/8. The promotion, protection and enjoyment of human rights on the Internet’](#), *Human Rights Council* (A/HRC/RES/20/8, 2012).
- 116 [‘12/16. Freedom of opinion and expression’](#), *Human Rights Council* (A/HRC/RES/12/16, 2009) [5(p)].
- 117 [‘32/13. The promotion, protection and enjoyment of human rights on the Internet’](#), *Human Rights Council* (A/HRC/RES/32/13, 10). Subsequently, the HRC reiterated its condemnation in 2018, 2020 and 2021. In 2020, the HRC denounced internet shutdowns and called upon states to “refrain from imposing restrictions that are inconsistent with article 19 of the International Covenant on Civil and Political Rights, including on the free flow of information and ideas, including through practices such as the use of Internet shutdowns to intentionally and arbitrarily prevent or disrupt access to or the dissemination of information online, the banning or closing of publications or other media and the abuse of administrative measures and censorship, and on access to or use of information and communications technology, inter alia radio, television and the Internet.” See A/HRC/RES/38/7 (n 127); [‘44/12. Freedom of opinion and expression’](#), *Human Rights Council* (A/HRC/RES/44/12, 2020); [‘47/16. The promotion, protection and enjoyment of human rights on the Internet’](#), *Human Rights Council* (A/HRC/RES/47/16, 2021).
- 118 A/HRC/RES/38/7 (n 127) [13].
- 119 [‘Joint Declarations of the representatives of intergovernmental bodies to protect free media and expression’](#), *OSCE Representative on Freedom of the Media* (2013) 66.
- 120 [‘International Mechanisms for Promoting Freedom of Expression: Joint Declaration on Freedom of Expression and the Internet’](#), *United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights Special Rapporteur on Freedom of Expression and Access to Information* (2011) (2011 Joint Declaration’).
- 121 Ibid; 2014 Joint Declaration (n 121).
- 122 2011 Joint Declaration (n 132).
- 123 [‘Joint Declaration on Freedom of Expression and responses to conflict situations’](#), *United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights Special Rapporteur on Freedom of Expression and Access to Information* (2015).
- 124 [‘Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade’](#), *United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights Special Rapporteur on Freedom of Expression and Access to Information* (2019).
- 125 [‘Joint Declaration on Media Freedom and Democracy’](#), *United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights Special Rapporteur on Freedom of Expression and Access to Information* (2023).
- 126 [‘Joint Statement by the Freedom Online Coalition’](#), *Ambassador Michèle Taylor* (2023).
- 127 [‘World Press Freedom Day’](#), *U.S. Department of State* (2021).
- 128 [‘Internet Shutdowns’](#), *United Nation Human Rights Office of High Commissioner* (2022).
- 129 [‘2021 Open Societies Statement’](#) G7 (2021); [‘G7 Accommodates Indian Stand on Internet Curbs’](#), *The Hindu* (2021).
- 130 [‘Commonwealth Cyber Declaration’](#), *The Commonwealth* (2018).
- 131 [‘Declaration of Principles on Freedom of Expression and Access to Information in Africa’](#), *African Commission on Human and Peoples’ Rights* (2019).
- 132 [‘Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa’](#), *African Commission on Human and Peoples’ Rights* (2019).
- 133 [‘362: Resolution on the Right to Freedom of Information and Expression on the Internet in Africa’](#), *African Commission on Human and Peoples’ Rights* (ACHPR/Res.362(LIX), 2016).
- 134 [‘70/1. Transforming our world: the 2030 Agenda for Sustainable Development’](#), *United Nations General Assembly* (A/RES/70/1, 2015).
- 135 [‘Declaration on freedom of communication on the Internet’](#), *Council of Europe* (2003).
- 136 [‘FOC Joint Statement on State Sponsored Network Disruptions’](#), *Freedom Online Coalition* (2017).
- 137 [‘FOC Joint Statement on COVID-19 and Internet Freedom’](#), *Freedom Online Coalition* (2020).
- 138 Furthermore, the *Universal Declaration of Human Rights* similarly provides the right “to seek, receive, and impart information and ideas through any media and regardless of frontier.” At the regional level, the right to freedom of expression is also enshrined in the *European Convention on Human Rights*, and the *American Convention on Human Rights*, the *African Charter on the Arab Charter on Human Rights*, and the *ASEAN Human Rights Declaration*.
