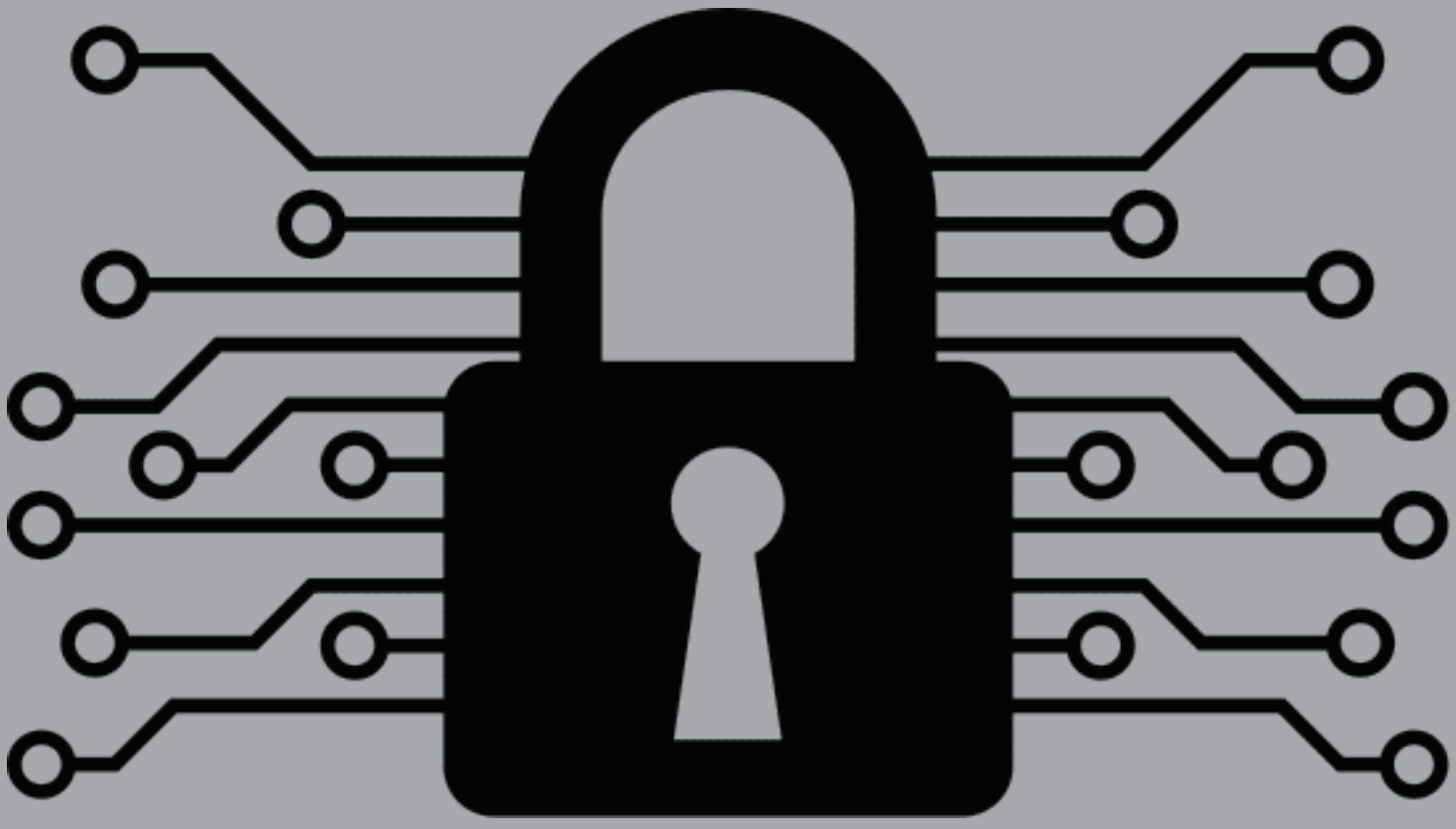
VOICE
VOICES FOR INTERACTIVE CHOICE & EMPOWERMENT

www.voicebd.org

A REVIEW OF

LEGAL INSTRUMENTS ON FREEDOM OF EXPRESSION IN BANGLADESH

FOCUSING ON DIGITAL SECURITY ACT



Review of

LEGAL INSTRUMENTS ON FREEDOM OF EXPRESSION IN BANGLADESH

Focusing on Digital Security Act

House 67, Block-Ka, Pisciculture Housing Society, Shyamoli, Dhaka-1207
info@voicebd.org; www.voicebd.org, +88-02-58150588

Review of

LEGAL INSTRUMENTS ON FREEDOM OF EXPRESSION IN BANGLADESH

Focusing on Digital Security Act

PUBLISHED BY VOICES FOR INTERACTIVE CHOICE AND EMPOWERMENT

HOUSE 67, BLOCK-KA, PISCICULTURE HOUSING SOCIETY, SHYAMOLI, DHAKA-1207
INFO@VOICEBD.ORG; WWW.VOICEBD.ORG, +88-02-58150588

PUBLISHED DECEMBER 2020

COVER & DESIGN ZAYED SIDDIKI

FOREWORD

The right to freedom of expression is one of the universal human rights that must be upheld and protected in a democratic state. And, in the present-day Bangladesh, digitally connected spaces including internet is one of the most widespread and commonly used tools for expression. It is very important that in digitally connected spaces and through the internet, people have the freedom to opine on any topics and to receive and impart ideas and information on any matters without interference by the authorities. So, similar to non-digital public spaces, internet, and online spaces must be free from restrictive laws and policies.

To this end, it's imperative that the civil society organize forums and creates public-spaces for comprehensive and methodical appraisal of internet and ICT related laws. Individuals and nongovernment organizations involved in information technology for development related activities, journalists and online activists will be directly benefitted from such efforts; they will have a comprehensive understanding of the legal policy in this regard and will be better equipped to face challenges.

In this report, we have tried to put together such an instrument for everyone involved in the quest of free and open online spaces in Bangladesh. We have prepared this appraisal of the Bangladeshi laws related to information and communication technologies and freedom of expression based on standard scientific research methodologies.

After the latest piece of legislation related to ICT and freedom of expression— the Digital Security Act was promulgated in 2018, VOICE started to assess new legal and de-facto landscape of online expression and legal protection in Bangladesh. For the assessment study, we have used standard methods of systematic qualitative study adapted from recent practices in human rights-related legal policy analysis. Based on the framework, we've reviewed provisions ICT related laws and analyzed how those provisions affect online freedom of expression.

This assessment recommends how to further amend the Digital Security Act in alignment to the principles of freedom of expression. The assessment maintains an objective and non-partisan stand and employs rigorous scientific research methodologies as to not compromise the authenticity of the work. We hope the struggle to ensure online freedom of expressions will be greatly benefitted from this assessment.

Ahmed Swapan Mahmud
Executive Director, VOICE

ACKNOWLEDGMENT

We have benefitted from valuable opinion and advice of eminent rights experts and practitioners, we are very grateful to them all. More particularly, we thank reviewers of this report for their time and efforts.

Again, we are very thankful to all participants, facilitators and speakers of dialogues, consultations and media workshops. We have sought their opinion on challenges and community-resilience related to freedom of expressions, digital rights, security and cyber peace in Bangladesh. Their valuable policy recommendations, technical opinion, and critic on the legal framework, internet infrastructure, and institutional practices helped us to deliver.

ACRONYMS

ASK:	Ain-o-Salish Kendra
BTRC:	Bangladesh Telecommunications Regulatory Commission
BDT:	Bangladesh Taka
CPC:	Civil Procedure Code
CRPC:	Code of Criminal Procedure
CT:	Cyber Tribunal
ECESCR:	International Convention on Economic, Social and Cultural Rights
GoB:	Government of Bangladesh
ICCPR:	International Convention on Civil and Political Rights
ICT:	Information and Communication Technology
IGF:	Internet Governance Forum
ITU:	International Telecommunication Union
MoPTIT:	The Ministry of Posts, Telecommunications and Information Technology
NGO:	Non-government Organization
SPA:	Special Powers Act
UDHR:	Universal Declaration of Human Rights
UPR:	Universal Period Review
UN:	United Nations
UNHRC:	United Nations Human Rights Council
VoIP:	Voice over Internet Protocol Services

TABLE OF CONTENTS

1. INTRODUCTION

The Internet is one of the most widespread and commonly used tools for expression. The unique characteristics of online spaces provide individuals with endless possibilities to deliver their ideas and opinions to anyone willing to listen across borders at relatively low cost, more so than has ever been the case before. Once seen through the lens of human rights discourse, online spaces are inevitable parts of the spaces where these universal rights to freedom of expressions must be protected.

Despite these challenges, Bangladeshi citizens try to use internet and online spaces as tool and platforms in exercising their rights to freedom of expression. Purpose of this study is to perform a comprehensive systematic review of the Information and Communication Technology Act, 2006, the Digital Security Act, 2018, and other related laws of Bangladesh. Non-government organizations involved in information technology for development related activities, journalists and online activists will be directly benefitted from this review and analysis. From the review and analysis of this law, they will have a comprehensive understanding of the legal policy in this regard.

