EngageMedia

ICT Policies and Implications on Digital Rights: South and Southeast Asian Context

JULY 2023

In collaboration with

NEWS NETWORK

CCIM cambodian center for independent media

SOCIETY FOR PEACE&DEMOCRACY

Digital Rights Nepal

Out of The Box MEDIA LITERACY INITIATIVE

#GENERATION பரපුර தலைமுறை

EngageMedia is a nonprofit that promotes digital rights, open and secure technology, and social issue documentary. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights.

Learn more at engagemedia.org.

News Network envisions a nation where citizens are aware of their rights, enjoy freedom of expression, dignity of life and gender equality and where the media is free. We promote democracy, freedom of press and expression, human rights, right to information and help media people improve their skills and encourage and equip women to take up journalism.

The Cambodian Center for Independent Media (CCIM) envisions a Cambodian society where everybody is well-informed and empowered to strengthen democratic governance and respect for human rights. CCIM believes that a well-informed Cambodian society will expect and demand good governance, and select leaders that will shape the society and economy in a way that will benefit the Cambodian people equitably.

Society for Peace and Democracy is a non-government organisation that empowers communities through awareness-raising and capacity-building to act and to participate in their own development. Through education and training, the organisation develops knowledge and skills, providing opportunities to advocate for improved policies to ensure human rights, inclusion and collective actions.

Digital Rights Nepal is a not-for-profit initiative dedicated to the protection and promotion of digital rights in Nepal. It focuses on digital rights issues such as right to online freedom of expression and association, online privacy, access to information, internet governance, cyber laws/policies, and cyber security. DRN is engaged in policy research and advocacy, public awareness campaigns, capacity building initiatives, and creating platforms to provide technical support, in collaboration with relevant stakeholders.

Out of The Box Media Literacy Initiative, Inc. is an educational nonprofit that creates innovative learning tools and experiences that foster media-literate Filipinos. It was awarded First Prize in the 2021 Global Media & Information Literacy Awards of the UNESCO MIL Alliance.

Hashtag Generation is an antiracist, feminist movement led and run by a group of young, tech-savvy Sri Lankans working towards building a society where everyone has the skills, information, and tools to be active participants in making the decisions that affect their communities, technologies, and bodies. Hashtag Generation mobilises digital media tools to raise awareness and catalyse dialogue on important social justice issues.

Project Lead

Phet Sayo, Executive Director, EngageMedia

Research Oversight

Vino Lucero, former Digital Rights Project Manager, EngageMedia

Prapasiri Suttisome, Project Officer, EngageMedia

Siti Rochmah Aga Desyana, Project Assistant, EngageMedia

Reviewer

Shabnam Mojtahedi, Legal Advisor, International Center for Not-for-Profit Law (ICNL)

Report Editor

Katerina Francisco, Editorial Coordinator, EngageMedia

Country Partner Reports

Bangladesh - News Network: Rezaur Rahman Lenin

Cambodia - Cambodian Center for Independent Media: Piseth Duch

Maldives - Society for Peace and Democracy: Mohamed Shumais and Adam Shareef

Nepal - Digital Rights Nepal: Santosh Sigdel, Rukamanee Maharjan, Saurav Bhattarai, Sadichchha Silwal

Philippines - Out of The Box Media Literacy Initiative, Inc.: Alex Valte

Sri Lanka - Hashtag Generation: Nethmini Medawala and Kalpani Ratnayake

Published July 2023

This report has been produced by EngageMedia as part of the Greater Internet Freedom project work in South and Southeast Asia.

TABLE OF CONTENTS

Executive Summary

Introduction

In South and Southeast Asia, the use of information and communication technologies (ICT) has exploded to unprecedented growth. More people in the region are using digital platforms to exercise their democratic rights. However, as people transition into more active online activities, they are also exposed to online threats like disinformation, fraud, online harassment, and data breaches.

EngageMedia, under the Greater Internet Freedom project conducted with Internews and supported by USAID, collaborated with six digital rights organisations to produce this qualitative research report titled "ICT Policies and Implications on Digital Rights: South and Southeast Asian Context", which aims to assess the digital rights impact of ICT-related laws and policies in select South and Southeast Asian countries.

Findings from the Focus Countries

The six countries studied in this research lack comprehensive forms of ICT-related laws and policies that can adequately guard against digital rights violations. Current laws contain vague and overbroad provisions open to interpretation, enabling authorities to weaponise these laws to stifle free speech. The current policies also carry risks of facilitating greater state surveillance and granting excessive powers to the state, with little independent oversight. Some of the country-specific findings that we found are:

Executive Summary

- Bangladesh: The Digital Security Act (2018) remains the most influential law for digital rights in the country, with its vague provisions and broad definition of authority enabling the government to arbitrarily arrest dissenters.
- Cambodia: The Law on Telecommunications (2015), its Sub-decree, and the Inter-ministerial Prakas 170 on Website and Social Media Processing vested excessive and arbitrary powers to the government, allowing authorities to target individuals for their commentary online.
- Maldives: The existing legal framework does not have a specific ICT policy or law, therefore creating policy gaps and a lack of attention to current and emerging challenges.
- Nepal: While the Electronic Transactions Act (2008) and the Individual Privacy Act (2018) are intended to help ensure legal norms for the security, protection, and deterrence of crimes and harms, concerns regarding the lack of scope and specificity in the provisions highlight a legal loophole that might not address all digital rights issues.
- Philippines: The Anti-Terrorism Act (2020) and SIM Registration Act 2022 may potentially be used to promote state surveillance, endangering actual lives in addition to the criminal penalties of fines and jail time.
- Sri Lanka: The recently-enacted Personal Data Protection Act (2022) raises concerns among journalists and civil society organisations as it challenges the right to access information under the Right to Information Act (2016), which is instrumental to exercising the right to free speech and expression.

Executive Summary

Regional Trends

The findings in the focus countries point to a larger trend of using digital tools and laws to infringe on human rights. In the regional outlook, we observe three themes shared by the six focus countries:

Restrictions on freedom of expression

ICT and cybercrime laws in the six countries contain provisions that allow for the restriction of speech under certain conditions, but these are currently vague and ill-defined. According to the International Covenant on Civil and Political Rights' three-part test for the validity of restrictions on freedom of expression, restrictions are legitimate only if they (a) are prescribed by law; (b) serve a legitimate aim; and (c) are necessary for the protection or promotion of the legitimate aim. When assessed under this test, various laws in the region fail to satisfy these conditions. With vague provisions, these laws can be used to harass, intimidate, or penalise those expressing opinions critical of the state.

Mass Surveillance

Provisions in the various ICT laws in the focus countries grant surveillance power to authorities in the name of public security but at the risk of privacy infringement. The laws lack clarity on who has access to people's personal information, and for how long the data will be stored, which implies expanded state surveillance and content censorship – infringing on people's right to privacy and right to information.

Executive Summary

Inadequate policymaking processes

The policy gaps and risks to freedom of expression and data privacy are indicative of the lack of public consultation in the policymaking process. These laws do not adequately reflect the needs and interests of the public. The country reports note that the needs of vulnerable groups are not sufficiently covered. Current legislation also lacks specificity in transparency and grievance mechanisms, making these inadequate to address emerging challenges in the digital rights space.

Recommendations

Safety and freedom in the digital space are fundamental to exercising one's digital rights. If one is to be active in public discourse, make informed decisions, and contribute to democratic processes, various stakeholders have a responsibility to take more initiative to guarantee freedom in digital spaces amid a context where new laws are enacted in a restrictive manner.

Therefore, governments in the six focus countries should amend laws that hinder the utmost protection of digital rights and fundamental freedoms online. Effective safeguards to uphold freedom of speech, the protection of personal data, and the right to privacy must be implemented.

Executive Summary

For researchers and academia, there is a need to conduct studies and launch programs to cultivate a community of passionate advocates who can help raise consciousness about the importance of protecting and expanding users' right to free expression online.

For human rights defenders and civil society, the urgency to come together to confront these challenges and demand for the greater protection of rights is even more pronounced. Raising awareness and deepening public understanding of these laws' impact on fundamental freedoms online and offline is critical in the advocacy for better safeguards of digital rights.

Regional Outlook

Introduction

The past decades have seen the rapid growth of internet use and digital technologies across South and Southeast Asia. Across the region, more people are turning to platforms to exercise their democratic rights: to express political dissent, gather support for mass movements, and call for social change. Governments too have recognised the clear need for information and communications technology (ICT) for national development, and – as the COVID-19 pandemic has shown – to facilitate resilient and sustainable economic recovery. But as people's lives and activities increasingly move to online spaces, they are also more exposed to digital dangers, such as disinformation, online harassment, cybercrime, digital security issues, and data privacy breaches.

To respond to the attendant challenges in a fast-evolving digital landscape, governments have sought to enact various rules, guidelines, and policies to provide legal frameworks governing ICT and digital spaces. In theory, these laws are well-intentioned: to protect the public against cybercrime, provide roadmaps for the country's ICT development, and crack down on harmful content and hate speech, among others. Yet the reality of implementation suggests that these laws are all too often weaponised by governments to maintain control over the population by curbing dissent, stifling free expression, expanding state surveillance, and other forms of creeping digital authoritarianism.

Methodology

EngageMedia collaborated with six digital rights organisations to produce this research report titled "ICT Policies and Implications on Digital Rights: South and Southeast Asian Context", which aims to assess the digital rights impact of ICT-related laws and policies in select South and Southeast Asian countries. The report aims to increase public awareness

Regional Outlook

of the digital rights implications of these various legal frameworks. By better understanding these laws and how they impact fundamental rights and freedoms, civil society actors, human rights defenders, and digital rights advocates would be better positioned to demand greater transparency and accountability from both public and private actors and push for critical amendments and the creation of more rights-respecting solutions.

This report is informed by local inputs from six countries – Bangladesh, Cambodia, the Maldives, Nepal, the Philippines, and Sri Lanka – under the Greater Internet Freedom project. The following digital rights organisations produced the respective country reports:

- News Network (Bangladesh)
- Cambodian Center for Independent Media (Cambodia)
- Society for Peace and Democracy (Maldives)
- Digital Rights Nepal (Nepal)
- Out of The Box Media Literacy Initiative, Inc. (The Philippines)
- Hashtag Generation (Sri Lanka)

The report is qualitative, relying on both primary and secondary data as its sources. The country reports analyse and interpret legal documents such as legislation and policies; previous research reports; news articles; and personal accounts from both experts and direct stakeholders to understand the context and draw conclusions about the matter. This regional outlook synthesises the overall findings and provides an analysis of regional trends.

Regional Outlook

Overall Findings

The six countries studied in this research lack comprehensive forms of ICT-related laws and policies that can adequately guard against digital rights violations. Current laws contain vague and overbroad provisions open to interpretation. Already, these laws have been used – and abused – and cited as the basis behind the legal cases and arrests filed against those expressing speech that the state deems offensive. Current policies also carry risks of state surveillance and granting excessive powers to the government, with little independent oversight.

Restrictions on Freedom of Expression

ICT and cybercrime laws in the six countries contain provisions that allow for the restriction of speech that threatens national security, but these are currently vague and ill-defined. According to the International Covenant on Civil and Political Rights' three-part test for the validity of restrictions on freedom of expression, restrictions are legitimate only if they (a) are prescribed by law; (b) serve a legitimate aim; and (c) are necessary for the protection or promotion of the legitimate aim.

When assessed under this test, various laws in the region fail to satisfy these conditions. This can be seen in Cambodia's law on telecommunications which does not sufficiently define 'national security', and in the Philippines' Anti-Terror Law, which fails to meet the standard for the third test.

Regional Outlook

With vague provisions, authorities can apply their own interpretations and use the laws to penalise those expressing opinions critical of the state. This was especially rampant at the height of the COVID-19 pandemic, which saw 'fake news' laws being wielded against those expressing discontent over their governments' pandemic mismanagement and hundreds of cases and arrests made against journalists, activists, and ordinary citizens. Such laws can also be used to avoid the legal process of obtaining a search or arrest warrant, as in the case of Sri Lanka where the Computer Crimes Act has been used to stifle critical content.

These policies may normalise a climate of censorship and reinforce a chilling effect among the public, undermining democratic expression.

Mass Surveillance

Provisions in the ICT laws grant surveillance power to authorities in the name of public security but at the risk of unduly infringing on people's rights to privacy. The laws lack clarity on who can access people's personal information, for which purposes, and for how long data will be stored. These were the very issues behind criticism of the Philippines' SIM Card Law, which was intended to curb phone-facilitated cybercrime but may instead endanger activists through expanded state surveillance. Cambodia's proposed National Internet Gateway, which would direct all internet traffic through a regulated gateway, also presents a danger of both mass surveillance and censorship as authorities may block content it deems offensive.

Regional Outlook

Inadequate Policymaking Processes

The policy gaps and risks to freedom of expression and data privacy are indicative of the lack of public consultation in the policymaking process. These laws do not adequately reflect the needs and interests of the public that such legislation will impact. The country reports note that the needs of vulnerable groups are not sufficiently covered, putting these already marginalised groups at risk of being subjected to more harms. In some cases, there are no specific provisions explicitly spelling out digital rights (Maldives), or policies related to ICT are fragmented and embedded in various laws and not in one comprehensive law (Nepal).

Current legislation also lacks specificity in transparency and grievance mechanisms, making these inadequate as legal deterrents or bases to address emerging challenges in the digital rights space.

It is telling how many of these laws have found use in times of crisis, such as elections in Cambodia, protests in Sri Lanka, and the COVID-19 pandemic across the region. Many people have been arrested and detained based on these laws, with national security being cited as the basis for what in reality is a restriction on free speech. Human rights defenders and the public must come together to confront these challenges and demand for the greater protection of rights. Raising awareness and deepening public understanding of these laws' impact on fundamental freedoms online and offline is critical in the advocacy for better safeguards of digital rights.

COUNTRY REPORTS

BANGLADESH

NEWS NETWORK[1]

Since 2000, Bangladesh has gradually adjusted to the Internet Age. The idea behind 'Vision 2021'[2] and 'Digital Bangladesh'[3] has resulted in the government moving many of its functions online. Moreover, the number of people and businesses relying on technology continues to grow. Digital platforms have made it easier to pay for services, organise protests, sign petitions, and write about civic issues. However, online criminal activity has also flourished, necessitating measures to protect people. In recent years, the Bangladesh government has passed a number of measures related to information and communication technology (ICT); however, these cyber laws – particularly the ICT Act 2006 and the Digital Security Act (DSA) 2018 – have curtailed people's digital rights in the following ways:

1. News Network prepared this draft in cooperation with Mr. Rezaur Rahman Lenin, an academic activist from Dhaka, Bangladesh.
2. The Government of Bangladesh has declared 'Vision 2021' with a target to make Bangladesh a middle-income country using Information and Communication Technology (ICT) and the development of a favourable business environment for innovative companies. http://bhtpa.portal.gov.bd/sites/default/files/files/bhtpa.portal.gov.bd/page/8f8ac427_fca2_4875_bf9a_65051666d011/Mission%20&%20Visson.pdf
3. The Constitution of People's Republic of Bangladesh, art 39.

- The arbitrary blocking of websites and the criminalisation of legitimate freedom of expression;
- The filtering and temporary restriction of internet content;
- The attempt to restrict online media through commercial pressure;
- The arrest, detention, and attempt to criminalise legitimate expression;
- Self-regulation and cultural norms protect against censorship;
- The lack of protection for personal data

According to Article 39 of the Constitution, each citizen has the right to freedom of expression, speech, and the press[4]. However, in recent years – and especially during the COVID-19 pandemic – the government of Bangladesh has been cracking down on these freedoms to regulate the flow of information and suppress people's ability to freely express their views. Beyond undue restrictions on civil and political rights, many people who have been detained or arrested have reported feeling socially humiliated, losing their social standing, and concerned about being falsely accused of crimes again.