- 139 [‘General comment No. 34’](#), *Human Rights Committee* [11], [46] (‘GC 34’); A/HRC/17/27 (n 120) [37].
- 140 Taylor’s Commentary on ICCPR (n 122) 544.
- 141 [‘International Covenant on Civil and Political Rights’](#), *United Nations General Assembly* (UNTS 999, 171, 1966) art 2 (‘ICCPR’).
- 142 Ibid art 5.
- 143 GC 34 (n 151) [43].
- 144 A/HRC/17/27 (n 120) [24].
- 145 GC 34 (n 151) [25].
- 146 A/HRC/50/55 (n 4) [11].
- 147 [‘The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights’](#), (E/CN.4/1985/4, 1984), principle I.A.5 (‘Siracusa Principles’).
- 148 GC 34 (n 151) [26].
- 149 Siracusa Principles (n 159) principle I.A.3.
- 150 GC 34 (n 151) [30].
- 151 Siracusa Principles (n 159) principle I.B.18.
- 152 A/HRC/50/55 (n 4) [13], [31].
- 153 Ibid.
- 154 GC 34 (n 151) 34.
- 155 2011 Joint Declaration (n 132).

- 156 [‘Freedom of Expression on the Internet’](#), *Organization for Security and Co-operation in Europe* (2012) 39.
- 157 A/HRC/17/27 (n 120) [78]-[79].
- 158 GC 34 (n 151) [43].
- 159 [‘The rule of law on the Internet and in the wider digital world’](#), *Council of Europe Commissioner for Human Rights* (2014) 66 (‘Council of Europe 2014 Issue Paper’).
- 160 A/HRC/50/55 (n 4) [13].
- 161 *Ibid.*
- 162 A/HRC/17/27 (n 120) [24].
- 163 [‘General comment No. 37 \(2020\) on the right of peaceful assembly \(article 21\)’](#), *Human Rights Committee* [42].
- 164 A/HRC/50/55 (n 4) para 12.
- 165 [‘Advancing Strategic Litigation on Internet Shutdowns cases in Africa: Promises and Pitfalls’](#) *Collaboration on International ICT Policy for East and Southern Africa*.
- 166 *Anuradha Bhasin v. Union of India* AIR 2020 SC 1308, [23], [25] (‘*Anuradha Bhasin* case’). Separately, in an unrelated case decided by the Kerala High Court in 2019, the court held that “when the [HRC] have found that right to access to internet is a fundamental freedom and a tool to ensue right to education, a rule or instruction which impairs the said right of the students cannot be permitted to stand in the eye of law.” See [Fahmeema Shirin v. State of Kerala and Others](#) WP (C) No. 19716 of 2019 (L).
- 167 *Anuradha Bhasin* case (n 178) [26]-[28], [152].
- 168 *Ibid* [99].
- 169 *Ibid* [118].
- 170 2023 HRW India Article (n 29); [‘4G restoration in J&K: 3 Must Reads’](#), *Supreme Court Observer* (2020).
- 171 [‘Restoration of internet services in Jammu and Kashmir: A timeline’](#), *The Indian Express* (2021).
- 172 [Cengiz v. Turkey](#) [2015] Eur Court HR, [7], [8], [65]-[67].
- 173 *Ibid* [51]-[52].
- 174 *Ibid* [63].
- 175 *Ibid* [65]-[66].
- 176 [Ahmet Yildirim v. Turkey](#) [2012] Eur Court HR [8]-[11], [69]-[70].
- 177 *Ibid* [43], [51].
- 178 *Ibid* [62], [67]-[70].
- 179 [Vladimir Kharitonov v. Russia](#) [2020] Eur Court HR [4]-[6], [35], [46]-[47].
- 180 *Ibid* [30].
- 181 *Ibid* [38]-[40].
- 182 *Ibid* 46-47.
- 183 [Amnesty International Togo v. The Togolese Republic](#) ECW/CCJJ/JUD/09/20 [2]-[4], [8], [19], [47].
- 184 *Ibid* [38].
- 185 *Ibid* [43], [45].
- 186 *Ibid* [47].
- 187 *Badiul Alam Majumdar v. Information Commission* 69 DLR (2017) 100 (‘*Badiul Alam* case’)
- 188 [Right to Information Act, 2009](#), sec 8 (‘2009 Act’).
- 189 *Ibid* s 9; *Badiul Alam* case (n 199).