1.1. Context

Expressing one's social, political and religious views in Bangladesh has become riskier than ever. Bloggers and online activists are being categorically targeted by both extremist groups as well as the law enforcement agencies. Physical attacks and killings of netizens have become the new norm. Since inception, the Information and Communication Technology Act 2006 has been riddled with sweeping controversies and criticism.

Enacted in 2006, and amended in 2013 and repealed some provisions in 2018 with the Digital Security Act, the ICTA is full of loopholes making it a perfect instrument to undermine online expression in Bangladesh. The law uses vague terminologies to criminalize publishing information online that 'hurts religious sentiment', 'creates possibility to deteriorate law and order,' or prejudices 'the image of the State'. The ICT Act has been routinely used to suppress freedom of speech and harass writers, activists, and journalists, often for their comments on social media and same is the case with the Digital Security Act, 2018. According to the Cyber Tribunal (CT) in Dhaka, around 700 cases have been filed under section 57 of the ICT Act between 2013 and early 2017. A total of 260 cases were filed till the first

week of June in 2017 alone. In 2018 the number of Journalist's harassment was 207 and in 2019 the number was 142.

Before its 2013 amendment, the maximum punishment for offences under the section was 10 years' imprisonment and a fine of BDT 10 million. Besides, police had to seek permission from the authorities concerned to file a case and arrest any person under the law. With the amendment, the maximum jail term was raised to 14 years. And law enforcers were empowered to make arrests without a warrant on charges of defamation. It is an accepted proposition that publication of any statement or writing with intent to create hatred towards the Government, its policies, activities and decisions and thereby instigating the people against the government is not permissible in law and a punishable offense. However, constructive criticism of the government policies with intent to demand betterment of social services is not punishable under any law of the country.

Writers, bloggers, journalists, newspapers, TV channels and social-media users of Bangladesh are directly affected by the adverse effects of the ICT Act. The situation has created a condition wherein media and journalists live in constant fear of sanction by the Government for labeling anything they write controversial and thereby, subject to legal action. This fear and thus the mindset of deference compels the media to comply with the process of 'self-censorship' which is followed in authoritarian countries, not in any democratic country having the practice of constitutionalism and pledging to ensure rule of law. Online activists have reduced writing in both print and online forums, as well as reducing their expression or posts on social media on topics related to freedom of expression, women's rights, labor rights, indigenous peoples' rights, freedom of religion and secularism.

Activists stopped working and have both fears of legal harassment, government's increased punishments for expression- related offenses and fear of physical attack following the murders of their colleagues. Censorship of digital content, including blocks on YouTube, Facebook and high-profile Bengali blogs have become increasingly common.

The 'freedom of expression and speech' and 'freedom of the press', as enshrined under Article 39 of the Constitution of The People's Republic of Bangladesh, are qualified rights and capable of being restricted. Hence, the ICT Act and the Digital Security Act are in direct conflict with the constitution of Bangladesh. Similarly, Bangladesh is a signatory of the Universal Declaration of Human Rights (UDHR). The ICT Act is also in collision with Article 19 of the UDHR which guarantees freedom of speech from all forms of censorship.

2. METHOD

For this study, we have used standard methods of systematic qualitative study adapted from recent practices in human rights related legal policy analysis. Based on the framework, we've reviewed provisions of ICT Act, the Digital Security Act, and other related laws and analyzed how those provisions restrict online freedom of expression. The study also identified priorities to recommend policy steps to reshape law as compliant to rights guaranteed in Bangladesh Constitution and international treaties and conventions. The desk-based qualitative study was peer reviewed and finalised. As in many cases ICT Act is being used in connection to other related penal laws such as Penal Code and Special Powers Act, we have also done a quick appraisal of laws which are deemed to be related to freedom of expression on internet in Bangladesh.

2.1 Scope

This study is conducted based on a 'comprehensive and methodical appraisal of the Bangladesh ICT Act and Digital Security Act based on standard scientific research methodologies and peer-review'. It will add to the body of evidence assessing the ICT Act and DSA Act related to internet and will create awareness about the adverse impact of such laws in Bangladesh.

3. LEGAL FRAMEWORK FOR ONLINE FREEDOM OF EXPRESSION

The concept of freedom of expression has a long history before it was recognized as a fundamental human right by the international community, and has been entrenched in various legal documents. The justification for freedom of expression is centered on the liberal understanding that the issues related to moral choice must be left solely to individuals (Oozeer, 2014).

Under international law, the state has a duty to treat its citizens equally, freedom of expression exists as a basic human right and it defends all kinds of speech and other forms of expression. This concept of free expression has been successfully translated in legal terms and incorporated in various jurisdictions across the world.

3.1 Global Policy Framework

As the general framework of this study' we are primarily using the scope outlined in Article 19 of the Universal Declaration of Human Rights (UDHR), the UN resolution on the promotion, protection and enjoyment of human rights on the Internet (A/HRC/20/L.13), and the UN resolutions on the Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, and other related legal and policy instruments under international law. Based on the above mentioned three basic pillars, the policy framework provided by global instruments urges the states to respect and protect rights of all individuals for freedom of expression online.

3.1.1. State's accountability to universal human rights

Obligations of the states and accountability for human rights are formalized in the United Nations (UN) system and in treaty law and national law. The UDHR is the foundation of international human rights law. It inspired the development of the legally binding international human rights treaties listed below. Bangladesh is a party to this instrument.

The International Covenant on Civil and Political Rights, (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR) were

adopted in 1966. They provide a framework for the treaties that followed which focus on particular populations, for example, children, women, and people with disabilities. ICCPR identifies rights that are directly related to democracy and the rule of law, for example, equality before the courts, and rights to freedom of expression, religion, and association with others. ICESCR refers to rights necessary for quality of life (and life itself in the case of food); including rights to an adequate standard of living, education, and health and to take part in cultural life. These rights are to be 'progressively realized'.

Most human rights treaties have a monitoring committee that receives reports from state parties to the treaty, and can receive complaints on rights abuses and initiate investigations where states agree to this mechanism. Every UN member state is subject to the Universal Period Review (UPR) process whereby they provide a report on the human rights situation in their country, as do Non-government Organizations (NGOs), both international and national, and National Human Rights Institutions. Other states make recommendations in a peer review process to the country being reviewed. These accountability mechanisms ensure that human rights challenges within states are visible and subject to pressure to improve. Reviews and analyses of related legal policies like this study help NGOs and citizens to hold the governments accountable during UPR.

3.1.2. Online as Space for Universal Rights to Freedom of Expression

The UN has established the Internet Governance Forum (IGF) in order to deal with existing challenges relating to the Internet. It is a very good platform to bring different people from various stakeholder groups and discuss current problems and challenges in the field. UNHRC, in its General Comment No.34, addressed the issues of the development of modern technologies, clearly indicating that State parties should take into account that the developments in information and communication technologies have substantively changed communication practices around the world. Similarly, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression issued two reports on key trends and challenges to the rights of individuals to seek, receive and impart information and ideas of all kinds through the Internet in 2011 and 2013 respectively.

Furthermore, the OSCE Special Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information addressed several times, separately as well as in their joint declarations the

importance of online space and the protection of the right to freedom of expression on the Internet.

On 29 June, 2012 the UNHRC adopted a landmark resolution on the 'Promotion, Protection and Enjoyment of Human Rights on the Internet' (A/HRC/20/L.13). The resolution states that human rights apply both 'online and offline', and must be respected. The right to freedom of expression constitutes the core of the resolution as the 'rapid pace of technological development enables individuals all over the world to use new information and communications technologies.'

3.1.3. Major references in global policy for online freedom of expression

• UNHRC General Comment No. 34

The UN Human Rights Committee (see below) adopts general comments from time-to-time highlighting its jurisprudence in a specific area in one easily accessible and comprehensive document. General Comment No. 34, adopted in 2011, is its most recent general comment on freedom of expression.

• International Covenant on Civil and Political Rights (ICCPR)

The ICCPR is a treaty promulgated by the United Nations General Assembly which is legally binding to 170 States (as of April 2018) that have ratified it Bangladesh ratified the treaty on 6 September 2000. It is the key international human rights treaty setting out civil and political rights.

• Special International Mandates on Freedom of Expression: Joint Declarations

Globally, there are four special international mandates on freedom of expression, namely the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information. Each year, they adopt a Joint Declaration on a freedom of expression issue. While not formally binding, these provide authoritative evidence of the scope and meaning of international guarantees of freedom of expression.

- **UN Human Rights Committee**

The UN Human Rights Committee is the official body which is responsible for overseeing compliance with the ICCPR. When States ratify the ICCPR, they accept this oversight power of the Committee. A key part of this is that they are obliged to submit a report to the Committee every five years on what they have done to implement the treaty and the Committee then adopts its own views on their performance, which are in turn made public. States which have ratified the (first) Optional Protocol to the ICCPR, which does not include Bangladesh, also accept the jurisdiction of the Committee to hear individual complaints about their failure to respect the provisions of the ICCPR.