This research aims to determine and analyse significant national cyber laws that are of concern because of their effect on digital rights in Bangladesh. This report is based on desk research and heavily relies upon primary and secondary online resources, which include journal articles, reviews, reports, newspapers, and academic books. The study also collected opinions and synthesis from influential national human rights defenders and civil society representatives for analysis. A list of recommendations has been proposed outlining next steps for advocates, policymakers, and the general public.

4. The Constitution of People's Republic of Bangladesh, art 39.

Cyber Laws in Bangladesh

On October 8, 2006, the Bangladesh parliament passed the Information and Communication Technology (ICT) Act 2006[5]. This Act aims to create the requisite legal framework to ensure that all transactions and other activities conducted electronically are treated with the same level of respect as paper-based ones. Sanctions for activities in cyberspace did not exist before the enactment of this law (later amended in 2009 and 2013).

In May 2015, the government began implementing a new regulatory statute, the 'Cyber Security Act', without consulting or receiving input from digital rights defenders and their organisations[6]. The Ministry of Posts and Telecommunications adopted the "National Cyber Security Strategy" (NCSS) and Information Technology on March 11, 2014[7]. They presented the Global Cyber Security Agenda at the International Telecommunication Union. It is written in English rather than following the Bangla Bhasha Procholon Ain 1987 (literally, the "Bangla Language Implementation Act, 1987"), which requires the use of the Bangla language in all records and correspondences. Sections 9 and 10 of the NCSS mandated a plan to "Enhance Bangladesh's Cyber Laws to Address Current and Emerging Threats", necessitating the passage of new legislation like the Digital Security Act[8].

In 2018 the Ministry of Information and Communication Technology formulated an ICT Policy[9], which emphasises the need for Bangladesh to work towards establishing an ICT infrastructure that can meet the country's socioeconomic needs and promote innovation. The policy also aims to improve access to, and use of, ICTs by vulnerable groups.

The Bangladesh National Assembly also passed the "Digital Security Act 2018"[10] by voice vote, despite strong opposition from journalists, lawyers, educators, and human rights activists.

5. https://ictd.gov.bd/site/view/policies/Policy-
6. Rezaur Rahman Lenin, 'Law Review; Digital Security Act 2018 And Questions Of Citizens' Basic Human Rights - শুদ্ধস্বর' (শুদ্ধস্বর, 2021) https://shuddhashar.com/law-review-digital-security-act-2018-and-questions-of-citizens-basic-human-rights/ accessed 18 January 2023.
7. Md. Riaz Uddin THE NATIONAL CYBERSECURITY STRATEGY OF BANGLADESH: A CRITICAL ANALYSIS https://www.biliabd.org/wp-content/uploads/2021/09/Md.-Riaz-Uddin.pdf
8. Ibid.
9. Ibid.
10. Digital Security Act 2018 http://bdlaws.minlaw.gov.bd/act-1261.html

In recent years, the government under the ruling Bangladesh Awami League has proposed three new laws, rules, and policies. These measures, if passed, pose significant risks to digital rights[11]:

1. Data Protection Act, 2022, which will require international platforms to store data locally with a national security agency headed by a government official acting as the data protection authority. The law will leave user data originating from Bangladesh vulnerable to government abuse due to this arrangement.
2. The Regulation for Digital, Social Media And OTT Platforms 2021, which will mandate platforms to remove a broad range of content within 72 hours of notification and have Bangladesh-based employees ensure compliance with the law.
3. Draft of the 'OTT Content-based Service Provision and Management Policy 2021,' which will be a similar regulation to the Social Media And OTT Platforms regulation drafted by the Ministry of Information.[12]

Analysis of the Information and Communication Technology Act (ICT) Act, 2006

Contents of the ICT Act

Bangladesh approved the ICT Act on October 8, 2006. It seeks to legalise all electronic data and activities. The Act addresses electronic records and signatures, their security, the institution that issues electronic certificates, the punishments for computer and internet offenses, and cyber tribunals and cyber appeal tribunals.

---

11. https://freedomhouse.org/country/bangladesh/freedom-net/2022
12. https://www.dw.com/bn/%E0%A6%AA%E0%A7%8D%E0%A6%B0%E0%A6%B9%E0%A6%B8%E0%A6%A8%E0%A7%87%E0%A6%B0-%E0%A6%AE%E0%A7%81%E0%A6%96%E0%A7%87-%E0%A6%AE%E0%A6%A4%E0%A6%AA%E0%A7%8D%E0%A6%B0%E0%A6%95%E0%A6%BE%E0%A6%B6%E0%A7%87%E0%A6%B0-%E0%A6%B8%E0%A7%8D%E0%A6%AC%E0%A6%BE%E0%A6%A7%E0%A7%80%E0%A6%A8%E0%A6%A4%E0%A6%BE-%E0%A6%93-%E0%A6%AE%E0%A7%8C%E0%A6%B2%E0%A6%BF%E0%A6%95-%E0%A6%AE%E0%A6%BE%E0%A6%A8%E0%A6%AC%E0%A6%BE%E0%A6%A7%E0%A6%BF%E0%A6%95%E0%A6%BE%E0%A6%B0/a-61782884

Chapter I of the Act covers ICT industry and cyber regulation terms. Chapter II covers e-governance and provisions on electronic signatures. Chapter III addresses electronic record attribution, acknowledgement, and transmission. Chapter IV regulates safe electronic records and digital signatures. Chapter V governs certifying authorities. Chapter VI discusses security, digital signature certificates, private control, and acceptance. Chapters VII and VIII cover penalties, adjudication, inquiry, judgment, and punishment for several offenses. Chapter VIII creates the Cyber Regulations Appellate Tribunal to review Adjudicating Officer orders.

Bangladeshis have suffered digital rights violations under the ICT Act, especially sections 46 (Power of Controller to give directions in emergencies) and 57 (Punishment for publishing fake, obscene or defaming information in electronic form). The law especially targets journalists; according to reports published by media platform Prothomalo in 2020, 46 cases against journalists have proceeded to the Cyber Crimes Tribunal over the last three years, of which only four cases were eventually dismissed[13]. According to human rights activist and researcher Rozyna Begum, the law has also been widely used before the 2014 national election. Section 57 of the ICT Act, which criminalised online defamation and blasphemy and silenced dissenters, was of particular concern.

The ICT Act was later replaced by the 2018 Digital Security Act, which eventually repealed ICT Act Sections 54, 55, 56, 57, and 66. Interestingly, the DSA has more repressive penalties, making it harsher than repealed section 57 of the ICT ACT 2006[14].

---

13. https://www.prothomalo.com/bangladesh/%E0%A6%A1%E0%A6%BF%E0%A6%9C%E0%A6%BF%E0%A6%9F%E0%A6%BE%E0%A6%B2-%E0%A6%A8%E0%A6%BF%E0%A6%B0%E0%A6%BE%E0%A6%AA%E0%A6%A4%E0%A7%8D%E0%A6%A4%E0%A6%BE-%E0%A6%86%E0%A6%87%E0%A6%A8%E0%A7%87-%E0%A6%97%E0%A7%9C%E0%A7%87-%E0%A6%AA%E0%A7%8D%E0%A6%B0%E0%A6%A4%E0%A6%BF%E0%A6%A6%E0%A6%BF%E0%A6%A8-%E0%A6%A4%E0%A6%BF%E0%A6%A8-%E0%A6%AE%E0%A6%BE%E0%A6%AE%E0%A6%B2%E0%A6%BE

14. Ibid.

Controllers' Discretionary Power

Section 46 of the original ICT Act allows the Government to order any law-enforcing agency to restrict information through any computer resource if they believe it is necessary or expedient for maintaining Bangladesh's sovereignty, integrity, or security, its friendly relations with other States, public order, or the prevention of any cognisable offense. Controllers are government-appointed. Section 46 allows a controller to offer emergency orders. Rights groups say Bangladesh has invoked Section 46 to justify website blocking and filtering[15].

This clause is exceedingly problematic for various reasons, including the controller's vast discretionary powers. Section 46's title implies that the power should only be used in emergencies, yet it does not define emergencies. Instead, it refers to numerous broad goals, some of which are not permissible under Article 19 (3) of the International Covenant on Civil and Political Rights (ICCPR), such as preserving cordial ties with other States or deterring criminal activity. Thus, Section 46 allows a public authority (the controller) to undertake surveillance or restrict information access in many scenarios.

In addition to the difficulties described above, it is unclear why the entity governing the certification authority should have surveillance tools and the capacity to ban internet access. Law enforcement should do the first under court supervision, and the courts should order the second. Section 46's provisions violate international law and should be eliminated. If the Bangladeshi government wants to provide law enforcement or intelligence services with more monitoring capabilities, it should do so through international law-compliant legislation.

15. Information and Communication Technology Act, 2006 s 46

Encouraging Pre-trial Imprisonment

It is concerning that section 76 of the updated ICT Act[16], which bars bail for certain offenses, violates the right to liberty and may further erode the presumption of innocence required by international law. Article 9 of the ICCPR specifies that "it shall not be the general rule that persons awaiting trial shall be kept in custody," protecting the person's liberty and security. International law also allows states to jail people before trial merely to ensure their appearance or preserve evidence. The ICT (Amendment) Act 2013's non-bailable Section 61[17] offenses violate Article 9(3) of the ICCPR.

The International Criminal Court worries that lengthy pre-trial imprisonment puts individuals at risk of torture. According to human rights groups, Bangladeshi police routinely torture detainees, as in the 2020 cases of journalist Shafiqul Islam Kajol, cartoonist Ahmed Kabir Kishore, and the late writer Mushtaq Ahmed, with Ahmed eventually dying in detainment.

Immunity of the Intermediaries

The Act grants internet service providers (ISPs) immunity for any activity that breaches the Act and uses them as intermediaries. Section 79 clarifies that no network service provider shall be liable under this Act or rules and regulations made thereunder for any third-party information or data made available by him if he can show that the offense or contravention was committed without his knowledge or that he had used all reasonable efforts to prevent such crime or contravention. ISP immunity poses the risk of facilitating an increased commission of cybercrime.

Unwarranted Arrest and Criminal Procedures

The Act allowed police to undertake warrantless searches and arrests in public. Per Section 80, the Act argued that requiring a warrant for search and arrests in private places takes time and risks secrecy, and the need for warrants is replaced by a letter of consent from the

16. Information and Communication Technology Act, 2006 s 76
17. Information and Communication Technology Act, 2006 s 51

relevant unit head. Warrants require a thorough legal justification to be made for arrest and search, and the elimination of such may allow for arbitrary arrests to be made on baseless allegations.

Provisions in Conflict with Public Interest Principles

According to Section 63, it is a crime to violate the ICT Act's powers or "rules and regulations made thereunder." Since this provision prevents confidential information from being disclosed without authorisation, this research report agrees that limiting its application to public officials exercising statutory powers is permissible. The provision is troubling, however, when applied to whistleblowers who expose corruption or other serious wrongdoing. Additionally, it is unclear whether one or more private individuals could be considered "a person" who obtains information under this Act or its rules and regulations. If so, such a provision is wildly disproportionate. Additionally, this provision should be in the data protection law rather than the ICT law because it protects personal data during automated processing.

It should also be noted that Section 4 of the Public Interest Disclosure (Protection) Act, 2011, states: "Any disclosure of information may, in reasonable consideration, disclose accurate information relating to the public interest." Under Section 5 of this Act, the publisher of accurate public interest information cannot be a victim of a criminal or civil case, demotion, harassing transfer or compulsory retirement, taking any other departmental action, discriminatory behaviour, etc., and the informant's identity must be kept secret. Thus, the current ICT Act contradicts the Public Interest Disclosure Act 2011, which must be addressed by legislative and adjudicative bodies to avoid legal confusion.

Insufficient Data and Privacy Protection

Article 43 of the Constitution states: "Every citizen shall have the right, subject to reasonable restrictions imposed by law in the interests of the security of the State, public order, public morality or public health- (a) to be secured in his home against entry, search and seizure and (b) to the privacy of his correspondence and other means of communication."[18]

Surveillance and national security, especially terrorism, are closely linked in Bangladesh. To protect state security and public peace, Section 97A[19] of the Telecommunication Act of 2001 allows the government to authorise any of its authorities to record, prevent, and collect telephone communications. This provision also states that the government may request assistance from any service provider, which must comply or face penalties.

The Telecom Act allows data collection without a warrant or court order. The 2006 amendment confirms this surveillance regime. According to the Code of Criminal Procedure and the ICT Act, an investigating police officer can intercept and monitor communication and request network administrator cooperation. Anyone who refuses to help may be penalised.

Judiciary, Judges, and Unjust Justification

Section 82(1) of the ICT Act requires the government to establish one or more Cyber Appellate Tribunals[20] to expedite and effectively prosecute ICT Act-related offenses. The government and Bangladesh Supreme Court will choose a session judge or assistant session judge for the cyber tribunal. The first very rapid cyber-tribunal was established in Dhaka in 2013. By April 2021, the government had established cyber tribunals in all seven divisions to hear cybercrime cases, including those filed under the Digital Security Act.

18. Information and Communication Technology Act, 2006 s 43
19. Bangladesh Telecommunication Act, 2001 s. 97 (A)
20. Information and Communication Technology Act, 2006 s 82 (1)

One needs a deep understanding of computer applications in information technology to resolve issues under IT laws. The tribunal must understand digital signatures, cryptography, and IT developments[21]. It is recommended that the government ensure that a technical member (with a computer science background) is part of the tribunal to ensure that correct IT concepts are applied. The ICT Act, however, does not specify any requirements regarding ICT understanding for the selection of tribunal judges, raising concerns from digital rights activists, professionals, and lawyers over the qualifications of judges appointed to such tribunals.

The Act created the Rajshahi Cyber Tribunal, which Md. Ziaur Rahman presided over in September 2021. Most of the cases handled by this tribunal were based on the now-repealed Section 57 of the ICT Act 2006 and brought to trial years later. Section 57 was frequently used to prosecute the dissemination of false, obscene, defamatory, and seditious information, carrying a 14-year sentence and a TK 1 crore fine.

This report finds the Rajshashi Cyber Tribunal's judicial conduct in two cases alarming: the cases of State v Md. Golam Rasul and State v Md. Akter Hossain, in which rulings were issued on September 28, 2021, and September 20, 2021, respectively.

In State v. Md. Golam Rasul, the defendant was found guilty of mailing obscene photos of the victim to village residents in January 2017. The defendant was imprisoned and fined TK 50 Lacs. In September 2015, Md. Akter Hossain was found guilty of publishing obscene photos of Bangladeshi Prime Minister Sheikh Hasina and former Indian Prime Minister Manmohan Singh. He received a TK 1 Lac fine and seven years of hard labour. A closer look at both judgment documents shows striking errors, overlapping evidence, and impartial judge observations. Forensic experts examined the defendants' mobile phones to determine if they owned and published the photos. Despite being adjudicated over a week apart, both defendants' cell phone models and numbers were the same. This error suggests the judge's negligence and taints the tribunal's two decisions.

21. Information and Communication Technology Act, 2006 s 74

The Supreme Court of Bangladesh has a judicial code of conduct to ensure a functional and ethical judiciary. However, Judge Rahman has shown subjective opinion; in State v. Md. Akter Hossain, he called the defendant a "political propaganda activist" based on how he used his personal Facebook account, implying a subjective opinion not based objectively on the evidence. In State v. Md. Golam Rasul, Judge Rahman spent over two pages discussing the impact of disseminating obscene photographs of women rather than the defendant's guilt based on the evidence.

Judge Rahman made several impactful and well-reasoned observations in both cases about the effects of crimes under the repealed Section 57 of the ICT Act 2006. Still, his handling of the cases raises concerns about thousands of other Bangladesh cyber tribunal cases.

Analysis of the Digital Security Act (DSA), 2018

The Bangladeshi government introduced the DSA to protect the country's critical information infrastructures from cyberattacks, with little regard for privacy, security, freedom of expression, and other human rights. The DSA aims to ensure national digital security and protect against online content deemed to harm the nation, but its vague provisions allow authorities to stifle free expression. It also gives authorities broad powers, such as the power to arrest people and search premises without a warrant, requiring only the suspicion that a crime was committed using digital media.