- 190 [Evidence Act, 1872](#), s 74(2)
- 191 *Badiul Alam* case (n 199).
- 192 2009 Act (n 200) s 24, 25, 27.
- 193 *Ibid* s 6.
- 194 *Ibid* s 7.
- 195 *Ibid* s 32.
- 196 In *Engineer Mahmudul-ul Islam v. Bangladesh* 2003 23 BLD 80, the High Court Division defined “public interest litigation” as “a legal action initiated in a court for the enforcement of rights and interest of the citizens in general or a section thereof” (‘*Engineer Mahmudul-ul Islam* case’)
- 197 [Constitution of the People’s Republic of Bangladesh](#), art 102(1) (‘Constitution’).
- 198 *Ibid* arts 102(2)(a)(i), 102(2)(a)(iii).
- 199 *Abdul Hakim v. Bangladesh* [2015] 67 DLR 83, [11]-[34].
- 200 *Afzalul Abedin v. Bangladesh* 8 (2003) BLC (HCD) [16].

- 201 *Constitution* (n 209) art 7(2). Notably, in *Abdul Mannan Khan v. Government of Bangladesh* 64 DLR (AD) (2012) 169, the apex court observed that all government organs and institutions, and their powers, owe their origin to the Constitution. Thus, a state agency can only enjoy such powers conferred upon them and must function within limits demarcated by the Constitution, with its actions subject to judicial scrutiny. No power can be claimed by any functionary which is not to be found within the four corners of the Constitution, nor can anyone transgress the specified limits.
- 202 *Engineer Mahmudul-ul Islam* case (n 208).
- 203 'Constitutional Law of Bangladesh', *Mullick Brothers* (2012) 607 ('Mahmudul Islam on Constitution'); *Children's Charity Bangladesh Foundation v. Bangladesh* [2017] 5 CLR (HCD) 278, [76].
- 204 *Dr. Mohiuddin Farooque v. Bangladesh* [2001] 53 DLR 125 [32].
- 205 *Constitution* (n 209) art 7(2), 26.
- 206 *Ibid* art 44; *Bangladesh v. Ahmed Nazir* [1975] 27 DLR (AD) 41 [36].
- 207 2001 Act (n 116) s 30.
- 208 *Dr. Mohiuddin Farooque v. Bangladesh* 49 DLR (AD) 1, 48. Similar views were expressed by Bimalendu Bikash Roy Chowdhury J., observing that "... if socially conscious and public-spirited persons are not allowed to approach the court on behalf of the public or a section thereof for the enforcement of their rights, the very scheme of the Constitution will be frustrated. The inescapable conclusion, therefore, is that the expression "person aggrieved" means not only any person who is personally aggrieved but also one whose heart bleeds for his less fortunate fellow beings for a wrong done by the Government or a local authority in not fulfilling its constitutional or statutory obligation." However, the filing of such lawsuits necessitates compliance with the guidelines set forth in *National Board of Revenue vs Abu Saeed Khan* 18 BLC (AD) 2013 116.
- 209 'Fundamental Rights in Search of Constitutional Remedies: The Emergence of Public Law Compensation in Bangladesh' *Australian Journal of Asian Law* (2020) 27, 29.
- 210 *Bangladesh National Women Lawyers Association vs. Bangladesh* [2009] 29 BLD 415; *Bangladesh National Women Lawyers Association vs. Bangladesh* [2011] 31 BLD 324.
- 211 *City Sugar Industries Ltd. v. Human Rights and Peace for Bangladesh* [2010] 62 DLR (AD) 428.
- 212 *Human Rights and Peace for Bangladesh vs. Bangladesh* [2019] (unreported).
- 213 See 'Internet Impact Brief Bangladesh: Regulation for Digital, Social Media and OTT Platforms, 2021', *Internet Society* (2022); 'Letter to the Bangladesh Telecommunication Regulatory Commission: withdraw the Regulation for Digital, Social Media, and OTT Platforms', *Access Now* (2023).
- 214 Mahmudul Islam on Constitution (n 215) 330-332, 341. See also *Bangladesh National Curriculum and Text-Book Board v. A.M. Shamsuddin* 48 DLR (AD) 184, at [52] and [58], where the apex court observed that inherent in the right to free speech is the right to propagate, publish, disseminate and circulate ideas, to any class and number of people.
- 215 *Md. Riaz Uddin Khan v. Mahmudur Rahman* 2011 (19) BLT (AD) 54.