3.2. National Policy Framework

3.2.1. Constitutional Protection

Freedom of thought, conscience, and speech is a fundamental right protected by Article 39 (1, 2) of the Constitution of the People's Republic of Bangladesh. It is considered that this constitutional protection of freedom of thought, conscience, and speech also cover online spaces. The Constitution is the supreme law of the land of Bangladesh. All legislations and acts of the government must be consistent with it. Just as legislation must be consistent with the Constitution, subordinate legislation, such as regulations, must be consistent with both the legislations in terms of which it is made and the Constitution. For example, sections 98 and 99 of the Bangladesh Telecommunications Act empower the Government as well as the regulator, Bangladesh Telecommunication Regulatory Commission, to make regulations, which must be consistent with the Telecommunications Act and the Constitution.

3.2.2. National Policies and Legislations

The government of Bangladesh acknowledges the significance of the internet and digitally connected spaces as part of the public spaces, and thus in recent years, GoB is active to strengthen legal and policy framework to govern the online space. The current policy and legal framework regarding digitally connected spaces is largely shaped by three major pieces of laws and policies, namely, National Telecommunication Policy, 1998; National Information and

Communication Technology (ICT) Policy, 2002; International Long Distance Telecommunications Services (ILDTS) Policy, 2010; National Broadband Policy, 2009; The Telegraph Act, 1885; The Wireless Telegraphy Act, 1933; The Bangladesh Telecommunication Act, 2001; The Information and Communication Technology Act, 2006; The Competition Act, 2012; and the Digital Security Act, 2018.

National Telecommunication Policy, 1998

This policy is, in fact, a summary statement of the philosophy, objectives, strategies and the methodology to ensure equitable and judicious execution of the business of telecommunications in the country. According to the policy (GoB, 1998), the strategic vision of the government is to facilitate universal telephone service throughout the country and where there is a demand, all those value added services such as cellular mobile telephone paging, data services, access to the Internet (including electronic mail), voice mail and video conferencing – all at an affordable cost without compromising performance. This policy is currently under a process of being updated. The policy also specifies the need for greater investment from the private sector to stimulate competition as well as creating an independent, separate and autonomous institution, the Bangladesh Telecommunications Regulatory Commission (BTRC), to regulate and monitor the Telecommunications Acts that were to be drafted later. With its emphasis on the right to "the exchange of information" amongst citizens and on the development of services from the private sector, the policy may appear fair and respectful of the public's needs. However, the underlying details of the policy give the state the ultimate control in regulating ICTs. Whereas the BTRC is meant to be fully independent, the functions given to it are broad and vague, including "any other functions and activities as may be considered necessary by the government". Indeed, it is only in 2002 that the BTRC became independent in reality. The BTRC has since proved to be inefficient in fulfilling its objectives and being true to its fundamental four features: Independence, Transparency, Adaptability and Objectivity.

National Information and Communication Technology (ICT) Policy, 2002

Ministry of Science and Information & Communication Technology of the Government of Bangladesh framed the ICT policy (GoB, 2002) with the aim to building an ICT-driven nation comprising of a knowledge-based society. In view of this, a country-wide ICT-infrastructure will be developed to ensure access to information by every citizen to facilitate empowerment of people and enhance democratic values and norms for sustainable economic development by using the infrastructure for human

resources development, governance, e-commerce, banking, public utility services and all sorts of online ICT-enabled services.

The policy outlines some of its objectives that are closely related to governance, transparency, data protection, security, and universal access:

- Promoting and facilitating use of ICT in all sectors of the economy for transparency, good and efficiency improvement;
- Establishing legislative and regulatory framework for ICT issues like IPR, data security and protection, digital signature, e-Commerce, ICT education etc. as well as to ensure quality ICT education provided by different private organizations; and
- Setting up national databases that are reliable and easily accessible to all the people of the country.

International Long Distance Telecommunications Services (ILDTS) Policy, 2010

This policy (GoB, 2010) has been formulated by MoPTIT in order to address the pressing issues that emerged during regulation of technologies of long distance calls especially through Voice over Internet Protocol Services (VoIP). VoIP has been very popular among the users as it provides inexpensive voice communication over the internet all over the world. VoIP has been the catchphrase in Bangladesh for quite some time. The issues of VoIP could not be addressed in the previous telecom policy of 1998 and in Bangladesh Telecommunications Act, 2001 as its success was not conceived at that time. Amidst confusion and delays in regulating VoIP services, many secret operations of VoIP services mushroomed depriving a huge amount of revenue to the Government. The new policy is formulated in order to regulate the call forwarding service of long distance international calls through approved technologies including VoIP.

National Broadband Policy, 2009

Right to internet access is considered to be an ancillary right to exercise and enjoy right to freedom of expression and right to information. In line with that, this policy (GoB, 2009) was unveiled in 2009. The broad objective of the policy is to provide broadband internet access across the country and set an ambitious target of broadband penetration of 30% throughout the country by the year 2015. The policy not only puts stress on internet infrastructure growth but also gives emphasis on local internet content development.

The Telegraph Act, 1885

The history of telecommunication legislation in Bangladesh dates back to 1885 when the first specific telecommunication law, the Telegraph Act, 1885, was passed. Although the Act has not been repealed by the subsequent legislation, it has almost lost

its practical application since telegraph services are obsolete now. Despite that, a few provisions of the Act could still be applied in supplement with the latest laws. For example, section 5 of the Act dealing with interception of message and communication is still operative.

The Wireless Telegraphy Act, 1933

The preamble of the Act states that this is an Act to regulate the possession of wireless telegraphy apparatus. This is a short Act containing only 11 sections. Section 3 prohibits possession of wireless telegraphy apparatus without obtaining a license the procedure of which is outlined in section 5. Whoever possesses wireless telegraphy without a license shall be punished with a fine of one hundred BDT and for subsequent offenses; a fine of two hundred fifty BDT will be imposed on the offender.

The Bangladesh Telecommunication Act, 2001

Enactment of Bangladesh Telecommunication Act, 2001 was a significant step from Bangladesh government to liberalize the telecommunication sector of Bangladesh. The major duties of regulating the sector are transferred to newly created and independent commission known as Bangladesh Telecommunications Regulatory Commission (BTRC). The 2001 Telecommunications Act was amended in 2006 in a move by the government to put a break on the progress that was being made on access to information and technology. Partly because of fears associated with the rise of terrorism and the bombing on the 17th of August 2006 by the terrorist group Jama'atulMujahideen Bangladesh (JMB), the amendment allows an officer of the intelligence agencies, national security intelligence, investigating authorities or law enforcing agencies to intercept and record telephonic conversations of, and exchanges of messages – electronic or otherwise – between private citizens. Where the initial Act meant to create an independent and objective commission, the amendment more or less gives the power back to the Telecommunications Ministry. It also calls for government's access to customer information that is held by telecommunications providers and alters the Act so that the general privacy guarantee is now subject to national security laws. As will be shown later, this amendment has terrible effects not only on the citizens' privacy but on access to information, the right to free speech and democracy.

The Information and Communication Technology Act, 2006, (amendment in 2013)

The primary stated objective of the Information and Communication Technology Act, 2006 is to provide legal validly and security to information and communication technology and to make rules in relation to that. This law, however, does not regulate the telecommunication sector in the manner of the Telecommunication Act. The significance of the ICT Act, in

relation to telecommunication, linked in the fact that this law removes and explains some of the legal uncertainties in relation to information and communication technology. The ICT Act deals with some specific subject matter: Authentication by Electronic Signature; Legal Recognition of Electronic Records; Communication of Electronic Records; Electronic Gadget; Certification Authority; Licenses; Cybercrimes and Punishment; and Cyber Tribunal. This Act aims to provide a legal framework so that legal protection is accorded to all electronic records and other activities carried out by electronic means. Simultaneously, ICT Act, 2006 provides that the controller of certifying authorities can order decryption of any information and if any person does not cooperate with the regulatory authorities for such decryption, he or she can be imprisoned up to 7 years. Similarly, under the Special Powers Act, the authorities can intercept communication including emails under stated procedures without the knowledge of the email user. Ever since the passing of the Information and Communication Technology Act by the parliament, a lot has been said both for and against the Act. The controversy seems to have largely revolved around the fact that the police have been given unfettered powers to surveil those who are reasonably suspected to have committed or about to commit an offence under the ICT Act. The Government on its part has defended above provisions by arguing that there is nothing new in enacting such a law and their similar provisions already exist in other status as well. The government also argues that there are adequate safeguards in the ICT Act itself, which provides that the provisions of the Code of the Criminal Procedure shall apply in relation to any entry, search or arrest made under the ICT Act.

4. ANALYSIS OF POLICIES AND LAW

Article 19(3) of the ICCPR states that the right to freedom of opinion and expression may be subject to certain restrictions which are provided by law and are necessary for the respect of the rights or reputations of others: for the protection of national security or of public order (order public), or of public health or morals. Similar limitations and restrictions are found in other international and domestic legal documents. But the ICT Act, in connection with other laws, severely restrict this inalienable rights to freedom of expressions in Bangladesh, and in many cases criminalizes such freedoms that is not consistent with such reasonable limitations.