Ambiguity and Poor Definitions

Section 17 of the DSA imposes punishment for “illegal access to any critical information infrastructure, etc.” but Section 2(g) which defines "critical information infrastructure" is not clearly defined[22]:

22. Digital Security Act, 2018, s 2 (g)

"critical information infrastructure" means any external or virtual information infrastructure declared by the Government that controls, processes, circulates or preserves any information-data or electronic information and, if damaged or critically affected, may adversely affect

(i) public safety or financial security or public health,
(ii) national security or national integrity or sovereignty;

Securitization of 'Institutional Arrangements'

The DSA is supposed to protect the state's critical information infrastructures from cyberattacks. "The agency"— the Digital Security Agency— will provide security with one Director General and two directors. The Act designs that, given its purpose, the agency will have full access to all computer systems and can digitally order data deletion.

Section 8(1) of the DSA states that the Director-General can request the Bangladesh Telecommunications and Regulatory Authority (BTRC) to remove or block data that threatens digital security. Section 8(2) states: "Law and order enforcing Security Force may request BTRC to block or remove the data-information via the Director-General of the Agency if it is evident that any data-information published or propagated in digital media hampers the nation or any part thereof in terms of nation's unity, financial activities, security, defence, religious values, public discipline, or incites racism and hatred." Sections 8(1) and 8(2) require the BTRC to notify the government of any Director-General request and immediately block or remove the requested data[23].

Section 8 does not comply with Article 19 of the ICCPR because it is vague about the type of data that is prohibited online. Overly vague provisions grant arbitrary power to authorities to enforce the DSA in ways that could prevent protected speech if authorities consider such speech to affect national unity, such as criticism of government policies or media reports about corruption. Moreover, Section 8 can have a chilling effect on speech, encouraging Bangladeshi netizens to self-censor, filter, and restrict content online to avoid having their sites blocked.

23. Digital Security Act, 2018, s 8

Section 8 is also disproportionate in both its language and application. According to international law standards, a judicial or impartial agency without political, commercial, or other conflicts of interest must decide on what content is prohibited. If it is possible to remove the harmful content without blocking the entire website, the government should not have the authority to block an entire site, online platforms, and instant messaging, as it is likely to be disproportionate and is in violation of Article 19 of the Universal Declaration of Human Rights. However, the DSA lacks such a clause and instead enabled the BTRC to block or filter any website without notice or justification. The government has not listed blocked websites or provided justifications for why they have been blocked.

According to Section 56 of the DSA, the Director-General may, if necessary, “delegate any power or responsibility entrusted to him under this Act to any employee of the agency and any other person or a police officer by written order." This section's syntax suggests a specialised delegation of power, which may allow massive abuse of power. The question remains whether the authorised person or persons have the knowledge or skills to carry out such broad powers.

Vague Cybersecurity Attack Definition and Emergency Response Team (ERT)

Section 9 of the Act establishes a National Computer Emergency Response Team, which should be composed of digital security experts and law enforcement. Section 9(5) states that the ERT must: (a) ensure the emergency security of critical information infrastructure; (b) act quickly to stop cyberattacks and security lapses; (c) take the necessary precautions to stop potential and impending cyberattacks, and (d) cooperate with a comparable foreign team or organisation with government approval. What constitutes a cyber or digital attack is unclear. An agency can act immediately to address a "cybersecurity breach," but with a lack of evidence, this power is likely to be abused to stifle reporting on government misdeeds.

Criminalisation of Legitimate Forms of Expression

Section 21 of the DSA 2018 penalises propaganda against the Father of the Nation, the national anthem, the national flag, or the Liberation War with a 10-year prison sentence, a 1-crore-taka fine, or both. Repeat offenders face life in prison, a Tk 3 crore fine, or both. First, since Bangladesh does not have a single authority to interpret or explain the "cognition or spirit of the liberation fight," this law could target those with opposing views. This law may hurt people who view the liberation struggle differently.[24] The law would also discourage independent history researchers and could penalise anyone conducting historical research and coming up with interpretations different from that of the ruling authority or other parties. Article 19(3) of the ICCPR does not allow such justifications for limiting free speech. Similar to the blasphemy law, this law essentially forbids people from having their own beliefs.

Section 28(1) of the law states: "Any person or group who intentionally or knowingly hurts religious sentiments or values, or provokes the publication or broadcast of such content on any website or electronic format, commits an offense. If such an offense is committed, the person will be sentenced to 7 years in prison, a 10 lac fine, or both."[25] ICCPR Article 19(3) protects public morals. No single entity should dictate public morality in a multi-ethnic and multi-cultural society like Bangladesh.

The DSA thus hinders religious or free speech, especially those who disagree with mainstream religions or express their views on religious issues. Thus, "religious sentiments or attacks on religious values" in this context may endanger people's diverse religions and beliefs.

Minors have frequently been detained for allegedly offending the religious sentiment of others. On October 29, 2020, a 17-year-old was held in a juvenile detention facility due to a Facebook post that allegedly intended to denigrate the Quran and offend devout Muslims. She was recently granted bail after spending one and a half years in the juvenile detention

24. Digital Security Act, 2018 s 21
25. Digital Security Act, 2018 s 28

facility in Rangpur. This was her fifth attempt to request bail in court. Meanwhile, 20 children and teenagers aged 13 to 17 have been victims of at least 18 reported cases across 12 districts.[26]

Online and offline defamation punishments differ significantly. Section 29(1) of the DSA states: "As defined in Section 499 of the Penal Code (Act XLV of 1860), a person who publishes or broadcasts defamatory information in any website or other electronic format will be sentenced to three years in prison, five lac taka in fine, or both. If a person commits the offense a second or subsequent time, he will be sentenced to five years in prison, ten lac in fines, or both." Meanwhile, under the Penal Code, defamation is punishable by two years in prison, a fine, or both.

International law mandates that fines and penalties, especially those involving freedom of expression, should be proportionate to the crime. "A person, media outlet, political or other organization may not be subjected to sanctions, restraints, or penalties for a security-related crime involving freedom of expression or information that are disproportionate to the seriousness of the actual crime," states Principle 24 of the Johannesburg Principles on National Security, Freedom of Expression, and Access to Information. According to Principle 46 of the Tshwane Principles on National Security and the Right to Information: "Criminal penalties for the unauthorized disclosure of information to the public or persons should be proportional to the harm caused"[27].

---

26. https://www.prothomalo.com/bangladesh/%E0%A6%B6%E0%A6%BF%E0%A6%B6%E0%A7%81-%E0%A6%95%E0%A6%BF%E0%A6%B6%E0%A7%8B%E0%A6%B0%E0%A7%87%E0%A6%B0%E0%A6%BE%E0%A6%93-%E0%A6%AE%E0%A6%BE%E0%A6%AE%E0%A6%B2%E0%A6%BE-%E0%A6%A5%E0%A7%87%E0%A6%95%E0%A7%87-%E0%A6%B0%E0%A7%87%E0%A6%B9%E0%A6%BE%E0%A6%87-%E0%A6%AA%E0%A6%BE%E0%A6%9A%E0%A7%8D%E0%A6%9B%E0%A7%87-%E0%A6%A8%E0%A6%BE

27. https://www.justiceinitiative.org/publications/tshwane-principles-national-security-and-right-information-overview-15-points#:~:text=June%202013-,The%20Tshwane%20Principles%20on%20National%20Security%20and%20the%20Right%20to,and%20national%20law%20and%20practices.

Sections 17 (illegal access to crucial information infrastructure), 18 (illegal access to computers, digital devices, computer systems, etc.), 19 (damage to computers, etc.), and 20 cover several offenses (change of computer source code). Three provisions stand out. First, criminal and public-interest hacking are treated the same. Secondly, the international cybercrime convention does not include all DSA crimes. The DSA has trouble clearly defining crimes and tracking criminal intent, thus providing a broad authority that allows law enforcement to punish internet users under several Digital Security Act 2018 provisions.

DSA Section 18(1) states, "Any person who knowingly and unlawfully enters or assists in entering any computer, computer system, or computer network, or computer to commit a crime, shall be guilty of an offense under this Act."[28] This clause violates the Johannesburg Principles[29], which states that no person may be punished on national security grounds for disclosure of information if (a) the act is unlikely to harm a legitimate national security interest and (b) the public interest in knowing the information outweighs the harm from the disclosure. Section 18(1) makes it a crime to gain unauthorised access to a computer, computer system, digital device, or system to learn about or disclose information or data that is in the public interest. This section will discourage reporting government agency corruption, misconduct, or crime.

Human rights organisations have uncovered a worrying trend in which people detained under the DSA for criticising the government are denied bail and held in pre-trial detention for periods longer than is permitted by the law. When cases brought under the DSA constitute a human rights violation, including excessive limitations on the right to freedom of expression or invasion of privacy, there are no protections under the law for people to seek compensation. As a result of the police's failure to complete the investigation within the 75 days required by section 40 of the Act, many individuals have been held without charge or trial for an indefinite period.

---

28. Digital Security Act, 2018 s 18.
29. https://www.article19.org/wp-content/uploads/2018/02/joburg-principles.pdf

The United Nations High Commissioner for Human Rights, Michele Bachelet, criticised the DSA after author Mushtaq Ahmed passed away in custody on February 25, 2021. Bachelet added: "Bangladesh urgently needs to suspend the application of the Digital Security Act and conduct a review of its provisions to bring them in line with the requirements of international human rights law."[30]

Since January 2020, the Centre for Governance Studies (CGS) has tracked and documented the cases filed under the DSA. Until December 30, 2022, the CGS has been able to track the details of 1,109 cases. These data were gathered from government-approved print and electronic media; the accused or their family and friends; the lawyer of the accused; and police stations and other concerned departments.[31] According to the data collected by the website named "DSA Tracker", 1,109 cases were filed under the DSA, of which around 60% were related to Facebook activities. A total of 2,889 individuals were accused. Of them, only 52 saw their cases coming to a close within the court system. Around nine others found some relief only because their accusers withdrew the cases against them. Meanwhile, police are still investigating three-quarters of the thousand or so cases, according to CGS's data.[32]

According to a UN Report of the Special Rapporteur for Freedom of Expression, a three-part test is used to assess whether limitations to free speech are justified: (i) the limitation must be provided for in law; (ii) it must pursue a legitimate aim; and (iii) it must be necessary for a legitimate purpose.

Bangladeshi cyber laws often fail this three-part test, specifically point III regarding necessity. The DSA, for example, contains provisions penalising content engaging in “propaganda” against the "spirit" of the 1971 Bangladesh war of independence and content criticising state symbols such as the national flag, anthem, and founders. The government has full liberty in interpreting what elements constitute such violation due to the vague

30. https://www.ohchr.org/en/2021/03/bangladesh-bachelet-urges-review-digital-security-act-following-death-custody-writer

31. https://freedominfo.net/

32. Ibid.

wording of the Act, thus allowing hyperbolic interpretations to be made as a basis for criminal allegations. The Act is often used to stifle free speech and force community members to self-censor[33]. The government blocked several websites, including YouTube, in early March 2009; in 2020, it blocked the website The Wire after it published an article on the role of the military intelligence agency in the illegal pick-up and secret detention of university academic Mubashar Hasan.

Conclusion

Cyber laws are being enacted to secure long-term political power and silence dissenters. These undermine a democratic political environment and endanger digital rights and online freedoms. These abuses have been exacerbated by the introduction of the contentious Digital Security Act of 2018, which the government uses as a weapon against journalists, writers, artists, and freethinkers who express dissent online. The situation has worsened as measures have been implemented to restrict and monitor online activity to exert more control over users' online behaviours.

In this situation, Bangladesh needs to implement effective protection strategies for digital rights like free speech online and offline, protection of personal data, and the right to privacy, all in line with international human rights norms and practices. There is also an urgent need to conduct studies and launch programs to cultivate a community of passionate advocates who can help raise consciousness, primarily in Bangladesh, about the importance of protecting and expanding users' right to free expression online.

Recommendations for the Government

- Ensure that various stakeholders are consulted before any cyber-related legislation or policy is approved by the cabinet or passed in parliament;
- Overturn controversial provisions in laws that infringe on human rights and are incompatible with the Constitution. In this light, sections 21, 25, 29, and 31 of the DSA Act should be repealed or amended to provide a clear definition of the digital crimes mentioned in the Act.

33. https://www.newagebd.net/article/201824/dsa-acts-as-deterrent-to-journalism-tib

- Ensure that Bangladesh satisfies its international obligations by bringing its internet policy in line with the prerequisites of international law and principles. This will guarantee that the internet continues to serve as an open public forum for people to exercise their right to freedom of expression online.
- Ensure any restrictions placed on the right to free expression adhere to the three-part test, which states that the restriction must be prescribed by law, that it must achieve one of the specified, legitimate aims, and that the restriction must be necessary for and proportional to the achievement of that aim.
- End the harassment against social media users expressing critical opinions.
- Drop charges and release from detention those arrested for exercising their right to freedom of expression, and end unlawful arrests and detentions.
- Increase technical awareness and capacity training for law enforcement agencies to reduce abuse of power.
- Restrict intelligence agencies' ability to access individuals' private communications; such access should be granted by a court order.
- Publish annual reports on legal actions taken by government agencies as a transparent measure to reduce the abusive use of such laws against activists, journalists, civil society representatives, and individuals' freedom of expression.
- Provide digital literacy education to marginalised communities to prevent the spread of disinformation.
- Create a new data protection law that conforms to the highest standards of international practice to give citizens greater control over their personal information.
- Create new laws or amend existing ones to ensure victims of human rights abuses, such as censorship or invasions of privacy, have access to effective remedies and reparations.
- Invite the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to carry out an independent assessment of the situation in Bangladesh.

CAMBODIA

CAMBODIAN CENTER FOR INDEPENDENT MEDIA (CCIM)

A surge in the use of the internet and social media, namely Facebook, was evident during the 2013 national elections which was considered to be a close contest between the ruling party and the main opposition party. At the time, an NGO report estimated that at least 74,000 Cambodian people between the ages of 18 and 30 were using Facebook to communicate socially or politically, with internet subscribers standing at about 3,861,979 in 2013. As of 2022, Cambodia has a total population of just over 17 million. Based on numerous reports, the country has about 13.44 million internet users and 12.6 million social media users, with Facebook users standing at 11.60 million, followed by TikTok users at 6.68 million.

This rapid growth of online and social media provides a unique opportunity for the general public to engage in democratic debates, exercise their rights to fundamental freedoms, in particular freedom of expression and diversity of public discourse, and hold duty-bearers accountable.

Although Cambodia commits to adhere to international human rights law and respect and protect the civil and political landscape of the country, recent events also observed by the United Nations Special Rapporteur on the situation of human rights in Cambodia

unfortunately suggest that this is not the case. The Cambodian government has been restricting and controlling the flow of information, cracking down on the already shrinking civic space both offline and online through arbitrary arrests and detention, and prosecuting political opponents and dissidents, journalists, human rights defenders, activists and others for allegedly disseminating "fake news" and "hate speech". It has also used the COVID-19 pandemic as an excuse to impose aggressive cyber-policing, virtual private network blockages, partial or total internet shutdowns, and increased online surveillance. In 2022, Cambodia was ranked 142 out of 180 countries in the Reporters Without Borders Press Freedom Index, dropping from 128 in 2016. In 2022, Freedom House also indicated that Cambodia was 'partly free' in terms of freedom on the net with scores of 43/100. This portrays the gradual shrinking of the civic space and increased restrictions on the freedoms of expression, association, press, and access to information and the internet.

In July 2012, the United Nations Human Rights Council unanimously approved a resolution to protect human rights online, with the reaffirmation that "the same rights that people have offline must also be protected online" and acknowledged how the Internet can be an "important tool for development and for exercising human rights".