- 216 *State v. Manabjamin* 57 DLR (2005) 359 ('Manabjamin case').
- 217 Mahmudul Islam on Constitution (n 215) 333.
- 218 *Ibid* 334.
- 219 *Ibid* 332, 334.
- 220 *Ibid* 329; *Abul Kalam Azad v. David Bergman* 5 CLR (2017) (HCD).
- 221 *Manabjamin* case (n 228) [58].
- 222 *Constitution* (n 209) art 39(2).
- 223 Mahmudul Islam on Constitution (n 215) 335.
- 224 *Ibid* 353.
- 225 *Ibid* 335.
- 226 A/HRC/50/55 (n 4) para 21.
- 227 See also *M Anwar Hossain v. Bangladesh* 1989 18 CLC (AD).
- 228 *Bangladesh v. Bangladesh Legal Aid and Services Trust* 69 DLR (AD) (2017) 63 ('BLAST case').
- 229 Mahmudul Islam on Constitution (n 215) 353
- 230 *BLAST* case (n 240).
- 231 *Constitution* (n 209) art 7(2).
- 232 *BLAST* case (n 240).
- 233 *Dr. Nilima Ibrahim v. Bangladesh* 32 DLR 203, [30]; *Afzalul Abedin v. Government of Bangladesh* (10) BLT (HCD) 490, [275]-[276] ('Afzalul Abedin case').
- 234 *Bangladesh National Curriculum and Text-Book Board v. A.M. Shamsuddin* 48 DLR (AD) 184, [61]; 'Interpretation of Statutes and Document', *Mullick Brothers* (2009) 39 ('Mahmudul Islam on Interpretation').
- 235 Mahmudul Islam on Interpretation (n 246) 123,124, 135.
- 236 *Constitution* (n 209) art 8(2).
- 237 *Ibid* art 11. On issue of invalidating a constitutional amendment, the court ruled in *Anwar Hossain Chowdhury v. Bangladesh* 41 DLR (AD) 165 that its "only function is to examine dispassionately the terms of the Constitution and the law ... [as neither] politics, nor policy of the government nor personalities have any relevance for examining the power of the parliament under the Constitution which has to be done purely upon an interpretation of the provisions of the Constitution with the help of legal tools." Additionally, in *Abdul Mannan Khan v. Government of Bangladesh* 64 DLR (AD) (2012) 169, the apex court alluded that a statute conflicting the basic feature or spirit of the Constitution and its convention can be declared unconstitutional.

- 238 Mahmudul Islam on Interpretation (n 246) 41.
- 239 *Afzalul Abedin* case (n 245) [50].
- 240 Ibid [62], [78].
- 241 Ibid [50].
- 242 *Dr. Nurul Islam v. Bangladesh* 1981 1 BLD (AD) 140, [86], [87].
- 243 In the unreported case of *Human Rights and Peace for Bangladesh v. Bangladesh*, at [4] and [45], in highlighting that the *Contempt of Court Act, 2013* and section 32ka of the *Anti-Corruption Commission (Amendment) Act, 2013* were declared as unconstitutional and void for its inherently discriminatory nature, the apex court also declared unconstitutional and voided section 41(1) of the *Government Services Act, 2018*.
- 244 *Anuradha Bhasin* case (n 178) [83].
- 245 ‘[Suspension of Telecom Services / Internet and its Impact](#)’, *Standing Committee on Communications and Information Technology* (2021) 36 (‘2021 Standing Committee Report on Internet Shutdown’).
- 246 *Anuradha Bhasin* case (n 178) [82].
- 247 2021 Standing Committee Report on Internet Shutdown (257) 32.
- 248 *Anuradha Bhasin* case (n 178) [109], [111].
- 249 Ibid [118].
- 250 2001 Act (n 116) ss 30, 31, 98, 99.
- 251 Ibid s 87.
- 252 ‘[Bangladesh](#)’, *Freedom House* (2023).
- 253 ‘[Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?](#)’, *Carnegie Endowment for International Peace* (2022).
- 254 *Constitution of the International Telecommunication Union*, art 34(2).
- 255 *Aftab Hossain v. Ministry of Home Affairs* 54 DLR (2002) 266 [12].
- 256 See generally *Khondaker Modarresh Elahi v. Government* 2001 21 BLD 352; Mahmudul Islam on Constitution (n 215) 340.