The ICT Act deals with some specific subject matter: Authentication by Electronic Signature; Legal recognition of Electronic Records; Communication of Electronic Records; Electronic Gadget; Certification Authority; Licenses; Cybercrimes and punishment; and Cyber tribunal. This Act aims to provide a legal framework so that legal protection is accorded to all electronic records and other activities carried out by electronic means. Simultaneously, ICT Act, 2006 provides that the controller of certifying authorities can order decryption of any information and if any person does not cooperate with the regulatory authorities for such decryption, he or she can be imprisoned for up to 7 years. Similarly under the Special Powers Act the authorities can intercept communication including emails under stated procedures without the knowledge of the email user. Ever since the passing of the Information and Communication Technology Act by the parliament, a lot has been said both for and against the Act.

4.1 Restricting Online Spaces and Criminalizing Expression

4.1.1 Criminalizing online freedom of expression and inflicting disproportionate punishment

One of the main pieces of legislation is in force related to online expressions are the ICT Act. Under this law, no warrant is required to make an arrest, and offenses under this act are non-bailable. Under Section 57 of this act, if social, political and religious contents that are distributed electronically deemed offensive, the offenses were punishable by a prison term from 10 to 14 years and

fines up to BDT 10 million. Sections 68 and 82 contain provisions for a Cyber Tribunal and Cyber Appellate Tribunal to judge offenses under this act (GoB, 2006). The Appellate Tribunal is yet to be formed.

Legal policy analysts and human rights advocates have analyzed that this law severely undermined freedom of expression and right to information (ASK, 2013). Criminal offenses under Section 57 were very loosely defined. By such definition that is contrary to the basic principle of Criminal law, had been expanded the state power upon the infliction of unnecessary and precarious punishment. Through the use of very vague terms of Section 57 ('creating a crisis for the image of the state', for instance) had been denied fundamental 'principle of certainty' of criminal law. It created the opportunity to bring any of the innocent or legitimate online publications or dissemination, under the wish of state and punishment. There has been 5 years imprisonment under Section 16 of Special Powers Act of 1974 for the publication of Prejudicial Report. This intrepid and widely blamed section had been considered as a great threat for the mass-media for long time. This provision was subsequently repealed. Currently, the majority of the daily newspapers publish online version. Upon this reality, Section 57 of ICT Act had created the opportunity to apply criminal power, probability of more punishment likewise under Section 16 (abolished) of the Special Powers Act.

The principle of proportionality has not followed in assessing the level of punishment provisioned in the ICT Act. A comparison with other common law offense, it is clearly evident that the amount of the penalty specified in Section 57 of the ICT Act 2006, was unreasonable and disproportionate. Such disproportion in case of level of punishment makes the ethical basis and effectiveness of implementation of criminal law feeble by final judgment. The Amendment of the Act in 2013 presented that probability more evident.

This provision also made several offences cognizable as such and non-bailable, thus created unlimited scopes for harassment by law enforcing agencies. 'Defamation' defined in Penal Code 1860 is bailable offense and the maximum penalty is imprisonment for 2 years. Until 2011, after taking the defamation case in cognizance, the courts used to issue warrant for the arrest of the accused. For such provisions, the journalists and activists have unexpectedly been harassed for long time. The present government through the amendment of 2011, made a regulation that court can issue summon instead of warrant. This creditable initiative in the development of independent media had been futile by the provisions of ICT Act. The government might apply Section 57 on any considering defamatory against any report published on any online journal. In such case, the offences were non-bailable and punishable for minimum 7 years and maximum 14 years

imprisonment respectively. In addition, the court could issue arrest warrant by taking cognizance of such offence.

4.1.2. Defamation or Injury to the Reputation

Under Sections 500, 501, and 502 of the Penal Code 1860, the authors of defamatory content which is communicated by any means (including email) can be punished with imprisonment of up to two years or a fine or both. Similarly, Section 57 of the ICT Act was to regulate content, including internet content which is obscene or if its effect was such as to tend to deprave and corrupt persons and which may harm the religious sentiment of the religious community. Under the act, offenders could face up to ten years of imprisonment or a maximum fine of BDT 10 million (approximately USD 140,500) for publishing content that is 'falsified or vulgar." This included defamatory content that might harm law and order and attack political elites. Laws against defamation aim to protect the rights and reputations of others thus are considered to pursue a legitimate aim under international law. However, criminal punishments are not viewed as passing the proportionality and necessity tests of the three-part test; civil law remedies are viewed as sufficient for protecting the rights and reputations of others and are less likely to have a chilling effect of freedom of expression. This will be discussed further below. In addition, there should be much tighter definitions for what constitutes defamation of political elites as a consequence of their public role and as a necessary protection of democracy.

4.1.3. Hate Speech, Blasphemy and Hurting Religious Sentiments

Section 153 (A) of the Penal Code prescribes punishments for promoting "enmity, hatred or ill-will between different class." This could be used to prosecute extremists who encourage religious hatred, particularly those whose 'malicious intent' is clear. In addition, the Penal Code, 1860 discourages blasphemy by a section that forbids 'hurting religious sentiments'. Under Section 295A of the Penal Code, any person who has a "deliberate" or "malicious" intention of "hurting religious sentiments" is liable to imprisonment.

4.1.4. Inadequate protection of the right to privacy and data protection

As online activity has increased, GoB says that it has also increased its surveillance of online spaces. Surveillance in Bangladesh is closely linked to fears about national security threats, specifically terrorist threats. According to Section 97(A) of the Telecommunication Act 2001, for the security of the state and public tranquility, the Government can empower any of its agencies to record, prevent and collect information regarding communications made by any person through telephone. This section also states that the Government can order any service provider for assistance and the service provider will be bound to assist the Government or face punishment. Under the Act, there is no requirement for any prior warrant or order of any court to collect information. The 2006 amendment of the Act confirms this surveillance regime and its extension. The ICT Act 2006 provides that the controller of certifying Authorities could order decryption of any information and if any person does not cooperate with the regulatory authorities for such decryption he or she could be imprisoned for up to 7 years. In addition, under the Code of Criminal Procedure, read together with ICT ACT, an investigating police officer has the right to not only intercept and monitor communication but also to requisition support from network administrators for the purpose. Any refusal could be considered punishable. On 27 January 2012 a new regulatory authority was created called the Bangladesh Computer Security Incident Response Team (BD-CSIRT) that is allowed to conduct wiretaps and internet surveillance for the purposes of tackling state security issues of counter-terrorism, external threats, and high-profile crimes. There is no transparency in the investigation process, especially with respect to obtaining personal information. The security agencies are accountable only to the Prime Minister's office. Surveillance is a growing phenomenon, with many legal underpinnings, but the exact scale and application of these surveillance measures is difficult to determine due to a lack of transparency of judicial scrutiny. None of the laws mentioned above include the requirement for judicial accountability to protect the rights of citizens, and this can have a serious impact on the ability of citizens to communicate freely online. Furthermore, while there are many laws sanctioning the surveillance regime, there is no data protection law. This means that companies can indiscriminately collect and use data (in fact they are required to) and the user has none of the accepted international recourses to protect their data, for example, by enabled to find out which of their data is stored, for what purposes and who has access to it.

4.1.5. Access to the Internet and the necessary infrastructure

The current government declared its long-term vision for the country as "Digital Bangladesh". According to the government, "Digital Bangladesh" does not only mean the broad use of digital technologies, it also means the effective and beneficial use of technology directed towards achieving better standards in education, health, job placement, poverty reduction etc. The government has emphasized four elements of "Digital Bangladesh Vision" which are human resource development, people involvement, civil services and use of information technology in business.

The International Telecommunication Union estimated internet penetration in Bangladesh at 18 percent in 2016. The Government of Bangladesh estimates were close to 46 percent. Information and Communication Technology usage is increasing fast, though Bangladesh lags behind globally. The World Economic Forum 2015 Global IT Report ranked Bangladesh 109 out of 143 countries worldwide, with infrastructure and regulatory environment scoring poorly, though overall communication service was comparatively affordable, a factor that is driving growth.

The vast majority of internet users are from the urban middle class. This is because connections are largely concentrated in urban areas, because they continue to be prohibitively expensive to most average citizens, there is insufficient local content and low literacy levels. These are all issues that the government must seek to tackle through investment, supporting innovation and developing an appropriate law and policy framework. More encouragingly, in recent years there has been a marker increase in local websites, Bangla content, and localized online tools and e-commerce.

4.2. The Digital Security Act 2018

On September 19, 2018, the Digital Security Act, 2018 (Act No. 46 of 2018) was passed by the National Parliament (Jatiya Sangsad). The Act is published in the official gazette on 8 October 2018. Section 61 of the Digital Security Act, 2018, repealed sections 54, 55, 56, 57 and 66 of ICT Act, 2006.