The adoption of the Law on Telecommunications and its relevant Prakas as well as the Sub-decree on the Establishment of the National Internet Gateway (Sub-decree on NIG), which are the main focus of this research, have raised serious concerns about human rights and fundamental freedoms. In this regard, the research is intended to provide a brief legal analysis of the Law on Telecommunications and the Sub-decree on NIG on key issues around surveillance, the right to privacy, restrictions to the freedom of expression, and grievance and safeguarding mechanisms. The analysis also assesses their compatibility with international human rights law and standards. Inputs from key civil society leaders and digital rights advocates are incorporated throughout this research. Immediate consideration should be given to the review of the Law on Telecommunications and Sub-decree on NIG together with civil society members, digital rights experts, and relevant stakeholders in public meaningful forums, to repeal or amend problematic provisions that are not in line with international human rights law.

Law on Telecommunications and Inter-ministerial Prakas 170 on Website and Social Media Processing

Overview

In 2015, Cambodia adopted the Law on Telecommunications as part of the government's efforts to strengthen and expand critical digital infrastructure development under its rectangular strategy phase 4. Despite the purpose of the Law aiming to develop Cambodia's telecommunications sector and protect users, some problematic and controversial provisions exist that appear to curtail human rights and fundamental freedoms, particularly the rights to freedom of expression and privacy, which have led local and international human rights experts to suggest that the existing Law is not fully compatible with international human rights and standards.

The Law has been weaponised as a tool against free speech and political participation. While the Law itself has not been used to criminalise freedom of expression, its relevant prakas (official declaration), namely an Inter-ministerial Prakas 170 on Publication Controls of Website and Social Media Processing via the Internet in Cambodia, issued jointly by the Ministry of Post and Telecommunications (MPTC) – a government-mandated body to draft and oversee the implementation of the Law – has proved problematic. A brief analysis of the Prakas will also be focused on in this report to demonstrate the Cambodian government's intention in introducing the Law and the Prakas before elections and how they have been used to restrict press freedom.

The most problematic provisions of the Law that are the main focus of this analysis include the excessive powers of surveillance given to the government, potential abuses of the rights to privacy and data protection, and restrictions and criminalisation of freedom of expression.

Surveillance powers and the right to privacy

The Law's stated main aim is to not only provide a framework for the legal and industrial regulation of the telecommunications sector of the country but also to protect users. It is, however, tailored to empower the government to surveil electric communications without safeguards or independent oversight, making no reference whatsoever to the internationally protected rights to freedom of expression and privacy of correspondence through telecommunications.

Article 6 of the Law states that the "MPTC shall have competence to control telecommunications, information and communication technology service data and newly established services in accordance with the technological development in this sector. All telecommunications operators and persons involved with the telecommunications sector shall provide to MPTC the telecommunications, information and communication technology service data". The unfettered authority given to the MPTC to demand the provision of data on users from all telecommunications service providers appears to be excessive and could lead to misapplication of the Law arbitrarily. Practically, this could also mean that telecommunications service providers are obliged to share the personal data of their users with the government without a requirement of a judicial decision. In the absence of a robust data protection law, this is a human rights concern.

Moreover, Article 97 of the Law permits covert listening and recording of dialogue by using any telecommunications system but only requires approval from a 'legitimate authority' which remains undefined. This could lead to arbitrary interpretation and a high likelihood of being abused for politically motivated reasons if this provision is not narrowly and precisely defined. As it stands, this Article is not compliant with the best practices of restrictions under international human rights law and standards.

The surveillance powers granted to Cambodian law enforcement are already troublingly broad and unaccountable. Article 70 of the Law grants 'telecommunications inspection officials', who are also judicial police officers, the power to "study, observe, monitor, prevent, and crack down on telecommunication offenses" without judicial oversight or procedural safeguards.

Despite Article 65 (b) claiming to protect the basic rights of users/subscribers by recognising their "rights to privacy, security and safety of using the telecommunications service", this protection appears to lack substantive value in practice as it may be superseded by the following phrase: "… otherwise determined by other specific laws." This exceptional clause appears unconstitutional as the "right to privacy of residence, and to the secrecy of correspondence by mail, telegram, fax, telex and telephone" is protected by Article 40 of the Constitution. A lack of precision in the language found in Article 65 is also not consistent with Articles 12 of the Universal Declaration of Human Rights (UDHR) and 17 of the International Covenant on Civil and Political Rights (ICCPR), with the UN Human Rights Council's resolution in 2019 also reaffirming equal protection of the right to privacy offline and online. A case in point to demonstrate an abuse of power to target critics is found in the case of environmental activists and opposition politicians who were charged in connection to comments made during a Zoom and private telephone conversation, respectively.

Restrictions and criminalisation of freedom of expression

Despite its binding national and international human rights obligations to observe freedom of expression, there have been problematic provisions of the Law on Telecommunications that appear to curtail the rights to freedom of expression and even criminalise legitimate free speech online.

Article 66 of the Law prohibits the "establishment, installation, utilization, and modification of telecommunication infrastructure and network or establishment, installation, and utilization of equipment in telecommunication sector which may affect public order and lead to national insecurity…" In addition, Article 80 of this Law stipulates criminal imprisonment sentences from seven to 15 years in the event that the same prohibited acts stated in Article 66 lead to "national insecurity". It criminalises any expression that is made via electronic communication if it is deemed to be promoting "national insecurity", irrespective of the intention. Furthermore, imposing heavy imprisonment sentences on the vague and overbroad language of the Law is neither necessary nor proportionate. In the absence of a well-defined term for "national insecurity", these legal provisions appear to fall short of the three-part test contained in Article 19(3) of the ICCPR of being provided for

by law, serving a legitimate interest, and being necessary to protect that interest. Also, the Human Rights Council has explicitly stated that "vague and overbroad justifications, such as unspecified references to "national security" do not qualify as adequately clear laws".

Another troubling provision of the Law on Telecommunications is Article 99 designed to criminalise telecommunications activities by introducing imprisonment sentences from six months to two years and heavy monetary fines for "any act of producing, installing or distributing software or hidden audio recorders for recording dialogue" without approval from the competent authorities. Such an over-broadly defined provision could see the criminalisation of the basic use, sharing, or development of software such as smartphone apps or digital platforms for legitimate purposes should the government or authorities deem it so. Again, this is neither necessary nor proportionate when it comes to permissible restrictions on freedom of expression (both offline and online) under international human rights laws and standards.

Despite the Law on Telecommunications having not been used widely to target dissenting voices, within just two months before the July 2018 national elections the MPTC, the Ministry of Information, and the Ministry of Interior passed an Inter-ministerial Prakas 170 on Publication Controls of Website and Social Media Processing via the Internet in Cambodia (the "Prakas"). The Prakas is aimed at regulating the publication of all news content or written messages, audio, photos, videos, and/or other means intended to create turmoil, leading to the undermining of national defence, national security, relations with other countries, the national economy, public order, discrimination, and national culture and tradition on websites and social media. The Prakas grants excessive power to government agencies for unchecked, systematic mass surveillance of online activities and is not compatible with permissible restrictions on the right to freedom of expression under Article 19 of the ICCPR. The Prakas also enables the Cambodian government to block or close websites and/or social media pages containing illegal content that is deemed to be "incitement," breaking solidarity, discrimination, and willfully creating social chaos that undermines national security, public interest, and social order. Without clearly and narrowly defined terms used in this Prakas and the Law, it would leave open the possibility of arbitrary interpretation and thereby lead to misapplication, which appears inconsistent with the permissible restrictions under the ICCPR.

On 28 and 29 July 2018 during the national election days, internet service providers, for example, were ordered to block the services of 15 independent media outlets or news websites, including Cambodia National Rescue Party's website, Voice of America, Voice of Democracy, and Radio Free Asia. The media outlets were accused of "citing sources who disrupted the election and were abroad" in violation of election law.

General Comment No. 34 of the Human Rights Committee, which provides an authoritative guide on Article 19, states "the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds regardless of frontiers." This includes political discourse, journalism, public affairs, and canvassing, among others. Receiving and imparting unbiased and uncensored information is essential for the independent and unhindered functioning of the press and media, which directly correlates with the citizens' right to access information as embodied in Article 19, paragraph 2 of the ICCPR. This plane of rights is equally applicable to online and offline modes of information disbursal as reaffirmed by the UN Human Rights Council's resolution in 2019. The contemporary Cambodian civic and political landscape of attacks against journalists and human rights defenders and an atmosphere of fear and self-censorship is in direct contradiction with an unfettered democratic society.

General Comment No. 34 also outlines international standards on the right to freedom of opinion and expression, including press freedom. According to the Human Rights Committee, "[t]his implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion." In keeping with the Universal Declaration of Human Rights' protection of the individual as a recipient of information, the General Comment states that the public "also has a corresponding right to receive media output."

National Internet Gateway (NIG)

Overview

On 16 February 2021, the Cambodian Government adopted a Sub-decree on the Establishment of the National Internet Gateway ("Sub-decree" hereafter) initiated by the MPTC, which was intended to increase the effectiveness of national revenue collection, guarantee transparency between the state and operators, and prevent illegal cross-border network connections and online-related crimes as part of the government's long-term goal of establishing a digital government under the adopted Digital Government Policy 2022-2035.

According to the press release issued by the MPTC on 19 February 2021, consultations with experts, private operators, and relevant institutions were organised before it was adopted. However, there was no consultation with civil society nor were there avenues for them to raise concerns about the human rights implications of the Sub-decree, including the right to privacy, freedom of expression, and access to information. The right to privacy and freedom of expression are closely interlinked and mutually dependent.

The Sub-decree will have nationwide applicability, requiring all internet communications and internet data traffic circulating within and entering Cambodia to pass through a gateway and be routed through a regulatory body charged with monitoring online activity before it reaches users. Respective monitoring powers were given to the MPTC as well as to the Telecommunication Regulator of Cambodia. The Sub-decree was due to come into effect in mid-February 2022 but the government has postponed it to an unspecified date, citing the lack of equipment and the COVID-19 pandemic as reasons for the delay.

Despite the government's public intention of the Sub-decree having nothing to do with restrictions on human rights and fundamental freedoms online, UN independent human rights experts have raised legitimate concerns if the Sub-decree is implemented. The experts claimed that the Sub-decree would empower the government to conduct arbitrary mass data surveillance, undermining the right to privacy and curtailing the right to freedom

of expression in a democratic society. These concerns have been echoed by 62 civil society organisations as the Sub-decree would have a chilling effect on internet users in particular and society in general, given that excessive powers are granted to government agencies while it was drafted without consultation with civil society members/organisations.

This analysis will focus on the surveillance powers given to the government that potentially may have adverse effects on the right to privacy, criminalisation of freedom of expression, particularly online expression, and a lack of grievance and safeguarding mechanisms to guarantee full respect for human rights.

Restrictions on freedom of expression, opinion and information

The objective of the Sub-decree as stated in Article 1 is to "facilitate and manage internet connections for the enhancement of effectiveness and efficiency of the national revenue collection, protection of national security and the assurance of social order, national culture and tradition." It has nationwide applicability, covering all infrastructure and network operations and internet service operations.

Article 6 of the Sub-decree allows for blocking all online connections or content that are deemed to "affect safety, national revenue, social order, dignity, culture, traditions and customs". This means that the Cambodian government has been provided with excessive power to arbitrarily block and disconnect certain websites, domains, and broad swaths of the Internet because all data would have to pass through one centralised point. Overbroad terminology and ambiguous and undefined grounds for action may enable authorities to carry out widespread censorship of online content. With the power conferred by the Sub-degree, Cambodian authorities can potentially block any content or website it deems "illegal". The government had done this before as demonstrated in the above example; it would only take a shorter process to block or suspend critical online content with the NIG. A failure by any National Internet Gateway operator to comply with the Sub-decree will be subject to penalties through restrictions on, suspension of, or removal of their licence through the power vested in the Telecommunication Regulator of Cambodia in Article 16.

Inevitably, there appears to be a strong likelihood that the Sub-decree will put pressure on companies to comply with the government's requests at the expense of users' fundamental human rights.

Article 6 of the Sub-decree appears to be in contravention of the right to freedom of expression guaranteed by Article 41 of the Constitution of the Kingdom of Cambodia. The Constitution states: "Khmer citizens shall have freedom of expression, press, publication and assembly. No one shall exercise this right to infringe upon the rights of others, to affect the good traditions of the society, to violate public law and order and national security." Prima facie, without narrow and precise language within the permissible scope found in Article 6, it appears to go beyond the permissible restrictions to freedom of expression established in Article 19(3) of the ICCPR, which provides strict conditions by which the authorities may be able to restrict the enjoyment of these rights. The restrictions must be provided by law, imposed to respect the rights or reputations of others and for the protection of national security or of public order (ordre public), or public health or morals. These conditions must conform to strict tests of necessity and proportionality. Instead, Article 6 excessively expands without clearly and narrowly defined terms other than the permissible legitimate restrictions under Article 19 by including "safety", "national revenue", "culture", "traditions" and "customs" – the terms that should not be used to justify restrictions on freedom of expression under international human rights law. It, therefore, fails to satisfy the permissible restrictions of Article 19 of the ICCPR.

Surveillance powers and the right to privacy

Article 14 of the Sub-decree requires NIG operators to "prepare and maintain technical records and lists of allocated IP Address and identification of route of traffic through NIG, compile and maintain reports and relevant documents concerning the connections and all internet traffic, and provide other information as required by the MPTC and Telecommunication Regulator of Cambodia."

Article 14 of the Sub-decree raised concern on the right to privacy as it grants exhaustive power to NIG operators to monitor websites that people visit, as well as the metadata related to every website visit. If personal data is collected in a centralised internet traffic

and data mechanism under the NIG, sensitive personal information is likely to be susceptible to a cyber-attack, unauthorised access, or improper surveillance. The creation of the NIG also provides the infrastructure for massive, widespread electronic surveillance. Although the NIG is administered by the MPTC and the Telecommunication Regulator of Cambodia, in some cases, it may be shared with or administered by a third-party technology provider.

Article 14(3) of the Sub-decree also establishes a requirement for NIG operators to "maintain technical records, lists of the allocation IP Address and identification of route of traffic through NIG of the last 12 (twelve) months". This means that service providers are obliged to track the IP addresses of users and report them to the requisite government authorities. In an atmosphere that is increasingly unsafe for members of civil society, journalists, and dissenters, this provision is the final blow. Not only does it discourage dissenting opinions and independent media from being voiced, but it also invades upon the right to privacy that every citizen is entitled to. As observed by the Secretary-General, "digital surveillance, data retention, anonymity policies and technologies, data localization, and domain name blocking may have far-reaching and sometimes unintended consequences on media freedom and the safety of journalists."

Article 14 appears to be in clear contravention of Articles 12 of the UDHR and 17 of the ICCPR, which provides that "1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation and 2) Everyone has the right to the protection of the law against such interference or attacks." Articles 12 of the UDHR and 17 of the ICCPR also include the right to the protection of personal data, which, among other things, prevents states from requiring the mass retention of personal data by companies and access to personal data outside of clearly defined circumstances and subject to safeguards. The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be regulated by law as General Comment 16 stated.

Moreover, the UN General Assembly's Resolution in 2018 on the right to privacy in the digital age went on to dictate that "the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference and the right to freedom of peaceful assembly and association, and is one of the foundations of a democratic society." This provision must be reconsidered in earnest.

Overall, excessive and arbitrary power vested in the government by the Sub-decree for digital surveillance of private communications, censorship of online content, and mass data collection of users may severely intrude on people's right to privacy. Robust safeguards should be implemented to ensure that the government or companies that collect confidential private information of individuals for purposes that are not necessary, justifiable, and proportionate do not misuse any such measures. While some national legislation covering some aspects of data protection exist, in the absence of comprehensive data protection legislation these concerns appear legitimate. It was evident in how Cambodian authorities disclosed the personal data of individuals affected by COVID-19, leading to discrimination – a move which was criticised by UN independent human rights experts.