- 257 ‘[Mandates of the Special Rapporteur on extrajudicial, summary or arbitrary executions; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association; the Special Rapporteur on the situation of human rights defenders; the Special Rapporteur on the human rights of migrants; and the Special Rapporteur on minority issues](#)’.
- 258 ‘[Shutting Down the Internet to Shut Up Critics](#)’ (*Human Rights Watch*) <<https://www.hrw.org/world-report/2020/country-chapters/global-5>> accessed 09 November 2023
- 259 Mahmudul Islam on Constitution (n 215) 340.
- 260 Ibid 344.
- 261 ‘[Open letter: authorities and telecom providers in Bangladesh must maintain unhindered internet access for all](#)’, *Access Now* (2023).
- 262 ‘[Laughing in the Face of an Internet Shutdown In Bangladesh](#)’, *Global Voices* (2018); ‘[Internet slowdown to stop question paper leaks](#)’, *Prothom Alo* (2018); ‘[BTRC reverses internet outage plan to fight SSC question leaks](#)’, *bdnews24* (2018).
- 263 ‘[Health minister for slowing down internet before MBBS admission test](#)’, *The Business Standard* (2023).
- 264 Internet shutdowns during examinations is practised in several jurisdictions. For instance, in India, shutdown orders to prevent cheating during examination have been successfully challenged over the years. In 2022, an order issued by the State Government of West Bengal was challenged before the Calcutta High Court, and the vagueness and absence of clearly reasoned grounds in the suspension order, the lack of authority of law, and disproportionality of the action, resulted in its dismissal. See ‘[Internet Shutdowns to Prevent Cheating During Exams is a Disproportionate Measure](#)’, *Internet Society Pulse* (2022); ‘[SC notice to Centre on plea against Internet shutdowns to prevent cheating during exams](#)’, *The Indian Express* (2022). Iraq also famously turns off the internet for three hours every year to curtail cheating in the country-wide high school exit exams. See ‘[Iraq shuts down the internet to stop pupils cheating in exams](#)’, *The Guardian* (2016). Disruptions have been used during professional and secondary-school exams in Algeria, Ethiopia, Syria, and Uzbekistan. See Jan Rydzak Report 1 (n 7).
- 265 ‘[Mobile internet services suspended in New Market area](#)’, *The Business Standard* (2022).
- 266 ‘[YouTube blocked in Bangladesh](#)’, *The Daily Star* (2012); ‘[Bangladesh lifts ban on YouTube, blocked after anti-Islam film](#)’, *Reuters* (2013).
- 267 ‘[Bangladesh shuts down mobile internet in lead up to election day](#)’, *Al Jazeera* (2018).
- 268 2021 Wired Report (n 5).
- 269 US 2022 Human Rights Report (n 110) 30.
- 270 ‘[\(Dis\)information Blackouts: Politics and Practices of Internet Shutdowns](#)’, *International Journal of Communication* (2021).
- 271 Jan Rydzak Report 2 (n 126).
- 272 2021 Standing Committee Report on Internet Shutdown (257) 18.
- 273 Jan Rydzak Report 1 (n 7).
- 274 ‘[Research Shows Internet Shutdowns and State Violence Go Hand in Hand in Syria](#)’, *Electronic Frontier Foundation* (2015); ‘[A Web of Impunity: The killings Iran’s internet shutdown hid](#)’, *Amnesty International* (2021). It is worth noting that studies have confirmed that a concentration of internet disruptions in the Syrian civil war was observed immediately prior to and during military offensives carried out by the Syrian army between 2011 and 2013. Occasionally presented by the government as technical outages or cable cuts, these incidents coincide with an increased number of killings attributed to government forces. Similarly in Nauru, a temporary ban on Facebook and other online services in 2015 raised concern among human rights advocates that the measure was used to conceal human rights abuses and deplorable living conditions in the island’s detention centres

for asylum-seekers attempting to reach Australia.

- 275 [‘Freedom of Expression on the Internet’](#), *Organization for Security and Co-operation in Europe* (2012) 39.
- 276 *Durnity Daman Commission v. G.B. Hossain* 74 DLR (AD) (2022) [1], [17] (*G.B. Hossain case*).
- 277 Mahmudul Islam on Constitution (n 215) 353.
- 278 *Salauddin v. Bangladesh* 2018 14 ALR (HCD) [1], [155], [158].