The law fails to respect those standards in a number of key respects. International standards dictate, among other things, that content restrictions and other criminal measures should not be vague, overboard or unnecessary, that parallel regimes for online activities are warranted only where the activity is either completely or substantially different, that penalties should not be

greater simply because an activity is carried out online, and that regulatory systems should be protected against political interference. The Act fails in important ways to respect all of these standards.

An initial problem is that the Act employs extremely broad definitions for key terms, including the very central notion of "digital security", which covers all types of security and not just external threats to security, and then grants regulators very broad powers in relation to digital security. Other notions which are defined too broadly include "unlawful access", which covers not only unlawful access but also any access, even if lawful, that prevents a system from sending information, which happens every time someone shuts down a computer. Similarly, "malware" is defined as any program that changes the tasks performed by a computer, whether or not this is done with intent to harm the computer, which would, as a result, include a user tweaking his or her own settings. Although we presume that these are mistakes, and that individuals will not be charged for shutting down their own computers, the fact that the Act allows for this means that it could easily be abused.

Another serious problem with the Act is that, instead of setting out clearly the functions and powers of the bodies it creates, and the procedures for applying the powers it grants, much of this is left to be determined by rules, which will be adopted later by the responsible minister. This includes the "[p]ower, duty and activities" of the Digital Security Agency, the key implementing body for the Act, which are almost entirely left to be determined by the rules. This not only fails to give citizens appropriate notice of what these powers will be, but it also grants enormous discretion to the minister to determine how very intrusive powers over online communications will work. It is also inconsistent with established practice in Bangladesh, as well as other democracies, whereby the powers of regulatory bodies are set out in the primary legislation.

The above problem is seriously exacerbated by the fact that the Agency, and its oversight body, the National Digital Security Council, are controlled by the government instead of being independent, as international law requires regulatory bodies which have powers in the area of freedom of expression to be. The Act fails to indicate who will sit on the Council, but it does stipulate that the Chair will be the Prime Minister. The government also constitutes the Agency, appoints its Director General and approves its organogram. The Act even appears to give law enforcement agencies the power to order Bangladesh Telecommunications Regulatory Commission to block a range of types of content, instead of granting this power to an independent body.

When it comes to the content restrictions, three general problems keep coming up, with some provisions exhibiting more than one problem at

the same time. First, a number of content restrictions are simply not legitimate according to international standards because they prohibit expression that is protected under international law. Obviously these should be removed from the Act. Second, several content restrictions duplicate restrictions which are already found in existing laws of general application, such as the Penal Code, often with heavier penalties being provided for in the Act. There have already been amendments to various laws, including the Penal Code, to ensure that it applies to digital means of disseminating content. There is, therefore, no need to duplicate these offences in a specific digital law. There is also no warrant for imposing harsher penalties on digital content than on its offline equivalent. Third, a number of content restrictions are worded too broadly, giving undue discretion to the authorities in how they are applied.

This is the fact that most of the offences in the Act, namely 14 out of the 18 separate sections providing for offences, are cognizable and non-bailable. For cognizable offences, the police can make arrests without a judicial warrant, with the result that these rules are far more open to being abused to harass journalists and citizens. For non-bailable offences, once charged an accused will normally be held in detention unless a court, in its discretion, agrees to grant bail. Given that almost all of these offences already fail to conform to international standards, these features are extremely problematic.

The following content restrictions limit forms of expression that are protected under international law:

- Information which "hampers unity, economic activity … religious sentiment" (section8(2))
- Propaganda "against the Liberation War of Bangladesh or the ideals of the Liberation War or against the Father of the Nation" (section 21) (cognizable and non-bailable)
- "Offensive" information (section 25(1)(a))
- Information that "can make a man corrupt or degraded" (section 25(1)(b))
- Information one knows to be false to "annoy, humiliate … someone" (section 25(1)(c))
- Knowing it to be false or propaganda, publishing information, "either in full or partially distorted to tarnish the image or the good name of the State" (section 25(1)(d))
- Publishing information with the intention and result of hurting "religious values or sentiments" (section 28) (cognizable and non-bailable)

The following content restrictions provide broad limits on expression:

Information which "hampers … security, defense … or public order or promote hatred towards a community in the entire country or in part of it" (section 8(2)), because "hamper" and

"promote" represent standards which are too low to restrict expression.

Publishing or broadcasting "intimidating" information (section 25(1)(a)), because this does not contain limits that a prohibition on issuing a threat would have information one knows to be false to "insult someone" (section 25(1)(c), because this does not contain defenses needed for defamation.

• Intentionally publishing information that "creates tension or chaos or deteriorate law and order or pose a threat to that effect" (section 31), because the standards associated with these offences are too low (cognizable and non-bailable).

In some cases, the offences described above provide harsher penalties for crimes committed online. This is particularly evident with the Section 29, which is exactly the same offence as under the Penal Code. While the Penal Code only provides for imprisonment for up to two years for defamation, Section 29 envisages imprisonment for up to three years, 50% longer. Similarly, Section 28 dealing with hurting religious sentiments, provides for seven years' imprisonment, whereas the analogous provisions in the Penal Code provide for only one or two years' imprisonment.

The Act also includes a large number of offences – in sections 17, 18, 19, 20, 22, 23, 24, 26, 27, 30, 32, 33 and 34 – that are not essentially content related, almost all of which are cognizable and non-bailable. A general problem with most of these provisions is that they fail to stipulate a clear and strong intent requirement, which should therefore, be added to all of them.

Section 38 is essentially positive in nature, providing for protection for service providers as long as they can prove that there were "not aware of the offence or tried its best to prevent the commission of offence". However, this standard is too limited because it is likely to lead to takedown whenever someone claims any content breaches the law. This is because service providers will not be able to verify all of the claims and so will simply take the content down rather than risk taking on liability. Better practice is to protect service providers unless they adopt or intervene in the content, or are ordered by a court to take it down.

Sections 22-24 deal, respectively, with forgery, fraud and fraudulent impersonation and appear to unnecessarily duplicate provisions in the Penal Code, which has extensive provisions dealing with these issues which already appear to cover the commission of these crimes using digital tools. Sections 17, 18, 32, 33 and 34 all deal with access issues, whether to information or computer systems. While it is legitimate to prohibit intentionally illegal access gained for purposes of causing harm, many of these provisions go beyond this. Clear requirements of intent to cause harm should be added to all of them (or they should simply be removed). In some cases, such as

section 34(a), dealing with hacking, the access does not even need to be unlawful, so that changing information in your own computer would be deemed to be hacking. Section 32 deserves special mention because it addresses accessing confidential government information. Better practice in this regard is to impose sanctions only on officials who are under a primary obligation to protect the information, and not to sanction third parties, including journalists, to whom information is leaked. These sorts of rules should also exempt whistleblowers – individuals who expose wrongdoing – from their scope.

These problems with both the content and other offences in the Act are exacerbated. Since the fact is that the penalties for violation of its provisions are, in most cases, very harsh indeed, providing for long prison sentences for content and actions that should not be criminalized in the first place. The combined effect of the penal prohibitions in the Act is very severe indeed. Some provisions appear to have been included by mistake, given how broad and unnecessary they are.

Others seem to have been included with intentions, giving the government broad grounds to charge individuals with crimes, even though there is no victim and the activity is otherwise perfectly normal. Yet others prohibit types of expression that are protected under international law. These loopholes are exacerbated by the lack of independence of the regulators, the power of the government to largely define the mandate and powers of the regulators (which they control), the very harsh penalties for breach of most of the provisions and the fact that most of the offences are cognizable and non-bailable. It is clear that major changes need to be made in the Act if it is not to become a tool for seriously undermining respect for freedom of expression in Bangladesh.

5. CASE HIGHLIGHT: SHAHIDUL ALAM

Started in late July 2018, the student movement for road safety was the biggest uprising by the youth in recent decades. Following the death of two students in a road accident, protests sparked in Dhaka and other cities of Bangladesh. Thousands of students joined peaceful protests, however, the government showed no sign of accepting any demand of student rather police fired tear gas at students, pro-government students launched counter-attacks, and anyone documenting the incidents was stopped. The government used ICT laws to stop the people who supported this movement. Series of cases under Section 57 of the ICT Act were filed and a number of people were arrested on charges of inciting violence by spreading rumours on social media. One of the arrestees is a prominent photographer, ShahidulAlam who was charged with spreading propaganda against the government during the road safety movement after he criticized the government's response to the protests in an interview with Al Jajeera and posted on Facebook.

Shahidul's arrest, detention and treatment violated his fundamental human rights that are protected by both the national and international laws. Shahidul is only one of many professionals including journalists, editors, professors and bloggers arrested on the basis of the ICT Act, and silencing of those who speak out against police brutality.

Shahidul Alam, a renowned photographer, documented the protests in early August 2018. Alam had gone live on Facebook several times to discuss clashes in the capital city's Jigatola area between students demonstrating for safer roads, and police and alleged activists of ruling party affiliate organizations. Later, in a Skype interview with Al-Jazeera, he commented on the excessive use of force by the police and that he had observed. Therefore, he had been a target of the government and a victim of the ICT Act.