A lack of grievance and safeguarding mechanisms

Although Article 15 of the Sub-decree provides complaint mechanisms against any penalty measures taken by the Telecommunication Regulator of Cambodia, there is concern about the independent, fair, and transparent process of decision-making. With a lack of independent oversight bodies, it is unlikely that the Minister of Post and Telecommunications would overturn a penalty decision made by the Telecommunication Regulator, as its chairperson and members are appointed by the Cambodian government at the request of the MPTC. This is yet another example of legislation that provides a broad array of restrictive powers to the government to control online narratives and public opinion under the guise of public order and national security and integrity. While Article 15 provides a complaint mechanism, most fear that it will be ineffectual. Despite Cambodia being a signatory and committed to the ICCPR, this Sub-decree is in direct defiance of the Convention, more specifically Articles 17 and 19.

Conclusion

Restrictions to freedom of expression online are on the rise. Cambodian authorities target individuals for their commentary online while enacting new, restrictive digital-related laws and regulations – either existing or in draft forms. Cambodia's civic space has been constricted for a long time, but in recent years authorities have sought to shrink it even further. Robbing citizens of their fundamental freedoms has been a key tool for this suffocation of civic space and has led to the permeation of a culture of self-censorship and fear throughout society.

Despite international protection for human rights, these rights are often undermined in Cambodia as the country does not sufficiently uphold the rights to fundamental freedoms, while the government continues to enact laws that weaken their protection. Excessive and arbitrary power vested in the government by the Law on Telecommunications, the Sub-decree, and the Prakas for digital surveillance of private communications, censorship of online content, and mass data collection of individuals, may severely curtail human rights and fundamental freedoms and intrude on people's right to privacy.

Recommendations

To the government of Cambodia:

- Repeal or reform the Law on Telecommunications and Sub-decree on the Establishment of the NIG that interfere with fundamental freedoms, in particular freedom of expression online, to bring them in line with international human rights law and standards;
- Introduce robust safeguards, in particular adopting a comprehensive data protection law, to ensure that the government or companies that collect confidential private information of individuals for purposes that are not necessary, justifiable, and proportionate do not misuse such measures;
- Ensure that the process of drafting new laws (namely draft data protection, cybercrime, and cybersecurity laws) and amending existing ones is open and transparent, facilitating meaningful public participation from civil society and relevant stakeholders;

- Cease all ongoing criminal proceedings against human rights defenders, activists, journalists, political dissidents, protesters, and other individuals for exercising fundamental freedoms both offline and online;
- Create an enabling environment for civil society and the media to exercise their internationally protected human rights and fundamental freedoms and to enable them to operate freely and independently, particularly in the digital space;
- Cooperate effectively in good faith with the UN Special Rapporteur on the situation of human rights in Cambodia (UNSR) and other UN mechanisms on addressing human rights issues and implementing recommendations made by the UNSR and other UN bodies on restrictions on online freedom of expression.

To digital rights advocates and the general public:

- Raise greater awareness of the impacts of laws and policies on digital rights among the general public to foster healthy democratic discourse and gather support for concrete reform;
- Capacitate members of civil society and the public on mitigating risks when using digital devices and platforms for expressing views online;
- Increase programs of work focusing on digital rights and digital security and mobilise more funding to support the implementation of these programs, where applicable, in cooperation with other NGO partners;
- Continue to monitor and report on the government's enforcement of laws and policies on digital rights and advocate collectively for amendments to laws contrary to international human rights obligations through policy analysis, consistent dialogue with concerned authorities, and UN human rights mechanisms, including the Universal Periodic Review;
- Engage closely with the UN Country Team to have in-depth dialogues on the situation of digital rights, including freedom of expression in the digital age, and to identify effective solutions to address the issues of shrinking digital space.

MALDIVES

SOCIETY FOR PEACE AND DEMOCRACY

This report aims to analyse the progress in the Maldives' Information and Communications Technology (ICT) policy framework in relation to digital rights and civil society. The Maldives has experienced rapid growth in the telecommunications and ICT sector over the past 20 years, and the increased acceptance and usage of mobile data, together with the available ICT infrastructure in the country, has redefined the social and economic landscape of the Maldives.

The report will examine the Maldives ICT policy framework, including the Maldives Telecommunication Policy 2006, the Maldives Telecommunication Law (2015), Communications Authority Act (2015), Strategic Action Plan 2019, and Draft Cybercrime Act 2022. Through analysis of the documents and a survey questionnaire[1], this report will highlight the positive aspects of the framework and identify any gaps and areas in need of improvement. Finally, the report will provide recommendations for future research and policy development in the Maldives' ICT sector.

1. We requested ten key representatives in civil society to provide their views, and five representatives responded. Except for one, all respondents preferred not to disclose their identity.

Maldives Telecommunication Policy (2006)

The Maldives Telecommunication Policy 2006 was formulated to facilitate sustainable development of telecommunication services between 2006 and 2010 and given the economic and social development needs of the country. The policy identifies and addresses key issues in the sector in five major areas:

- Telecommunications charges shall be non-discriminatory, affordable, and cost-oriented.
- Telecom infrastructure shall be expanded and developed to provide basic, enhanced and broadband services throughout the country.
- The regulatory authority shall be autonomous by law with clearly defined powers and resources to effectively carry out its duties and protect the interests of both the consumers and the operators.
- The policy aims to establish a separate emergency telecommunication network in case of disaster.
- The policy aims to establish reasonable communication means for people with special needs.

The contents of the policy indicate that it aims to provide affordable and non-discriminatory telecommunication services and expand telecom infrastructure throughout the country, which can potentially benefit digital rights by making access to communication services more inclusive. The policy also includes provisions for an autonomous regulatory authority, which can ensure that the regulator can act independently in the best interest of both consumers and operators, potentially benefiting civil society by providing a space for them to cooperate. Additionally, it addresses the need for an emergency telecommunication network and communication means for people with special needs.

However, the policy does not specifically mention civil society. It also does not address the current and emerging challenges in the field of telecommunications, such as data privacy and security, net neutrality, and the need for digital literacy among citizens. Given the rapid advancements in technology and the increased importance of digital rights and civil society in the modern world, there may be a need to update the Maldives Telecommunication Policy 2006 to specifically address these issues. This would ensure that the policy is equipped to address the current and emerging challenges in the field of telecommunications and to protect the rights and interests of civil society concerning the use of technology. It would also reflect the current and future needs of the Maldives in the field of telecommunications, and ensure that the country can fully leverage the opportunities presented by technology for economic and social development.

The Maldives Telecommunication Law (43/2015)

The Maldives Telecommunication Law, which was ratified in 2015, comprises policies to be used in the design and implementation of all telecommunication-related activities in the Maldives. The Law includes matters related to issuing telecommunication licenses to service providers. It aims to promote a competitive environment for the provision of domestic and international telecommunication services. It also promotes national policy objectives for the telecommunications industry, which include making all telecommunications services more affordable, equitable, and competitive; developing telecommunications infrastructure and services to reduce the disparity between Malé and the rest of the Maldives; introducing, encouraging, and maintaining competition in telecommunications services; providing the Authority with the necessary means and powers to regulate the telecommunications industry in accordance with the national policy objectives; and developing and promoting information and communication technologies.

Emphasis on access to telecommunications services and the development of information and communication technologies are closely related to digital rights. For example, affordable and accessible telecommunications services can facilitate access to information and freedom of expression, which are key components of digital rights. Additionally, policies that promote competition and encourage the development of new technologies can potentially lead to a more diverse and robust digital ecosystem, which can in turn support the digital rights of citizens.

However, the Maldives Telecommunications Law does not specifically address the digital rights of civil society. Access to telecommunications services and the development of information and communication technologies are closely related to digital rights, but the Law does not provide any explicit protection for them. For example, it does not include any specific provisions or protections for the digital rights of civil society such as privacy.

Communications Authority Law (42/2015)

The Communication Authority Law of 2015 in the Maldives establishes an institution to set guidelines and administer all telecommunication and postal services in the country, as well as regulate "infocommunication" which the Law defines as ICT and telecommunication services. The Act states the responsibilities and jurisdiction of the institution, with the purpose of protecting the interests of the people in matters related to infocommunication, ensuring that telecommunications services provided are of good quality, competitive in international trade and meet the needs of society, promoting a competitive environment in the provision of telecommunications, postal services and infocommunication services, implementing national policies in the telecommunications and postal industries, and licensing telecommunications and postal service providers.

Concerning the digital rights of civil society, the Law is relevant in that it aims to protect the interests of the people in matters related to infocommunication and ensure that services provided are of good quality and meet the needs of society. However, it does not specifically address digital rights or the protection of civil society in relation to the use of

technology. The Law makes it clear that both ICT and telecommunication are to be regulated by the communication authority. The Law does acknowledge certain rights of individuals. For example, it states that if someone believes that their rights have been infringed by a decision of the Authority under the powers conferred by the Act, they can file a statement of reasons within 30 days of the Authority's decision.

Strategic Action Plan (2019)

The Maldives government introduced the Strategic Action Plan in 2019 as a guide for national development. Its purpose is to be used as a central policy framework and planning document, directing the development of the Maldives between 2019 and 2023 by combining government pledges with existing sectoral priorities. Section 3.4 is for community empowerment and civil society, while section 4.8 is for the ICT sector. The Strategic Action Plan includes the following policies in sections 4.8:

- Policy 1: Modernise the governance mechanism of the ICT sector to prepare the Maldives for a digital economy.
- Policy 2: Establish digital infrastructure, platforms, and ecosystems that are capable of providing ICT solutions that are more efficient, secure, and consistent.
- Policy 3: Modernise government services through digitalisation for data-driven policy-making and efficient delivery of information and services.
- Policy 4: Encourage digital innovation and create a conducive environment for businesses to thrive in a digital economy.
- Policy 5: Develop a digital-ready workforce and build human capacity in the ICT industry.

As per the contents, the Strategic Action Plan includes some policies that are relevant to the digital rights of civil society. These policies address the need for a clear and effective governance structure for the ICT sector, reliable and secure digital infrastructure, and efficient and accessible government services, which are all necessary for the protection of digital rights. The Strategic Action Plan also includes specific targets, such as the establishment of a National Help Desk and increasing interoperability between public and

private organisations, which can be used to measure progress and evaluate the effectiveness of the policies. These policies can potentially support the protection and promotion of digital rights for civil society. The Strategic Action Plan also includes a section on community empowerment that aims to create a dynamic CSO-Portal with an updated online database of civil society organisations and establish connections between all registered CSOs, which can assist CSOs to work smarter and more efficiently.

However, there are also gaps in the Strategic Action Plan concerning digital rights. It does not specifically mention digital rights in its content, meaning that the protection and promotion of digital rights may not be a direct focus of the Strategic Action Plan and may not be prioritised in its implementation. Additionally, while the policies outlined in the Strategic Action Plan address some important aspects of digital rights, they may not address all the important issues related to digital rights such as surveillance, data protection, and accessibility for disabled people. There are no specific measures or actions to counter digital rights violations and it is not clear how the government will monitor and report them.

Draft Cybercrime Act 2022

The Draft Cybercrime Act 2022 of the Maldives, drafted by the Attorney General's Office, aims to criminalise cybercrime and establish policies for the investigation and prosecution of cybercrimes in the country. The draft is not yet available to the public. However, information on the draft law has been shared in the media. According to media reports, the draft law proposes changes to the Penal Code, Criminal Procedure Code, and Act on Mutual Legal Assistance in Criminal Matters. If enacted, the draft law will give authorities the power to take action against crimes that involve electronic evidence. The proposed law criminalises and establishes penalties for acts such as unauthorised access to a computer system, an unauthorised inspection of computer data, misuse of a device, cyber violence, and acts of deception involving a computer. The Act on Mutual Legal Assistance in Criminal Matters will establish policies for mutual assistance in seeking electronic evidence and related matters and will set up a 24/7 network to provide real-time mutual assistance for

the investigation and prosecution of cybercrimes. The proposed changes to the Criminal Procedure Code will establish procedures for the retention of subscriber information and community data by service providers, quick preservation of stored computer data, and enforcement of production orders for computer data and subscriber information.

The Draft Cybercrime Act 2022 is relevant for the digital rights of civil society as it aims to address the increasing threat of cybercrime in the Maldives and protect citizens from cybercrimes. It provides for the criminalisation of various cybercrime activities and sets penalties for these activities. Additionally, the Act provides for the preservation of electronic evidence, which is essential for the investigation and prosecution of cybercrime cases.

However, it is important to note that the information relating to the draft law as reported in the media does not specifically mention civil society or their digital rights, and therefore it is still too early to understand the implications of the Draft Cybercrime Act.

Perception of Civil Society

According to key informants, there is a lack of awareness among Maldivians about ICT policies. Most respondents from civil society were not familiar with any policies related to ICT and did not have a clear understanding of how their work related to digital rights and human rights in the context of ICT policies. This highlights the need for greater awareness and education about ICT policies among civil society members.

The survey also revealed that the reasons or context behind the creation of ICT policies in the Maldives are not well understood. Some respondents believe that ICT policies were created to protect the country from different social issues, while others are not aware of the reasons behind their creation. However, one respondent indicated that the Telecommunication Policy (2006) was prepared during the reforms of former President Maumoon Abdul Gayoom who ruled the Maldives from 1978 to 2008. During his last term,

he introduced reforms to several governance issues including changes to a multi-party election system. The subsequent government under President Mohamed Nasheed discussed forming laws on the protection of intellectual property, although no policy was introduced on it. However, according to another respondent, the background behind the introduction of the current policies related to ICT has been to allow "data collection for advertising purposes, conducting surveys for dissemination purposes".

When it comes to the impact of ICT policies on digital rights and the needs of civil society, the survey results are mixed. Some respondents believe that such policies support civil society, while others believe that they hinder it. According to one respondent, civil society is affected not because of the current ICT policies, but rather due to the absence of specific ICT policies. This leads to a lack of transparency in decision making which can be ad hoc and inconsistent. This would also mean that civil society may not be prepared to face such situations. One respondent cited the following as an example: In the Maldives, there is only one government-funded school that has Arabic as the medium of instruction. Due to some cracks in the building, the government decided to move the classes to a temporary building across a heavy traffic area. A group of parents started a social media campaign to advocate for a safe and permanent building for the children. In the midst of this, the Ministry of Education moved the school principal to a different school. The parents believed that it was his neutrality in not commenting against the parents that cost him his job. After investigating the matter, the Employment Tribunal ordered the Ministry of Education to overturn the decision and reinstate the principal. Similarly, the Employment Tribunal also ordered that a teacher who was suspended from the same school after a tweet post against a government foreign policy should be reinstated. It is a positive sign that there are independent institutions that can look into matters in which individuals are vulnerable in issues relating to expressions in social media, such as losing employment.

The survey results also indicate that non-government organisations and journalists are being mentioned as examples of vulnerable segments. Respondents recommend that ICT policies should include awareness training and other measures to make it easy for people

to understand these policies and that these initiatives should be strengthened to prevent ad-hoc decisions by the government. Respondents suggest the need for a participatory process and evaluations to ensure that the unique needs of vulnerable groups are considered in the development of ICT policies. One respondent states that "ICT expansion is necessary to mainstream digital safety, as more and more services rely on digital technology." Another respondent emphasised having a "specific focus on protecting women from cyberbullying and online harassment." While cybercrime is a global issue, implementing targeted policies and measures at the national level can help to address it in the local context.

The survey results suggest that there is a lack of awareness and understanding of ICT policies among civil society members and that there may be a need to improve education and awareness about these policies. The survey also highlights the need to involve civil society in the policy development process and to consider the needs of vulnerable groups in the development of ICT policies. One respondent stated: "ICT expansion is needed to bring inclusiveness as more and more services are dependent on digital services".