- 279 (1947) 1 KB 223; (1947) 2, All ER 680.
- 280 See *Abul Asad v. Secretary, Ministry of Education* 72 DLR (2020) 195; *Fatema Enterprise v. Bangladesh* 8 SCOB (2016) HCD 59; *Jamal Uddin Sikder v. Government of Bangladesh* 21 BLC (2016) 162; *Soya-Protein Ltd v. Secretary Ministry of Disaster Management and Relief* 22 BLD 378.
- 281 *G.B. Hossain case* (n 288) [1], [19].
- 282 *Ibid.* See also Mahmudul Islam on Constitution (n 215) 353.
- 283 Mahmudul Islam on Interpretation (n 246) 136.
- 284 *R v. Goldsmith* [1983] 1 WLR 151, 155.
- 285 *Anuradha Bhasin case* (n 178) [33]-[34].
- 286 *Ibid* [60].
- 287 *Ibid* [99].
- 288 *Ibid* [71], [72].
- 289 *Ibid* [36].
- 290 Mahmudul Islam on Constitution (n 215) 359-360.
- 291 Council of Europe 2014 Issue Paper (n 171) 68.
- 292 [‘COVID-19: Governments must promote and protect access to and free flow of information during pandemic – International experts’](#), *United Nations* (2020).
- 293 [‘Bangladesh: Internet Ban Risks Rohingya Lives’](#), *Human Rights Watch* (2020).
- 294 [‘Network shutdowns in Rohingya camps: how they’re damaging the fragile information ecosystem of refugees from Myanmar’](#), *Access Now* (2023).
- 295 See [‘Internet Subscriber’](#), *Bangladesh Telecommunication Regulatory Commission*.
- 296 See [‘Internet Shutdowns and the Limits of Law’](#), *International Journal of Communication* (2020).
- 297 [‘Joint letter on keeping the internet open and secure during the election in Bangladesh’](#) *Access Now* (2018).
- 298 In 2020, the Four Special Rapporteurs on Freedom of Expression recognised the positive potential of digital technologies and accessible internet in ensuring free and fair elections, for instance, by providing voters with access to information, enabling them to express their opinions, facilitating direct interaction with candidates, and empowering candidates and parties, particularly those with limited resources, to disseminate their messages and mobilise support inexpensively. It was also recommended that states should prioritise the promotion of effective internet access and other digital technologies for all segments of the population, and specifically ensure that there is no prior censorship of the media, including through means such as the administrative blocking of media websites or internet shutdowns. See [‘Joint Declaration on Freedom of Expression and Elections in the Digital Age’](#), *United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, and the Organization of American States Special Rapporteur on Freedom of Expression* (2020).
- 299 [‘Policy Brief: Internet Shutdowns’](#), *Internet Society* (2019).
- 300 [‘How ‘Internet Express’ is helping Kashmiris go online’](#), *Al Jazeera* (2020).
- 301 [‘The economic impact of disruptions to Internet connectivity: A report for Facebook’](#), *Deloitte* (2017).
- 302 *Ibid.*
- 303 [‘Internet shutdowns cost countries \\$2.4 billion last year’](#) *Center for Technology Innovation at Brookings* (2016); [‘The economic impact of disruptions to Internet connectivity: A report for Facebook’](#), *Deloitte* (2017).
- 304 [‘Government Internet Shutdowns Have Cost \\$50 Billion Since 2019’](#), *Top10VPN* (2023).
- 305 [‘Myanmar Economic Monitor Contending with Constraints’](#), *The World Bank* (2022).
- 306 A/HRC/50/55 (n 4) para 33.
- 307 [‘Indian Kashmir sees more than \\$2.4 billion losses since lockdown: group’](#), *Reuters* (2019); [‘Asia’s Internet Shutdowns Threaten the Right to Digital Access’](#), *Chatham House* (2020); [‘Sudan’s military has shut down the internet to crush a popular revolt. Here’s how it could backfire’](#), *The Washington Post* (2019).
- 308 See [‘NETBLOCKS: MAPPING INTERNET FREEDOM’](#): According to their website, all estimates are based on indicators from the World Bank, International Telecommunication Union, Eurostat and US Census, and assessed based on development indicators used by the Brookings Institution. It estimates the economic impact of a single hypothetical internet disruption of the specified type, location and duration, primarily modelling internet shutdowns and outages which impact entire populations typically lasting on the order of a few hours or days. Economic indicators for 2020 have been applied.