Shahidul Alam's Arrest, Charges, Detention and Treatment

On the night of August 4, 2018, a celebrated photographer, 63-year-old ShahidulAlam was picked up around 10:30 p.m. from his home at Dhanmondi. Dhaka Metropolitan Police (DMP) Detective Branch later confirmed that they had picked him up for interrogation. Shahidul, also the founder of Drik Gallery and Pathshala South Asian Media Institute.

Drik, Shahidul's photography agency, later issued a statement stating Shahidul was forcibly abducted. Security guards of the apartment building and other

eyewitness reported, there were roughly 30 to 35 men in plain clothes, who claimed to be from the Detective Branch (DB). The men went upstairs, brought down Shahidul, who was screaming as he was forcibly pushed into the waiting car. They taped up the CCTV camera, and took away the CCTV camera footage. The guards were manhandled and locked up. (Dhaka Tribune, August 5, 2018)

On August 6, Inspector Md Mehedi Hasan of the Detective Branch of Police (north zonal team) filed the case against Shahidul Alam with Ramna Police station where he said the noted photographer tried to instigate students and create instability in the country by spreading false information and rumors on social media. The inspector alleged that Shahidul's remarks were aimed at worsening the law and order situation, tarnishing the image of the country, and hurting the sentiments of students by spreading rumors to instigate them to be engaged in destructive acts. Police filed a case under Section 57(2) of the ICT Act.

On August 6, 2018, a Dhaka court placed him on seven-day remand for interrogation in a case filed with Ramna police station. The case statement filed by the DB says Shahidul was charged under Section 57(2) of the ICT Act because he used electronic media to instigate disorder in the country and spread fabricated information and rumors via social media. The FIR also mentioned that his remarks were aimed at worsening the law and order situation, tarnishing the image of the country and hurting the sentiments of the students by spreading rumors. When he was produced before the court on August 6, Shahidul Alam said, 'I was hit [in custody]. [They] washed my blood-stained punjabi and then made me wear it again'. However, as always has been the case, police refuted the allegation.

Shahidul's arrest and imprisonment sparked outrage and condemnation at home and abroad. Since his detention, civil society groups, activists and others have called for his release. 24 civil society groups including Transparency International Bangladesh, Reporters Without Borders and the Committee to Protect Journalists issued a statement condemning the "blatant violation" of Alam's right to freedom of expression and calling for his "immediate and unconditional" release. A change.org petition for the release of Alam was launched by rights group Amnesty International. Five renowned intellectuals and authors - Arundhati Roy, Eve Ensler, Naomi Klein, Noam Chomsky and Vijay Prashad - issued a statement urging Bangladeshi government to "immediately release" Alam and drop all charges against him. Others who have expressed concern and demanded release and charges dropped include Nobel Laureate in Economics Joseph Stiglitz, Binayak Sen, Gayatri Chakravorty Spivak. AmartyaSen also voiced support for Shahidul Alam. Noam Chomksy called for Shahidul's release. British MP and Prime Minister's elder sister's daughter

Tulip urged Prime Minister Sheikh Hasina to release Shahidul Alam.

On August 11, 2018, Prime Minister's son and her ICT Advisor Sajeeb Wazed Joy in a Facebook post said Shahidul Alam's claim of torture is another of his false accusations against the government. Joy claims Alam pretended to be hurt in front of the cameras."This just proves how dishonest Shahidul Alam is."

On August 12, 2018, a Dhaka court sent Shahidul to jail, rejecting his bail petition, after the police had produced him before the court on completion of his seven-day interrogation. On September 4, 2018, a High Court Division bench declined to hear Shahidul's bail petition as a Judge felt embarrassed. The bench of Justices MdRuhul Kuddus and Khandaker Diliruzzaman was set to hear the bail petition on September 4. His lawyers filed the bail petition on August 28, 2018.

Later on September 11, 2018, Dhaka Metropolitan Sessions Judge KM Imrul Kayes rejected Shahidul's bail petition. Shahidul filed a bail petition with the High Court Division. On October 7, 2018, The High Court Division issued a ruling asking the government why acclaimed photographer Shahidul Alam should not be granted bail. On November 1, 2018, a High Court Division bench dropped Shahidul Alam's bail petition from the cause list. On November 6, 2018, Shahidul filed a bail petition with another bench of the High Court Division.

Bail and Release

Following a petition filed by 63-year-old Shahidul, the High Court Division on November 15, 2018, granted him bail considering his age and the time he spent behind bars on charges of "spreading propaganda against the government". On 20 November 2018, After 107 days in jail, acclaimed photographer ShahidulAlam was finally released, five days after he had secured permanent bail from the High Court. In an instant reaction, Shahidul said, "We expect that in independent Bangladesh, people will be able to speak freely. If that does not happen, being inside [jail] or out in the open is the same." However, the government filed a petition with the Appellate Division of the Supreme Court seeking stay on the High Court Division verdict that granted permanent bail to acclaimed photographer ShahidulAlam. The apex court is yet to fix any date for hearing the petition.

Shahidul Alam is still facing charges under section 57(2) of the ICT Act that could sentence him punishment of imprisonment for up to 14 years.

5.1 Example of a case under the Digital Security Act

Five young people were arrested from different parts of Dhaka during a CID raids. They were charged under sections 23, 24 and 26 of the Digital Security Act, 2018. The charges brought against them were digital or electronic fraudulence and identity theft. This was the first case filed under this law. These young people are said to have cheated admission seekers by selling fake question papers of medical college admission test. They are also accused of being part of a syndicate which used to leak questions of different public universities' admission tests.

CID said at a press briefing that, these boys used fake Facebook IDs for selling question papers, assuring admission seekers of having a '100 percent common' from their questions in the exam. They also took money in advance through mobile wallet. (The Daily Star, October 12, 2018).

5.2. Why Sampadak Parishad opposes the Digital Security Act

Sampadak Parishad has rejected DSA by providing detailed critical explanation on different sections of the Act. They also translated relevant sections of the Act from Bangla to English. Only Englsih version of their translation is drawn below. Their views were published in the Daily Star. The reference is given as well.

The Digital Security Act (DSA) just passed in the parliament suffers from the following fundamental flaws:

1. In trying to make a law to prevent crimes through digital devices and provide security in the digital sphere the Act ends up policing media operations, censoring content and controlling media freedom and freedom of speech and expression as guaranteed by the Constitution.

2. The Act gives unlimited power to the Police to enter premises, search offices, bodily search persons, seize computers, computer networks, servers, and everything related to the digital platforms. According to the Act, the Police can arrest anybody on suspicion without warrant and do not need any approval of any authorities.

3. The Act suffers from vagueness and uses many terms that can be misinterpreted and used against the media.

4. DSA will create an atmosphere of fear and intimidation which will make journalism and especially investigative journalism virtually impossible.

5. In addition to media professionals, the law will create panic among all users of computers, computer networks, etc.

When the ICT Act was made in 2006, the government said journalists had nothing to fear as its aim was to prevent cybercrimes and punish cyber criminals. The reality is journalists and people who exercised their constitutional rights to freedom of speech suffered imprisonment and harassment under Section 57 of the ICT Act. The same is now being said that Journalists have nothing to worry about the DSA, but the apprehension is that journalists will again face the same kind of harassment by this law.

The purpose of the law as mentioned in its preamble is to "ensure digital security and prevent crimes committed on digital platforms". Hence we should not have been worried about the law. But the problem is that DSA goes much beyond its defined scope and ventures into the territory of media and journalism. The law goes against the very nature and practice of independent journalism that stands to protect people's right to know and exposes abuse of power and corruption.

The DSA deals with the digital world which is ever evolving. Digital technology is all pervasive from national security to food production to health services to financial transactions, and media are no exceptions.

While other fields mentioned above may require "regulations" media needs "freedom". The DSA is focused only on the "regulation" aspect and totally neglects the need for media freedom. This is one of the fundamental flaws of DSA making it so dangerous for the media.

A frightening aspect of the DSA is the enormous arbitrary power given to the Police who may arrest a journalist just on suspicion of a so-called crime that he thinks may be committed in the future. The police are allowed to make such arrests which have been made mostly non-bailable without any warrant. In practical terms, this will bring journalism under police control.

What is also alarming is that out of 20 or so provisions of the law that deal with offences and punishments, 14 are non-bailable, five are bail-able and one can be negotiated. The lowest punishment is 1 year in prison and the highest life-term but mostly in the range of between 4 and 7 years. This will inevitably create an atmosphere of FEAR and INTIMIDATION under which normal functioning of journalism will become extremely risky if not impossible. Not only does this law go far beyond what it was supposed to address, it is also full of vagueness that leave scopes for abusing of the law. Experience shows both in Bangladesh and abroad that laws that are clearly-worded, crimes that are specified and punishment proportionate to crimes lead to better "rule of law". Vagueness leads to misinterpretation of crimes and misuse of the law. When law is misused freedom is curtailed.