Conclusion

The Maldives has made some progress to promote sustainable development of the telecommunications and ICT sector by providing affordable and non-discriminatory telecommunications charges, expanding and developing telecom infrastructure, and establishing an autonomous regulatory authority. However, it is important to note that there is no specific ICT policy or law in the Maldives. What is available, including the Maldives Telecommunication Policy 2006, the Maldives Telecommunication Act (2015), Communications Authority Act (2015), Strategic Action Plan 2019, and Draft Cybercrime Act 2022, are more general policies that relate to telecommunication, communication, and strategic action plans. Therefore, there are policy gaps such as the lack of focus on digital rights and civil society, lack of attention to current and emerging challenges, and limited ability to address specific issues that arise in the ICT sector.

Based on this analysis, some recommendations for future research and policy development include:

- Addressing digital rights and civil society: To update the ICT policy framework to specifically address digital rights and civil society, in order to ensure that these issues are protected and that the rights and interests of all stakeholders are taken into account.
- Addressing current and emerging challenges: To conduct research to identify current and emerging challenges in the ICT sector, such as data privacy and security, net neutrality, and digital literacy, and include measures to address these challenges in the policy framework.
- Improving specificity: To carry out research and develop specific measures and policies to address any specific issues or challenges that arise in the ICT sector, to ensure that the policy framework is equipped to promote sustainable development and address the needs of all stakeholders.
- Increasing awareness: To enhance awareness and understanding of ICT policies among civil society members, and promote education and awareness about these policies.
- Encouraging civil society participation: To encourage civil society participation in the development and implementation of ICT policies to ensure that the rights and interests of all stakeholders are taken into account.
- Monitoring and evaluation: To establish monitoring and evaluation mechanisms to ensure that the policies are being implemented as intended and that they are achieving their intended objectives. This will help to identify any areas where the policies are falling short and to make any necessary adjustments. It is suggested that more research be done once the Draft Cybercrime Act is made public to better understand its effects on digital rights and civil society.

NEPAL

DIGITAL RIGHTS NEPAL

In these modern times, information and communication technology (ICT) has been part of our personal and professional lives. All sectors, including business, education, and health care, have seen an unprecedented use of ICT, especially in the post-COVID-19 world.

One of the visible impacts of COVID-19 on Nepal is the rapid transition to digitisation. The government and private sector have accelerated efforts to automate and digitise their services and processes. This is reflected in the vision for the Digital Nepal framework, which focuses on eight sectors, namely digital foundation, agriculture, health, education, energy, tourism, finance, and urban infrastructure.[1]

Despite technological advancement and the striving for digitisation in Nepal, the country does not have comprehensive laws and policies relating to ICT. Laws are fragmented and scattered in various other legislation.[2]

1. Digital Nepal Framework
2. See Annex 1 for the detail ICT laws in Nepal

For instance, acts like the Electronic Transactions Act 2006, National Civil Code 2017, National Penal Code 2017, Individual Privacy Act 2018, Advertisement (Regulation) Act 2019, National ID and Civil Registration Act 2019, National Broadcasting Act 1993, and the Telecommunication Act 1997 have provisions relating to ICT, digital space, and cybercrimes.

Among these, the Electronic Transaction Act (ETA) 2006 is widely used as the cyber law in Nepal. Therefore, it is important to review this Act. The primary aim of the ETA is to establish a secure environment for the internet, e-mail, and online transactions, but it has been misused to silence journalists writing dissenting political opinions or criticising the government.[3]

Likewise, personal privacy is valued as a fundamental human right protected in both physical and digital spaces nationally and internationally. However, digitisation has impacted and posed risks to personal privacy. The government enacted the Individual Privacy Act 2018 without proper consultation with the stakeholders and general public to meet the constitutional deadline. [4]

In this light, the report will review the Electronic Transaction Act 2006 and Individual Privacy Act 2018.

Review of the ICT Laws

Electronic Transaction Act, 2006

The Electronic Transaction Act 2006 is the only law that specifically regulates and monitors cyberspace, including cybercrime. ETA was promulgated by the parliament of Nepal, recognising the need for legal provisions to ensure the integrity, reliability, and security of electronic transactions.[5] The key features of the ETA are as follows:

3. https://kathmandupost.com/national/2019/04/15/journalist-charged-under-electronic-transaction-act-for-reporting-about-financial-fraud
4. https://myrepublica.nagariknetwork.com/news/parliament-passes-16-various-bills-before-deadline/
5. Preamble of the ETA

- Objectives of the ETA:
  - To make legal provisions for the authentication and regulation of electronic data;
  - To make a reliable data generation, communication, and transmission;
  - To make a secured and authentic means of electronic communication; and
  - To regulate all related matters of electronic transactions.

- Electronic Record and Digital Signature

The Act ensures subscribers' right to authenticate any electronic record by their personal digital signature.[6]

- Legal Validity of Electronic Record and Digital Signature

The electronic record is considered to be legally valid if the information, document, or record is maintained in an electronic form that fulfils the procedures as stipulated in this Act or its Rule.[7]

The digital signature is considered to be legally valid if such information, documents, records, or matters are certified by the digital signature after fulfilling the procedures as stipulated in this Act or its Rules.[8]

- Provisions Relating to Controller and Certifying Authority: The government of Nepal may, by notification in the Nepal Gazette, designate any government officer or appoint any person who has qualifications as prescribed in the office of the Controller.[9]

An application with required documents must be submitted to the Controller appointed pursuant to the Act to obtain a licence as a "Certifying Authority".[10] The license must be renewed every year by filing an application in the prescribed format to the Controller at least two months prior to the expiry period.[11]

---

6. Section 3(1) of the ETA
7. Section 4 of the ETA
8. Section 5 of the ETA
9. Section 13 of the ETA
10. Section 16 of the ETA
11. Section 16 of the ETA

- Procedure to obtain a digital signature certificate[12]
    - An application must be submitted to the Certifying Authority along with the applicable fees.
    - Certifying Authority must issue a digital signature certificate within seven days, affixing their signature if it decides to issue such a certificate.
    - If the Certifying Authority decides to reject the application, the applicant must be notified of the reasons for rejection within seven days.

- Suspension of certificate

The certificate may be suspended under the following conditions:

- If the subscriber obtaining the certificate or any person authorised to act on behalf of such a subscriber requests to suspend the certificate;
- If it is found necessary to suspend the certificate that contravenes public interest;
- If it is found that significant loss might be caused to those persons who depend on the certificate by the reason that provisions of this Act or the rules framed thereunder were not followed at the time of issuance of the certificate; or
- If the Controller instructs to suspend the certificate having specified the aforementioned grounds.[13]

- Revocation of certificate

The certificate may be revoked under the following conditions:

- Where the subscriber or any other person authorised by such person requests to revoke a certificate;
- If it is necessary to revoke a certificate that contravenes the public interest;
- Upon the death of the subscriber;

12. Section 31 of the ETA
13. Section 32 of the ETA

- Upon the insolvency, winding up, or dissolution of the company or corporate body under the prevailing laws, where the subscriber is a company or a corporate body;
- If it is proved that a requirement for issuance of the certificate was not satisfied;
- If a material fact represented in the certificate is proved to be false; or
- If a key used to generate a key pair or security system was compromised in a manner that affects materially the certificate's reliability.[14]

14. Section 33 of the ETA

Offenses	Punishment
Piracy, Destruction or Alteration of computer source code (Section 44)	Imprisonment not exceeding three years or with a fine not exceeding two hundred thousand rupees or both (Section 44)
Unauthorised Access in Computer Materials (Section 45)	Fine not exceeding two hundred thousand rupees or imprisonment not exceeding three years or both depending on the seriousness of the offense (Section 45)
Damage to any Computer and Information System (Section 46)	Fine not exceeding two hundred thousand rupees or imprisonment not exceeding three years or both (Section 46)
Publication of illegal materials in electronic form (Section 47)	Fine not exceeding one hundred thousand rupees or imprisonment not exceeding five years or both (Section 47)
Divulsion of confidentiality (Section 48)	Fine not exceeding ten thousand rupees or imprisonment not exceeding two years or both, depending on the degree of the offense (Section 48)
Providing false statement (Section 49)	Fine not exceeding one hundred thousand rupees or imprisonment not exceeding two years or both (Section 49)
Submission or Display of False Licence or Certificates (Section 50)	Fine not exceeding one hundred thousand rupees or imprisonment not exceeding two years or both, depending on seriousness of the offense (Section 50)
Computer Fraud (Section 52)	Fine not exceeding one hundred thousand rupees or imprisonment not exceeding two years or both (Section 52)
Abetment to commit computer-related offense (Section 53)	Fine not exceeding fifty thousand rupees or imprisonment not exceeding six months or both, depending on the degree of the offense (Section 53)
Punishment to the Accomplice (Section 54)	Half of the punishment for which the principal is liable (Section 54)
Punishment in an offense committed outside Nepal (Section 55)	Same as offense committed in Nepal (Section 55)
Other offenses (Section 58)	Fine not exceeding fifty thousand rupees, or imprisonment not exceeding six months or both (Section 58)

- Formation of Tribunal

The Act contemplates the formation of an Information Technology Tribunal consisting of three members for proceedings for offenses under the Act. Further, the Information Technology Appellate Tribunal formed under this Act will hear the appeal against the decision or order made by the Controller, Certifying Authority, and Information Technology Tribunal. However, the tribunals have not been established so far.

Key Concerns on the ETA

The Act does not recognise many cybercrimes, prominent among them being spamming. Digital signatures have been laid out as a major thrust of the ETA, but a number of gaps exist in the provisions. Broadly, ETA has criminalised 11 types of acts as cybercrime, and the Act has categorised the offenses related to computers and offenses related to obtaining certification licenses for digital signatures under the same heading.

The ETA does not provide remedies to victims of all types of cybercrime; it only addresses certain types of cybercrimes, such as character assassination on online platforms and social media.[15] On the other hand, Section 47 violates the fundamental guarantees provided by the Constitution and puts limitations on freedom of expression in the digital space.[16] Among all the provisions, Section 47 of the ETA is the most misused provision in the field of digital rights in Nepal.[17] Likewise, most individuals accused under the ETA are released on bail, and this does not make the victims feel a sense of justice.[18] The legality of Section 47 of the ETA has already been challenged in the Supreme Court of Nepal.[19]

15. KII with Pabitra Raut
16. KII with Pabitra Raut
17. KII with Anil Raghubansi
18. KII with Pabitra Raut
19. Advocate Pratyush Nath Upreti filed the writ petition before the Supreme Court of Nepal.

Exceptional power is given to the controller[20] to intercept information, which is against the essence of what is laid down in Article 17[21] of the constitution of Nepal. Any form of restriction on opinion and expression over the internet is a violation of freedom of speech and expression guaranteed under Article 17(2)(a)[22]. Therefore, the provision of the ETA like Section 47, if abused, may restrict freedom of opinion and expression guaranteed by the Constitution, as well as international instruments such as Article 19 of the International Covenant of Civil and Political Rights to which Nepal is a party.

The wording of Section 47 of the ETA explicitly includes online harassment, cyberbullying, indecent acts, and defamation against women, but does not mention the LGBTQI+ community or people with disabilities[23]. It should be noted that harassment affects anyone, not just women, yet the current laws only recognise women as the only vulnerable group for online harassment or cyberbullying[24]. The ETA, especially Section 47, has not included other vulnerable groups like children, marginalised communities, and minorities[25]. It is crucial to include considerations for different vulnerable groups in ICT laws to ensure a safe and accessible internet for all.[26]

Section 60 and 66 of ETA provides for the formation of an IT tribunal and IT Appellate Tribunal for adjudication of the cases relating to the ETA; however, the government of Nepal has not formed these tribunals. Instead, the Kathmandu District Court is designated as the court to try, hear, and settle cases relating to ETA and cybercrimes. This means that regardless of where the cybercrime is committed or where the victims are located, the case should be initiated in Kathmandu. With the rise of reporting on cybercrimes, this centralised provision is taking a toll on the police, prosecutor, and legal counsels, as well as the victims, witnesses, and defendants. It is very hard for the victims in rural areas to travel to Kathmandu for legal proceedings[27]. This leads to exclusion and marginalisation and decreases access to justice for rural populations[28].

20. Chapter 4 of the ETA
21. Article 17 of the Constitution of Nepal (2015) is related with the right to freedom including freedom of opinion and expression and freedom of assembly.
22. Article 17(2)(a) of the Constitution of Nepal (2015) is related with freedom of opinion and expression
23. KII with Sonika Baniya
24. KII with Sonika Baniya
25. KII with Anil Raghuvashi
26. KII with Sonika Baniya and KII with Anil Raghuvashi
27. KII With Pabitra Raut
28. KII With Sonika Baniya and Pabitra Raut.

The ETA is not a comprehensive law and is insufficient as a legal deterrent to cybercrimes[29]. According to the National Penal Code 2017's classification, offenses in which the punishment is up to three years imprisonment are considered ordinary crimes, whereas offenses in which the punishment is up to 10 years are considered serious offenses while those above 10 years imprisonment are considered heinous crimes. The offenses and corresponding punishment in the ETA are classified as ordinary crimes, except offenses under Section 47. It is hard to articulate the rationale behind prescribing the punishments under the ETA.

Individual Privacy Act, 2018

The right to privacy is protected by Article 28 of the Constitution of Nepal which reads:

"The privacy of any person, his or her residence, property, document, data, correspondence and matters relating to his or her character shall, except in accordance with the law, be inviolable."[30]

In order to fully implement Article 28 of the Constitution, the federal parliament has endorsed the Individual Privacy Act 2018. It is the first law in Nepal specifically addressing the protection of individual privacy. The key features of this act are as follows:

- Scope of the Act

The Act protects the privacy of body and personal life of a person (Section 3); family (Section 4); privacy relating to reproductive health and pregnancy (Section 6); privacy relating to residence (Section 7-9); privacy of property (Section 10); privacy relating to document (Section 11); privacy relating to data (Section 12); privacy relating to correspondence (Section 13); privacy relating to character (Section 15); and privacy of electronic means (Section 19).

29. KII with Taranath Dahal
30. Article 28, Constitution of Nepal (2015)

- Personal Information and Sensitive Personal Information

The Act classifies certain information as personal information and certain information as sensitive information. Section 2(c) defines personal information as information related to "(1) caste, ethnicity, sexuality, gender disclosure, birth, origin, religion, race or marital status; (2) education or educational degree; (3) address, telephone or e-mail address; (4) passport, citizenship certificate, national identity card number, driving license, voter identity card or details of identity cards issued by public authorities; (5) any documents sent or received by the individual which contains personal information; (6) fingerprint, handprint, retina of eyes, blood group or other biometric information; (7) criminal background or details regarding punishment awarded to or suffered by an individual for any offense, and (8) any professional or expert opinion or view delivered by an individual in the course of making a decision."

Information relating to (1) caste, ethnicity or origin; (2) political affiliation; (3) religious belief; (4) physical or mental fitness or condition; (5) sexual orientation or incidents concerning sexual life; and (6) details of property are defined as sensitive personal information[31].

Under the Act, the management, protection, and secured utilisation of personal information is entrusted to public authorities[32]. It also specifically restricts public authorities from processing sensitive information[33].

- Rights of Citizens Under the Act

Under this Act, Nepalese citizens have the following rights as it pertains to data protection and personal privacy:

  - The right to be informed[34];
  - The right to access information[35];
  - The right to rectification[36];

31. Section 27 of the Individual Privacy Act 2018
32. Section 23-26 of the Individual Privacy Act 2018
33. Section 27 of the Individual Privacy Act 2018
34. Section 23(3) of the Individual Privacy Act 2018
35. For example Section 26 of the Individual Privacy Act 2018
36. Section 28 of the Individual Privacy Act 2018

- The right not to have their sensitive personal data processed[37]; and
- The right to file a complaint and seek compensation[38]

- Collection of Personal Information

The Act emphasises that personal information will be collected in accordance with law and will not be used without consent[39]. It should be done by officials authorised under the law or persons permitted by such officials.