- 309 Marchant and Stremlau Report (n 9) 9.
- 310 See *Mark Builders Limited v. The Commissioner of Taxes* 59 DLR (2007) 463; *Proshika Manobik Unnayan Kendro v. The Commissioner of Taxes* 2019 (27) BLT (HCD) 185.
- 311 *BLAST case* (n 240) [73], [84], [89]; *G.B. Hossain case* (n 288) [15], where the apex court held that “[t]he executive instructions without having the sanction of any statutory power cannot be construed as law.”
- 312 *Engineer Mahmudul-ul Islam case* (n 208).
- 313 In *Md. Delwar Hossain v. Bangladesh* 2016 (24) BLT(HCD) 226, [23], an executive order cancelling a permission of a newspaper on grounds that it used different

addresses in the printing line of the newspaper and published the newspaper irregularly was declared as unconstitutional as the reasons mentioned in the order was “vague, imaginary, indefinite and inadequate and highly discriminatory” and it violated the rules of natural justice. See also *Abdul Quddus Khan Salafi v. The State*, a case relating to the banning of a known terrorist organization under the anti-terrorism law, where the High Court Division observed that “[i]t is also necessary to point out here that freedom of assembly, right to association and freedom of thought and speech are inviolable fundamental rights guaranteed under articles 37-39 of the Constitution. So, any order restricting the above rights must be well reasoned and supported by law enacted within the constitutional scheme.”

- 314 2001 Act (n 116) ss 30, 31, 98, 99.
- 315 [‘Internet throttling in Bangladesh: government, telcos must #KeepItOn’, Access Now \(2022\).](#)
- 316 [‘Bangladesh and the U.S.: Internet shutdowns are the wrong response to national security threats’, Access Now \(2023\).](#)
- 317 Ibid.
- 318 *Anuradha Bhasin* case (n 178) [14], [15], [17].
- 319 Ibid [96].
- 320 Ibid [17]-[18].
- 321 Mahmudul Islam on Interpretation (n 246) 68-70.
- 322 *Bangladesh v. Abdul Quader Molla* 8 LM (AD) 2020 375 (*‘Abdul Quader Molla case’*)
- 323 Ibid [611].
- 324 Ibid [643].
- 325 Ibid [646], [662].
- 326 Ibid [677]-[678]. See also *Constitution* (n 209) art 25; *Professor Nurul Islam v. Bangladesh* 2000 20 BLD 377, which states in [8] “Article 25(1) of our Constitution casts on obligation upon [the state to respect international law] and the principles enunciated in the United Nations Charter ...” and the judiciary, as one of the organs of the state, cannot escape this obligation.
- 327 Ibid [763]-[764].
- 328 *Md Salauddin Dolon v. Bangladesh* [2011] 63 DLR 80, [22]/
- 329 *Abdul Quader Molla* case (n 334) [195].
- 330 *Hussain Mohammad Ershad v. Bangladesh* [2001] 21 BLD (AD) 69 [2].
- 331 2001 Act (n 116) ss 30, 31, 98, 99.
- 332 Ibid s 87.
- 333 According to the [Article 31A\(1\) of the Rules of Business](#), where “the [Government of Bangladesh] decides to pre-publish draft proposal for making or amending any rule or regulation, such rule or regulation shall be published in the official Gazette as well as website of the concerned Ministry or Division with notice specifying at least three weeks’ time for seeking public opinion. The [concerned Ministry or Division] shall send a notice regarding the pre-publication of the rule or regulation in their website along with the website address to at least three daily newspapers to print.” Opinion received from public consultation is mandatorily required to be taken into consideration.
- 334 [‘Guiding Principles on Business and Human Rights’ United Nations Human Rights office of the High Commissioner.](#)
- 335 [‘Legal Guidance on Internet Restrictions and Shutdowns in Africa’, International Commission of Jurists \(2022\).](#)
- 336 [‘30 governments step it up to denounce internet shutdowns at RightsCon Brussels’, Access Now \(2023\).](#)
- 337 For the methodology used in scoring and categorisation, see [‘Freedom on the Net Research Methodology’, Freedom House \(2023\).](#)
- 338 For the methodology used in ranking, see [‘Methodology used for compiling the World Press Freedom Index 2023: From 2022 onwards’, Reporters Without Border \(2022\).](#) Other methodologies may have been used for earlier years.

opt 
 ima 