Another flaw of the DSA is the level of punishment meted out to "offenders". Let's take the case of the Road Safety Act which was passed along with the DSA. The former provides for a maximum

punishment of 5 years for killing people in accidents while a journalist can be punished for up to life-term for violating the colonial era Official Secrets Act (1923) which can happen if a reporter takes pictures of an unpublished government document with his mobile phone, which is now a very common practice.

Detailed Explanation

Below we present a detailed analysis as to why Editors' Council considers this law to be anti-free press, against freedom of speech and antithetical to democracy.

Section 8

Power to remove or block information and data:

(1) If the Director General is satisfied that something that is published or disseminated in the digital platform falling within his domain may poses threat to digital security, he may request Bangladesh Telecommunication Regulatory Commission (BTRC) to remove such information or data or, in specific cases block the platform.

(2) If it is evident to the law enforcing agencies that something published and disseminated through any digital device or digital medium can create disunity in the country, disrupt economic activities and security, defence, hurt religious values, create communal hatred or bad feelings, create law and order situation then the law enforcing agencies can request the BTRC to remove such content or block it.

(3) On receipt of such requests, BTRC while informing the government will take immediate actions to remove or block the content.

Sampadak Parishad's Comment:

There are two issues of concern here -- the power of the Director General and the power of the law enforcement agencies. The power to block contents will hit the heart of publication either in print or online. Any report may be blocked or a photograph may be confiscated that may lead to disruption of any media outlet.

The justification needed to remove or block content are too vague and subject to individual interpretation and hence leave the scope for abuse of the law. For example, if exposing corruption in a project leads to stopping its financing by any donor or a private investor, then a journalist can be accused of "disrupting economic activity" under this law and this can lead to blocking or removal of the content.

Section 21

Punishment for any propaganda against the Liberation War, Spirit of the Liberation War, Father of the Nation, National Anthem and National Flag:

(1) If an individual makes propaganda against The Liberation War, Spirit of Liberation War, Father of the Nation, National Anthem and National Flag or assist in such a process then such an action will be considered as a crime.

Sampadak Parishad's Comment:

We are fully committed to the preservation of the dignity and correct history of our Liberation War and given the past experience of attempts at its distortion, we understand the need to do something in this regard. However, "Spirit of Liberation War" is rather vague term. Without further defining the "crimes" under this section and clearly specifying what constitutes a "crime" we run the risk of serious abuse of this law and harassment of journalists and the punishment is up to life-term or (and) Tk 3 crore in fine or both.

"Mukti Juddher Chetona" (Spirit of Liberation War) is a vague term and is very subjective and cases can be brought against journalists as interpretations can vary.

We reiterate that we are in favour of protecting the great legacy of our Liberation War for the future generations. However, when laws are being framed, we need to be very clear and specific. Given its present form, not only journalists but historians, researchers and even creative writers like novelists will also suffer. It may even result in people not writing or researching much on our Liberation War fearing misinterpretation and the possibility of punishment.

Section 25

Publishing or distributing attacking, false or intimidating information or data:

(1) If any person using a website or any digital device-deliberately or knowingly distributes any information or data that is attacking or intimidating in nature; or if a person publishes or distributes any information despite knowing that it is false to irritate, humiliate, defame or embarrass or to discredit a person

Or

(b) Damages the image and reputation of the State or spreads confusion or with the same purpose publishes or distributes fully or partially distorted information or data despite knowing that it is false, and if any one assists in such actions then all such actions of the individual will be considered a crime.

Sampadak Parishad's Comment:

This will directly affect all investigative reporting in the media. Such reports are usually about some irregularities performed by institutions and individuals. Corrupt people will use this law to intimidate journalists and media organizations and try to prevent publication of such stories on the pretext that the reports have attacked or intimidated them. Actually every such report can be said to fall under one or more of the above categories and can be used to harass the media.

Any investigative report that reveals corruption about a person or an institution is bound to "irritate", "embarrass" or "humiliate" someone. This provision will make it impossible to publish any negative report about any corrupt person. This will reduce newspapers to PR outfits. Journalism of even the most rudimentary investigative nature will become impossible.

The second part of this provision talks about "spreading confusion". Without specifying the meaning of "confusion", it may become a weapon of media harassment. What is confusing to one may not be confusing to another. This will surely create a new avenue to intimidate the media.

Then again, what constitutes damaging the "image/ reputation" of the State? Recently we have reported about the corruption in the banking sector by unscrupulous business groups. We have reported that the banks face grim crisis. Does it constitute damaging the "image/ reputation"? We have reported corruption in the law enforcement agencies. We have reported on "custodial deaths" "disappearances", and "extra-judicial killings". If someone interprets all these reports as damaging the "image" of the State then this law lagalises punishment of journalists and newspapers for making such reports as all newspapers have websites.

Section 28

If in any website or electronic system publishes or broadcasts anything that hurts religious values and religious sentiments etc:

1) if any person or group deliberately and knowingly and with the intention of hurting religious values or sentiments or with the intention to provoke such sentiment publishes or broadcasts information then such actions will be considered a crime.

Sampadak Parishad's Comment:

The term "religious sentiment" is a very undefined term. How can a reporter know how and when religious sentiment has been hurt? This term lends itself to diverse interpretations and no journalist will feel comfortable about reporting on such issues. This will prevent journalistic scrutiny over a large area of the society. The recent reporting on the sexual harassment by Catholic priests would not have been possible if those countries had a law preventing reporting that "hurts" religious sentiments. Criticizing unlawful fatwa or women's property rights may be interpreted by some as "hurting" their religious values. This section can lead to widespread harassment of journalists.

Section 29

Publishing and distributing defamatory information, etc.

1) If a person publishes or distributes any defamatory information mentioned in Section 499 of the Penal Code (Act XLV of 1860) on a website or any other electronic format, they will get a maximum penalty of 3 years in jail or Taka 5 lakh in fine, or both.

Sampadak Parishad's Comment:

A law already exists to deal with defamation and so a separate law for digital media is not needed. Moreover, there is no logic for enhanced penalty for digital media from print media for the same crime.

Section 31

Crimes and penalty for deterioration of law and order, etc

(1) If a person deliberately publishes or broadcasts onS a website or any digital platform anything that creates enmity, hatred or acrimony among different classes or communities, or upsets communal harmony, or creates unrest or chaos, or causes or begins to cause deterioration in law and order, then that activity of the said person will be considered a crime.

Sampadak Parishad's Comment:

A news concerning discrimination about Dalits, or ethnic groups and exploitation of disadvantaged groups may be interpreted as causing disaffection between different groups. Any news highlighting plights of the people of Chittagong Hill Tracts may be interpreted as "creating unrest" among different communities. Similarly, news about possible labour unrest, impending hartal or demonstration can be construed as reports that are "creating law and order situation" and thus bring action under this law. There could be a story that a person has died in a demonstration which may later prove to be untrue. Will the media be "guilty of spreading rumour"? Such errors regularly occur in reporting which are corrected immediately. In Bangladesh, death figures from floods, cyclones or even roads accidents vary. Government figures are always at variance with privately gathered figures. In such cases according to the DSA media can be sued for "spreading rumour". Sometimes reports may forecast certain developments which may not exactly happen later. That also can be considered as "spreading rumour". Thus we find this section as seriously jeopardizing freedom of journalism.

Section 32

Offence and penalty for breach of Official Secrets

(1) If a person commits a crime or assists someone in committing a crime under the Official Secrets Act, 1923 (Act No. XIX of 1923) via a computer, digital device, computer network, digital network or any other digital media, they will get a maximum penalty of 14 years in jail or Tk 25 lakh in fines, or both.

(2) If a person commits a crime mentioned in the sub-clause (1) for a second time or repeatedly, they will be sentenced to life in prison or a maximum fine of Tk 1 crore, or both.

Sampadak Parishad's Comment:

This is a sweeping restrictive law from the colonial times that was promulgated to protect the British administration from any sort of accountability. It is shocking to see it being incorporated for digital platforms. Anything that is not made public by the government is deemed an "Official secret". Let us take one example. We have published dozens of reports about bank defaults based on Bangladesh Bank's findings. All such reports can be said to have violated the official Secrets Act. All government

reports which have not been made public, say, on pollution or child nutrition, are a part of the Official Secrets Act. Is journalism of any worth possible without the use of such official reports? And why should using them be a "crime" as people have a "Right to Know" under the RTI Act, especially when all such reports are funded by public money.

Could we have done any of the reporting on default loans, gross irregularities in Farmers 'Bank or Basic Bank without Bangladesh Bank or government departments' reports which were yet to be made public? And our reporters often use their mobile phones to take pictures of such documents. So they can be thrown into jail for up to life-term, right?

Proponents of this law may find our examples to be "ludicrous". But real life examples from the use of Section 57 of the ICT Act give journalists no reasons for comfort.

Section 43

Search, Seizure and Arrest without Warrant

(1) If a police officer has a reason to believe that a crime under this law has been or is being or will be committed in any place, or there is a possibility of it happening, or if there is a possibility of evidence being lost, destroyed, deleted or altered or being made scarce in some other way, then the officer, upon putting in writing the reason for his/her belief, can undertake the following tasks:

(a) Enter and search the said place and, if intercepted, take necessary action in accordance with the Code of Criminal Procedure;

(b) Seize the computer, computer systems, computer network, data and information or other objects used in committing the crime or documents that can help prove the crime while conducting a search in the said place;

(c) Bodily search anyone present in the said place;

(d) Arrest anyone present in the said place if suspected of committing or having committed a crime under this law.