The authorised official/person is required to comply with the following requirements regarding the collection, storage, retention, analysis or publication of personal information:

- The purpose of collecting the information and its intended use should be clearly disclosed to the concerned person.
- In case the information is to be collected for the purpose of study or research in any particular area or for collection of public opinion, the following matters should be clearly disclosed.
- The following matters shall be clearly set out:
  - Time of collection of information
  - Subject matter for which the information is collected
  - Nature of information
  - Purpose of collection of information
  - Methodology and process of information processing
  - Assurance that the privacy of individual information is not breached
  - Matters related to the security of the collected information
  - Use of personal information

37. Section 27 of the Individual Privacy Act 2018
38. Section 30-31 of the Individual Privacy Act 2018
39. Section 23 and 26 of the Individual Privacy Act 2018

- Disclosure of Personal Information

Public authorities or corporate bodies are restricted from using or disclosing personal information collected, stored, or retained by them without the consent of the concerned person. However, this restriction does not apply when information is collected during the course of a criminal investigation, as per the order of a court, or as required by an official authorised to require such information[40].

Similarly, the Act permits disclosure in the following instances: (a) publication of personal correspondences or study, research, or verification of a certain portion of such correspondence in situations where the person has consented; (b) document bearing personal information is necessary for identification purposes to avail 'public services' or, (c) an order is issued by the court or competent authority in a pending case or during the course of investigation or prosecution of any criminal offense[41].

It should be noted that the personal information or data may be used or disclosed to others by the officials, without obtaining the consent of the data subject, under the following circumstances:

- For the purpose for which it was collected,
- Written request from the investigative or adjudicating authority in the course of investigation or adjudication of criminal cases,
- Order from the court in the course of proceedings of sub-judice cases,
- To resolve any questions on qualification or other matters of a public official, and
- Written request from the competent authority to resolve any specific questions relating to a specific subject matter.[42]

- Use of CCTV Camera

The Act allows the installation of CCTV cameras in any public place other than the toilet, bathroom, or changing room[43]. It is mandatory to display the notice regarding the installation or use of CCTV cameras[44].

40. Section 26 of the Individual Privacy Act 2018
41. Section 26 of the Individual Privacy Act 2018
42. Section 26 of the Individual Privacy Act 2018
43. Section 20 of the Individual Privacy Act 2018
44. Section 20 of the Individual Privacy Act 2018

- Prohibition on Surveillance or Espionage

For the purpose of obtaining anything confidential, the residence or office should not be surveilled by using electronic means or photography or any other method[45].

- Use of drone

The Act provides that drones should not be used for the purpose of obtaining any secret information about any public body, archaeologically important place, building of security agency, protected zone or zone of mine or mineral, or at the residence of any person, without permission of the authorised official/person[46]. The exception to this provision includes two places, i.e. border area or/and public place of the country.

- Obligation of Public Authority

The Act imposes upon the public authority an obligation to protect the personal information collected or retained by them. Furthermore, public authorities are required to arrange effective security measures against risks involving unauthorised access, use, alterations, disclosure, publication, or broadcasting of such data.

- Offense and Punishment

The violation of the Act is a criminal offense where the case may be initiated by either an individual or the State as per the nature of the offense[47].

The offender is liable for imprisonment of up to three years or a fine of up to NPR 30,000 (USD 230 approximately) or both[48].

The aggrieved party is also entitled to compensation for the loss suffered due to the violation of the provisions of the Act[49].

45. Section 21 of the Individual Privacy Act 2018
46. Section 22 of the Individual Privacy Act 2018
47. Section 29(3) and 30 of the Individual Privacy Act 2018
48. Section 29(2) of the Individual Privacy Act 2018
49. Section 31 of the Individual Privacy Act 2018

Key Concerns on the Individual Privacy Act

The law does not clearly define whether "person" referred to in the definitions for personal information and sensitive personal information pertains to a natural or legal person[50]. However, the specific examples cited in the definition (such as caste, ethnicity, education, passport, etc.) suggest that it applies to natural persons. The protection and management of information about legal entities are currently uncertain.

The Act applies to the collection and use of personal information and aims to govern the data or information generally collected, retained, analysed, or processed by public authorities or corporate entities incorporated under Nepalese law. However, it is unclear how the Act would be enforced in regards to personal information of Nepalese residents collected (a) outside of Nepal, or (b) by an offshore entity within Nepal.

The Act includes some problematic provisions, such as Section 3(5) stating that the privacy of a person's physical or mental condition or private life may be disclosed in the following circumstances:

- If it is a matter involving the consent of the person concerned,
- If the matter is already made public by the person concerned through his or her own will,
- If the matter is under investigation as related to an offense, by the investigating or prosecuting official,
- If the matter which is related to biological or biometric identity, gender identity, sexuality, sexual relation, conception or abortion, virginity, potency, impotency or physical illness has to be disclosed for obtaining any concession, and he or she obtains or desires to obtain such a concession.

The State should assess potential harms before disclosing the information and undertake measures to protect people from such harms. Concessions can be provided alongside protecting the privacy of a person.

50. KII with Pabitra Raut, Anil Raghuvanshi, and Sonika Baniya

Likewise, Section 5(2) allows "any security check under the prevailing law or to search any person in the course of investigation of a criminal offense." This is not necessarily perceived as an intrusion of privacy. The Act provides more exceptions in the name of investigation of a criminal offense or necessity.

Police investigation into a case or any necessary step to gather evidence and find perpetrators is not always viewed as an invasion of privacy.

- In practice, state intervention in private matters has been increasing. CCTV cameras are widely used in the Kathmandu valley officially for security reasons but at the risk of undermining existing law. It is not clear how the recording, preserving, handling and sharing of CCTV recordings will be done while giving due importance to the protection of data and individual privacy.
- It is often reported that intelligence and security agencies operate surveillance technology amid declining rule of law, incompetent governance, and high-profile corruption cases shaking public faith in government institutions[51]. The privacy of citizens is on the back burner in a weakening democracy[52].

In this light, Section 19(4) is very problematic as it empowers authorised officers to intercept, monitor, record or transmit any electronic message or data. This clause could have a serious impact. An individual may not know if his/her electronic communications are being monitored. This can make surveillance provisions prone to misuse.

In the view of one expert interviewed for this research, there should be a differentiation between private individuals and public figures, and public figures should declare their properties for better transparency and accountability[53]. According to the current Act, information related to personal property is protected by the right to privacy.

51. https://www.recordnepal.com/sleepwalking-into-a-digital-world
52. https://www.recordnepal.com/sleepwalking-into-a-digital-world
53. KII with Taranath Dahal

As Nepal is moving towards digitisation and the rapid growth of IT and private companies, the Act should have a separate provision relating to violation of privacy by IT companies and service providers[54]. Individual hackers are not the only ones responsible for privacy breaches. It is important to have a provision to make the government, its agencies, or IT companies accountable for violations and intrusion on individual privacy[55]. In many instances, private companies or service providers not only directly collect information, but also store certain private information in their systems and they should be liable for its protection. Therefore, it is important to elaborate on data protection provisions more comprehensively.

The gravity of the punishment appears to be very low, i.e. imprisonment of up to three years or a fine of up to NPR 30,000 (USD 230 approximately) or both. Likewise, there is no guarantee that compensation for the violation of privacy is not adequately provided[56].

This Act was passed to meet the constitutional deadline, so it did not see any meaningful participation of the public in the lawmaking process and it does not include the experience and needs of the public who are impacted and affected by the Act[57].

Cases of privacy breaches should be civil cases, rather than criminal cases, as they provide a means of relief for the victims[58].

54. KII With Pabitra Raut
55. KII With Pabitra Raut
56. KII with Sonika Baniya
57. KII with Taranath Dahal
58. KII with Pabitra Raut, Anil Raghuvanshi, and Sonika Baniya

Conclusion and Recommendations

Conclusion

Both the ETA and Individual Privacy Act have tried to ensure legal norms for the security, protection, and deterrence of crimes and harms. However, as seen above, these laws have concerns and loopholes. Therefore, it is necessary to amend these laws to ensure the utmost protection and safeguards of digital rights and fundamental freedoms online.

ETA

The problem with the current ETA is that it attempts to cover computer-related crimes or cybercrimes in general and does not have specific provisions, as it was enacted to make legal provisions for the authentication and regulation of electronic data and electronic transactions. ETA has been used to control and limit digital rights, especially freedom of expression in digital spaces. The government has adopted a control mechanism rather than the maximisation of the right in terms of use and enjoyment[59]. Because Section 47 of the ETA has been widely misused by law enforcement authorities, this section should be quashed.

Only the Kathmandu District Court is empowered to hear and decide cases relating to cybercrimes. As previously mentioned, this centralised provision is taking a toll on the police, prosecutor, legal counsels and defendants. This leads to exclusion and marginalisation and curtails rural populations' access to justice. Hence, it is high time that the government set up a specialised IT Tribunal and Appellate Tribunal as envisaged by the Act and delegate power to concerned District Courts to look into cybercrimes of a trivial nature.

59. KII with Pabitra Raut

Conclusion and Recommendations

Individual Privacy Act

The Act has missed the point of arbitrary or/and unlawful interference of the State to the privacy of a person. The Act has not taken a holistic approach to individual privacy and data protection. It is not clear on the access and control over individual data being collected and recorded, and the involvement of public authorities as well as private entities. Therefore, it is imperative to amend the Act with a holistic approach to collecting, preserving, handling, and sharing of data so that the protection of data and privacy could be given due importance. The Act should be amended to include more provisions on data protection.

During the key informant interviews, it was viewed that cases of privacy breaches should be civil cases, rather than criminal cases, as they provide a means of relief for the victims. These breaches typically involve violations of personal rights, such as the right to privacy, and not criminal acts. Through civil cases, victims can seek compensation for damages such as emotional distress and financial loss, as well as an injunction to stop future violations. This approach offers a more suitable solution for individuals whose privacy has been compromised, unlike criminal cases which primarily focus on punishing the offender rather than addressing the victim's harm.

Policy Recommendations

- Role of the Government

To advance and safeguard digital rights, the government should be a protector rather than a controller. This can be achieved through the adoption of a non-interventionist or a less interventionist approach. By taking a hands-off approach, the government allows individuals to freely exercise their digital rights without undue interference. This approach not only ensures the protection of digital rights but also promotes an environment of innovation and progress within the digital space.

- Timely and Informed Consultation with Multiple Stakeholders

Laws and policies relating to ICT should address the needs and concerns of gender minorities, marginalised people, ethnic communities, and individuals with disabilities. This is because these groups face unique challenges in accessing and using technology and they must not be excluded or marginalised. By addressing these issues through legislation, the government can help ensure that everyone has equal access to technology and its benefits, promoting inclusivity and equality in the digital space.

- Public Awareness of the ICT Laws

The general public is not aware of the potential digital safety and security implications of Section 47 or provisions of the Individual Privacy Act. This is the case especially for children, women, LGBTQI+ communities, and people with disabilities. Therefore, to ensure digital rights, public awareness and digital literacy are a must. The government and civil society need to focus more on enhancing public awareness about digital rights and improving digital literacy.

Policy Recommendations

- Collaboration and Accountability

The government should collaborate with various stakeholders regarding digital rights to consider diverse perspectives and interests. This is because digital rights impact a broad range of individuals and organisations. Tech companies, civil society organisations, and individual users are among the stakeholders the government can work with to gain a comprehensive understanding of the digital world's challenges and opportunities. By collaborating, the government can create well-informed and inclusive policies that address the needs and concerns of all parties involved. Furthermore, involving stakeholders in the law and policymaking process increases transparency and accountability, ensuring the outcomes are a reflection of society's diverse views and needs. Therefore, government collaboration with stakeholders is crucial in establishing a comprehensive and effective approach to digital rights.

Private companies and governments need to be held accountable to protect, promote and ensure digital rights, such as freedom of expression, rights to privacy, and accessibility to the internet, among others.

- Specific laws on cybercrimes

Separate and specific laws on cybercrime stem from the emerging and unique challenges posed by the digital world. Existing laws are inadequate to handle the rapidly evolving landscape of cybercrime, which encompasses a range of activities such as hacking, identity theft, and online fraud. These crimes require a specialised legal framework to effectively address their specific nature and the means by which they are committed. Without specific laws, the current legal system may be unable to prosecute and punish perpetrators, leaving individuals and organisations at risk. By having dedicated laws for cybercrime, the government can guarantee the protection of victims' rights and accountability for those who commit these crimes.

Annex 1

Mapping ICT laws and policy in Nepal

Constitution	Legislation	Delegated Legislations	Policy	Draft Bill
Constitution of Nepal (2015)	Electronic Transactions Act, 2006	Online Media Operation Directives, 2017	Telecommunications Policy 2004	Information Technology Bill, 2018
	National Civil Code, 2017	Information Technology Emergency Response Team (Operation and Management Team) Directive, 2075	Information and Communication Policy 2015	Media Council Bill
	National Penal Code, 2017	Cyber Security Bylaw, 2020	National Broadband Policy 2071	Social Media Regulations
	Individual Privacy Act, 2018		Digital Nepal Framework 2019	
	Advertisement (Regulation) Act, 2019		National Cybersecurity Policy, 2021	
	National ID and Civil Registration Act, 2019			
	National Broadcasting Act 1993			
	Telecommunication Act, 1997			

Annex 2

List of Key Informant Interviews

S.N.	Name of Expert	Detail	Date	Mode of Meeting	Venue
1	Pabitra Raut	Lawyer with expertise in media and cyber law	22 January 2023	Physical	Babarmahal
2	Anil Raghuvashi	Child Safety Net	23 January 2023	Physical	Jawalakhel
3	Mahima Pradhan	Body and Data	25 January 2023	Online	-
4	Sonika Baniya	Women in Technology	28 January 2023	Physical	Gairidhara
5	Tara Nath Dahal	Freedom Forum, pioneer in RTI and FOE	27 January 2023	Physical	Thapathali

PHILIPPINES

OUT OF THE BOX MEDIA LITERACY INITIATIVE, INC.

The Philippines has garnered consistently low rankings in indices on press freedom, internet freedom, and civil liberties: 55/100 or "partly free" as of 2022 in Freedom House's Global Freedom Score; 65/100 or "partly free" in Freedom on the Net; and 147th out of 180 countries in the latest Press Freedom Index. The common issues cited in these reports are political interference from government officials who both interpret current laws and legislate to stifle dissent, the weaponisation of social media to spread disinformation in insidious ways by firms and public officials, a culture of widespread government corruption, and the continued stranglehold of political dynasties.

The Philippines also remains one of the deadliest countries for activists for almost a decade now, according to Global Witness. For 15 straight years, it has consistently been among the top seven countries in the Committee to Protect Journalists' Global Impunity Index, a ranking of the worst countries with unsolved killings of journalists.

It is within this context of an increasingly fragile democratic veneer and deeply-rooted culture of impunity that civil society raises alarm over the passage of two pieces of legislation within 27 months albeit under two different regimes: the Anti-Terrorism Law and the SIM Registration Law, which are deemed as additional ammunition in the government's arsenal in its legal warfare against targeted enemies.

The Anti-Terrorism Law was signed into law on July 3, 2020, by then-President Rodrigo Duterte. The Duterte regime was notorious for its war on drugs, which saw a death toll of at least 8,600 to around 30,000 Filipinos and is currently the subject of an official investigation by the International Criminal Court. Under the Duterte administration, the persistent problem of red-tagging, or labelling individuals or groups as communists or terrorists, has worsened. The Anti-Terror Law was controversial for, among other things, granting state authorities the ability to designate organisations or individuals as terrorists arbitrarily and extending overbroad powers to police forces for surveillance.

The SIM Registration Law, on the other hand, was signed on October 10, 2022, the first law enacted by President Ferdinand Marcos Jr., who is inextricably linked to his late dictator father's martial law regime. The law's proponents aimed to crack down on the proliferation of scams and spam via anonymous prepaid SIM card users. Digital rights advocates have challenged the law over its serious privacy concerns, including the ability of authorities to misuse the personal information of its critics and the inability of the government to enact proper digital security measures in the past.