Sampadak Parishad's Comments

This is by far the most dangerous of the provisions of the law.

This empowers the police to enter any premises, search any computer system, seize any computer network and its servers, bodily search anybody and also arrest anybody on suspicion.

First, the threat of arrest without warrant will naturally prevent a journalist from doing their work. When the police get the power to arrest without warrant, and on mere SUSPICION then media freedom will be buried under this law. Given the fact that 14 out of 20 provisions of punishment are NON BAILABLE the threat of arrest becomes like the "Damocles' Sword" constantly hanging over the head of every

journalist, causing mental stress. This will prevent all forms of real journalism and make our media nothing more than public relations and propaganda outlets.

Even if the law is not implemented (and why not if the law exists?) the environment of fear will prevent journalists from doing their job. The fear of arrest will become a regular part of the "mental environment" and debilitate a journalist from taking legitimate risks that he or she regularly takes to file their stories. The "emotional stress" that it will create should not be underestimated. It can easily be expected that people in power will abuse this law, provoke or "manage" law enforcers to threaten or even arrest journalists for any story that will reveal something that the rich and powerful will want to hide.

The most dangerous side of this law is that since every newspaper and TV station works on digital system, by giving the power to confiscate a computer, a network of computers including servers, the law enforcing agencies have been given, in effect, the power to shut down a newspaper or TV station or a news portal by confiscating its computers, computer system, computer network and other equipment. Thus without closing down a media outlet, this clause opens up the possibility of stopping the publication of a newspaper or the operation of a TV station by the law enforcing agencies.

Section 53

Offenses those are cognizable and bailable. In this law

(a) Sections 17, 19, 21, 22, 23, 24, 26, 27, 28, 30, 31, 32, 33 and 34 are cognisable and non-bailable offenses and

(b) Section 18, and sub-section (1) (B) 20, 25, 29 and 48 sub-clause(3) are non-cognisable and bailable.

SampadakParishad's Comments

Under this law out of 20 or so provisions dealing with crimes and punishment, 14 are cognisable and non-Bailable. Given the fact that police have the power to arbitrarily arrest without warrant and on mere suspicion, this law presents a real threat to media freedom as so many offences have been made cognizable and non-bailable.

Conclusion

1. The DSA clearly violates the citizens' Constitutional Right to Freedom of Speech and Expression and freedom of the press, within reasonable restrictions, guaranteed in the most sacred document, the Bangladesh Constitution.

2. This law violated the spirit of the Liberation War and the high ideals of freedom that our martyrs laid down their lives for.

3. This law is against the fundamentals of democracy, democratic governance and all the rights that our people fought for repeatedly during our struggle

against the Pakistani rule and against all martial law regimes after 1971.

4. The Digital Security Act is against all the fundamental values of ethical and independent journalism.

5. The Digital Security Act is in contradiction with the Right to Information Act.

We have explained in detail and made a section by section analysis as to why the Digital Security Act is against the Constitution, against our Fundamental Rights, against freedom of speech and freedom of journalism and as such against democracy.

It is thus that the Sampadak Parishad is forced to reject this law.

Last but Not the Least, The internet has proven its revolutionary power in respect to the practice of freedom of speech and expression. Through this amazing technology, anybody can express their thoughts and ideas to the whole world. But this has also created room for abuse. Cyber-bullying, cyber-attacks, plotting against a particular person or group or framing the innocent using the news or social media is becoming more and more common. Strict laws such as the Information and Communication Technology Act or the Digital Security Act might be the answer or the efforts to find an answer to this atrocity. But it can also not be denied that these possible 'answers' are creating more 'questions', as there are socially proven evidences of these laws being misused.

The present situation of Bangladesh is very much paradoxical in this regard. On the one hand, the government is promising the people and also trying to establish a Digital Bangladesh. And on the other hand, it is implementing laws such as the ICT and Digital Security Act with severe loopholes which can easily be manipulated to repress free public use of the digital advancements. It is taking steps such as barring Facebook or tuning down the internet speed on different situations, which goes totally against the concept of a Digital Bangladesh.

Nevertheless, there is a saying: "With great power, comes a great responsibility". Freedom of expression and the vastness of the internet, both are excessive powers; but so is the power of governing a country where the citizens and the mass media can feel free.

6. CONCLUSION AND RECOMMENDATIONS

This analysis shows the rights to freedom of expressions severely restricted in Bangladesh through unjust and unreasonable laws that also in many cases criminalizes such freedoms and impose disproportionate punishments. We recommend the government of Bangladesh should rethink and reshape related legal and policy frameworks to uphold the right to freedom of expression in online spaces. Although Section 57 of the ICT Act is repealed, however, the provisions of the Digital Security Act are more of same nature. These provisions also do not conform to international standards for the protection of freedom of expression. The government should also consult with various UN mechanisms, including the UN Special Rapporteur on the promotion of the right to freedom of opinion and expression to ensure the Digital Security Act conforms to international standards.

We recommend the following changes to the Digital Security Act.

Section 38 should be amended to provide simply that service providers are not responsible for content as long as they have not intervened in the content or been ordered by a court to remove it. At a minimum, the burden should rest on the party bringing a criminal prosecution against a service provider to show that they were aware of the offence.

Sections 22-24 should be removed. The provisions on forgery, fraud and fraudulent impersonation in the Penal Code should be reviewed and, if they fail to cover the commission of these crimes online, they should be amended to address those lacunae.

Sections 17(1)(a) and 18(1)(a) should either be removed (with the types of harm in section 18(1)(b) being expanded) or have intent and harm requirements added. Section 32 should be limited in scope to those who are under a primary obligation to respect government confidentiality (i.e. normally officials) and those who directly, illegally and intentionally access it, and it should also include a public interest override to protect whistleblowers.

An intent requirement should be added to Section 33 and it should include protection for whistleblowers.

Section 34(a) should be removed and an intent requirement should be added to section 34(b).

Section 19 should apply only where the person does not own the computer in question or have lawful access to it. Section 19(1)(a) should be removed, section 19(1)(e) should be limited in scope along the lines suggested above and consideration should be given to the purpose of section 19(1)(f) and whether or not it is needed.

Section 20 should be limited in scope to cases where the person does not have lawful access to the computer and where the action causes harm or damage of some sort.

Consideration should be given to whether Section 26 belongs in the Act at all and, a requirement of intent should be added.

A clear intent requirement should be added to Section 27. Consideration should be given to whether section 27(1)(c) should be removed from the Act. Section 27(1)(d) should either be removed or fundamentally revised so that it focuses on illegitimate activities which should in fact be prohibited.

7. REFERENCES

ASK. (2013). ICT (Amendment) Act, 2013: Right to Information and Freedom of Expression under Threat. Dhaka. Retrieved from http://www.askbd.org/ask/wp-content/u loads/2013/10/ICT-Act-Mahbub.pdf

GoB. National Telecommunications Policy 1998 (1998). Bangladesh: The Ministry of Posts, Telecommunications and Information Technology, Government of the People's Republic of Bangladesh. Retrieved fromhttp://www.btrc.gov.bd/sites/default/files/telecom_policy_1998_0.pdf

GoB. National Information and Communication Technology (ICT) Policy 2002 (2002). Bangladesh: Ministry of Science and Information & Communication Technology, Government of the People's Republic of Bangladesh. Retrieved from http://www.btrc.gov.bd/sites/default/files/ict_policy_2002_0.pdf

GoB. Information and Communication Technology Act 2006, Pub. L. No. Act 39 of 2006 (2006). People's Republic of Bangladesh: Ministry of Law, Justice and Parliamentary Affairs. Retrieved from http://bdlaws.minlaw.gov.bd/bangla_pdf_part.php?id=950

GoB. National Broadband Policy 2009 (2009). Bangladesh: Ministry of Posts, Telecommunications and Information Technology, Government of People's Republic of Bangladesh. Retrieved from http://www.btrc.gov.bd/sites/default/files/national_broadband_policy_2009_0.pdf

GoB. International Long Distance Telecommunications Services (ILDTS) Policy 2010 (2010). Bangladesh: Ministry of Posts, Telecommunications and Information Technology, Government of People's Republic of Bangladesh. Retrieved from http://www.btrc.gov.bd/sites/default/files/ildts_policy_2010_english_0.pdf

GoB. Digital Security Act 2018 (2018). Ministry of Law, Justice and Parliamentary Affairs.

Oozeer, A. (2014). Internet and social networks: freedom of expression in the digital age. Commonwealth Law Bulletin, 40(2), 341–360. Retrieved from https://doi.org/10.1080/03050718.2014.909129

VOICE
VOICES FOR INTERACTIVE CHOICE & EMPOWERMENT

CELEBRATING 20 YEARS