To counter the adverse impacts on the general observance of human rights, digital rights included, advocates are advised to strengthen the campaign for the repeal of both laws while proactively pushing for policies that protect affected sectors. Doing so would deepen rights education and nurture networks of tighter civil society cooperation.

The Anti-Terrorism Law

Seeking to "make terrorism a crime against the Filipino people", the Anti-Terrorism Law (ATL) replaced the Human Security Act (HSA) of 2007, which proponents believed was "lenient to offenders, and restrictive to enforcers". One proponent, then-senator and former national police chief Panfilo Lacson, claimed that the provisions in the HSA that could potentially penalise enforcers far outnumbered the provisions that prosecute terrorists. The ATL aims to remedy this by expanding the definition of terrorism and creating the Anti-Terrorism Council which has the power to designate individuals and organisations as terrorists.

Three months into what would become one of the world's longest and strictest COVID-19 lockdowns, Duterte himself pressured the House of Representatives into adopting in full the ATL's Senate version by writing a letter to Congress certifying the ATL as urgent. This prioritisation of the ATL over an economic stimulus package, which was then pending in Congress, drew criticism, as the country was also then experiencing its worst economic contraction since World War II.

Other important elements to note in contextualising the passage of the ATL are the whole-of-nation approach to counterinsurgency laid out by Duterte in his Executive Order 70 in 2018, the breakdown in 2017 and the eventual permanent termination in 2019 of the peace negotiations between the government and the Communist Party of the Philippines-New People's Army (CPP-NPA), and their declaration as a terrorist organisation.

Also of interest is the adoption in 2019 of the more insidious National Action Plan on Countering and Preventing Violent Extremism, the key features of which are its criticism of the "inadequate capability of teachers, guidance counselors, school administrators and parents to identify early signs of radicalization among children and students" and its focus on the "exposure of individuals to the violent extremist community through digital media platforms".

Since its passage, the ATL has faced massive public outrage from civil society organisations and individual citizens along with widespread online and offline protests. It has also become the most contentious law to date, with 37 complaints filed before the Supreme Court questioning its constitutionality.

"A country of unquestioning individuals": The ATL's chilling effect

Journalists and media organisations under the Freedom for Media, Freedom for All coalition were among the petitioners against the ATL, citing its chilling effect on their profession. Longtime alternative media practitioner and press freedom advocate Prof. Danilo Arao noted: "The chilling effect is very much spelled [out] in a situation where journalists and even vloggers and content creators could be charged with terrorism based on the sources of information that they choose to interview."

“If we want to adhere to the highest standards of the profession, we should be able to enjoy an atmosphere that would be conducive to our practice, whether it's journalism, advertising, public relations or entertainment. The ATL doesn’t create an atmosphere that’s conducive,” he added.

Prof. Arao also points to the sociopolitical milieu within which the ATL was passed, particularly the atmosphere of antagonism to the media enabled by Duterte himself. He cited instances demonstrating how Duterte has become an enemy of press freedom: the shutdown of television broadcaster ABS-CBN, legal cases filed against news website Rappler, relentless red-tagging against news organisations, and cyberattacks and the blocking of websites of alternative media such as Bulatlat and Pinoy Weekly.

Aside from the ATL being “inherently problematic” because of its overbroad definition of terrorism, Prof. Arao also highlights how the law further enables law enforcement agencies’ bias against criticality.

“The anti-terrorism law has emboldened law enforcement agencies and even civilians who are notorious red-taggers in terms of persecuting critical voices from various strands of the political spectrum. So we're not just talking about activists. Even ordinary citizens, or even celebrities, are being red-tagged just for the simple reason of questioning certain policies and programs,” he explained.

“Of course, the government would counter-argue and say that it's okay to be critical as long as you don't violate the law. But the problem there is we have a government that would want to have less criticality,” he added. “Not just among citizens, but even within the education sector, which would explain the relentless red-tagging against certain higher education institutions or even elementary and high schools.”

Petitioners under the Freedom for Media, Freedom for All network say that the ATL will not be able to quell the threat of terrorism but will instead “reduce the country to a field of submissive and unquestioning individuals, to be herded like sheep by the police and military.”

Anti-terrorism Council: "Prosecutor, judge, jury and jailer"

Atty. Mack Hale Bunagan, legal and data privacy officer of legal advocacy and service institution IDEALS, also cited the bias of the implementers as one major deal-breaker for the ATL. The nine-member Anti-Terrorism Council (ATC) is composed of the executive director of the Anti-Money Laundering Council secretariat, the secretaries of foreign affairs, national defence, interior and local government, finance, justice, information and communications technology, and the executive secretary and national security adviser as chair and vice chair.

On top of what petitioners against the ATL see as a de facto usurpation of judicial powers by the ATC, Atty. Bunagan believes that there is a very basic incompatibility of the Council's delegated tasks with what he calls a law enforcement body's "mentality of prosecution" – a bias or tunnel vision for "convicting people." With this, he says that it would be better not to delegate to the executive branch the power of designating individuals and organisations as terrorists and limiting the movement and freezing of assets of suspected terrorists.

Atty. Bunagan also mentions the proclivity for red-tagging by the current justice secretary Jesus Crispin Remulla, who also sits as a member of the ATC. As laws do not operate in a vacuum and are influenced by various cultural, social, economic and political forces, Bunagan said it was important to note that while the ATL's intent may be "noble on paper", it is still very much susceptible to implementers' abuse of the discretion granted to them by the law, or what he euphemises as "human moral frailty".

Also important to consider, in terms of bias, is the long history of discrimination and human rights violations suffered by the Moro people in the southern Philippines. Wilnor Papa, Philippine human rights officer at Amnesty International, raised the possibility of the ATL resulting in the disproportionate targeting of the Moro population and undermining the progress in peacebuilding in the Bangsamoro.

For Papa, it all boils down to the level of trust from civil society that the government enjoys. "Why are we always wary when laws like this are being proposed, [to] the point that we almost always combat them? It's reflective of what kind of government we have: a government that is highly abusive and very corrupt. And the systems in place are either not working correctly or not working at all. If we look at those who are going to implement this, various agencies and bureaus under the security sector, do we really trust them to do good? To do justice to the 'spirit of the law'?"

Papa's misgivings are not unfounded. In 2019, before the enactment of the ATL, the Anti-Money Laundering Council, whose executive director is a member of the ATC, had already frozen multiple bank accounts of the Rural Missionaries of the Philippines, a grassroots non-profit run by nuns which has long been a target of red-tagging by the National Task Force to End Local Communist Armed Conflict. In June 2022, with the ATL already in effect, the assets of retired Catholic priest Walter Alipio de Asis Cerbito were frozen, along with those of five others whom the ATC had designated as terrorists.

In June 2022, the National Telecommunications Commission, upon the request of then-national security adviser Hermogenes Esperon, blocked the websites of alternative media outfits Bulatlat and Pinoy Weekly along with 26 others belonging to several advocacy groups alleged to be affiliated with the CPP-NPA. The alternative media outfits have been suffering cyber-attacks traced to the Philippine army since 2018.

The first to be charged under the ATL were members of an indigenous people in Central Luzon, the Aeta. In August 2021, Jay Garung and Junior Ramos were accused of being members of the NPA and detained. They were charged with terrorism, murder, attempted murder and illegal possession of firearms and explosives. They have also reportedly been tortured for a week. National minorities have also been victimised by the ATL's precursor, the Human Security Act. Edgar Candule, an Aeta, and Datu Jomorito Goaynon, a Lumad leader, were both charged with terrorism in 2008 and 2019 respectively.

In January 2023, the ATC designated community doctor Natividad Castro as a terrorist. Dr. Castro has previously been arrested on kidnapping and serious illegal detention charges in February 2022, but was released a month later after a regional court dismissed her case "due to denial of her substantive right to due process". Three months later, a court ordered her re-arrest. Castro, known for initiating health programs for the Lumad in Mindanao, is now being charged for her alleged involvement in "the planning, training, preparing, and facilitating the commission of terrorism and recruitment and for supposedly providing material support to terrorist organizations."

Phil Robertson, deputy Asia director at Human Rights Watch, warns of a "human rights disaster in the making" with the ATL taking effect and a Council that will be "prosecutor, judge, jury and jailer."

Terror in the details

Aside from the ATC's power overreach and the overbreadth of the definition of terrorism (Sections 4 to 12), critics point to specific provisions that pose a threat to civil liberties: (1) warrantless arrest and detention that can be prolonged up to 24 days (Sections 25 and 29), which can already be considered torture according to Wilnor Papa of Amnesty International; (2) surveillance and interception of communications (Section 16), which can potentially conflict with provisions of the Data Privacy Act; (3) the waiver of bank secrecy (Section 35); and (4) the removal of award for damages in case of acquittal, which was previously provided for in the Human Security Act.

All these create a chilling effect that would result in stifling the exercise of basic freedoms of speech, expression, the press, association, and assembly.

Although the Supreme Court has upheld the ATL as constitutional and has struck down only portions of Sections 4, a qualifier for a terroristic act, and Section 25, a method of terrorist proscription, it can still be scrutinised using the three-part test established in Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR), which is used to assess the legitimacy of limitations on freedom of expression.

The ATL minimally passes the first test with the bare minimum of its passage as a law and enjoys the presumption of legality with the Supreme Court upholding it. But it can be counter-argued that a law must also be precise and provide guidance and that restrictions that are "unduly vague, or otherwise grant excessively discretionary powers of application to the authorities" – which are provided in controversial sections of the ATL – "fail to meet the main purpose of the first test, that is to "limit the power to restrict freedom of expression to the legislature". The first test essentially deems the ATL as a circumvention of democratic control and as "inconsistent with democracy".

As for the second test requiring a restriction to serve a legitimate aim, the ATL also superficially passes with its purported aim of protecting national security and public order. But a qualifier of the second test casts a shadow of doubt on this, in that it requires that any restriction must serve the legitimate aim in both purpose and effect. It can be argued that the ATL, taking into consideration the sociopolitical context within which it will be implemented and the track record and biases of its enforcing body, subverts its touted objective of ending terrorism with a foreseen infliction of, ironically, state terror upon not just its targeted enemies, "terrorists", but also its supposed beneficiaries, ordinary citizens.

Unfortunately, the ATL fails to overcome the high standard presented in the third test, which is the necessity for the restrictions imposed by the law in the protection or promotion of the said legitimate aim. Without minimising the imminent threat of terrorism, it can be argued that other societal problems both undergirded and exacerbated by structural inequities in the country are more pressing for the ordinary Filipino. The ATL's insidiousness, in terms of its chilling effect intruding into the collective psyche, is a disproportionate bargain for the elusive promise of a life lived without terror.

The SIM Registration Law

The SIM Registration Law, first proposed in the 18th Congress but vetoed by then-outgoing President Duterte, was passed by the 19th Congress and signed by President Ferdinand Marcos Jr. to curb the proliferation of spam texts and scams. In 2020, the police tallied 6,110 cybercrime offenses while in 2021, Globe Telecom monitored a total of 1.15 billion scam and spam messages.

The law directly affects 75.4 million unique mobile users, as per Department of Information and Communications Technology (DICT) data. It requires all SIM users to register their cards by submitting personal data such as their name, birthday, gender and address to telecommunications providers along with a government ID to prove their identity. Under the law, unregistered SIMs will be deactivated 180 days after the law's effectivity, and the sale and use of SIMs registered using false information will be penalised.

The law will chiefly be implemented by the National Telecommunications Commission (NTC), in coordination with the DICT, the Department of Trade and Industry, the National Privacy Commission, and private telecommunications companies. Violators are subject to prison time ranging from six months to six years and/or fines ranging from P100,000 to P4,000,000.

According to UK-based Privacy International, since the first SIM registration law was passed in South Africa in 2002, such laws have "threatened vulnerable groups and facilitated generalized surveillance" by making it "easier for law enforcement authorities to track and monitor people." The international privacy protection group even warns against such a policy, based on the experiences of 155 countries that have implemented their own SIM registration. The group pointed out a rise in identity theft and black markets for unregistered cards, like in Pakistan, and an increased vulnerability to hacking attacks, as experienced in Indonesia last year when 1.3 billion SIM registration details were leaked.

The Philippines, which has around 160 to 180 million active SIM cards, could face the same problem as attempts at data breaches are not unfamiliar in the country. A few weeks before the 2016 polls, the Commission on Elections said that the information of over 70 million voters had been leaked. During the 2022 election period, the DICT reportedly warded off over 20,000 attempts to hack the automated election system. The Office of the Solicitor General has also experienced cyber-attacks, with its website being hacked in December 2020 and with documents containing sensitive information leaked to the public between February to April 2021.

Although the law purports to protect against text scams, the Anti-Money Laundering Council and the Philippine National Police, both part of the ATC, have also touted the law as "anti-terrorism measures".

Activists have opposed the SIM Registration Law, fearing it will legitimise further surveillance and violations of data privacy amid the current climate of "intensified red-tagging, killings, and arrests by the government since the Duterte administration".

The SIM Registration Law also doesn't allay the surveillance woes of journalists when handling sensitive stories and gaining the confidence of possible whistleblowers. The National Union of Journalists of the Philippines's secretary-general Ronalyn Olea shared: "We have always assumed that journalists have been subjected to surveillance. And in the past, we have recorded incidents of surveillance and some of these actually translated to physical harm, which included the arrest, detention, and trumped up charges against our colleagues." Two journalists, Renato Blanco and Percival Mabasa, have already been killed since Marcos Jr. took office in June 2022.

A continuation of the Duterte regime's threat to freedom of expression

For Prof. Arao, these fears are not unwarranted as he views the Marcos presidency as a continuity of the Duterte administration's strongman approach and the crackdown on dissenters.

He even posits that the current administration is much worse "in the sense that the Marcos Jr. administration has some pretension of democracy and political neutrality." In reality, the Marcos government is "still weaponising the laws and the bureaucracy to repress our basic freedoms including press freedom", with the SIM card registration law being one such manifestation.

Prof. Arao sees the SIM Registration Law not just as a threat to the right to privacy but also to freedom of expression. Even before the law's passage, the height of the COVID-19 lockdowns in 2020 already saw ordinary citizens face legal troubles through comments critical of the government. Now, critics surmise that individual SIM users can suffer the same fate.

An unnecessary burden

Other groups, such as the Foundation for Media Alternatives, also criticise the SIM Registration Law for its imposition of an "unnecessary burden on mobile phone users and third-party resellers, which consist mainly of small businesses" while yielding "no improvement in the prevention, investigation and prosecution" of the crimes it is supposed to deter, as proven in the experiences of other countries.

The SIM Registration Law may also disenfranchise those with limited mobility and access to the technical and logistical requirements in registering their SIMs, specifically low-income and less technologically-literate groups, further making them vulnerable to opportunists who have recently turned SIM registration assistance into a scam. An LGBTQIA group also asserted that the law is "fascist and transphobic" for forcing transgender people to use their dead names, or birth names that they no longer use.

As for the law's implementation, it does not so far look promising. In the first two days of registration which began in December 2022, the DICT already received at least 500 complaints over glitches in the registration systems due to a high volume of traffic.

A surprise additional selfie requirement not included in the SIM Registration Law has also become a cause for concern. According to telecommunications companies, real-time selfies are an additional verification system to protect SIM users from spoofing or identity theft. But the Junk SIM Registration Network isn't buying it, highlighting that it is these same telcos that failed to protect the public from the text scams which necessitated SIM registration in the first place.

The scam that is SIM registration Law

The seeming alignment of the telcos' and authorities' interests can be gleaned even before the passage of the SIM Registration Law, when, according to Olea, the telcos "readily implemented the order from the NTC to block the 28 [alternative media] websites without questioning the legality or the authority of the NTC to do so."

Olea believes that the spate of text scams last year was a calibrated prelude to the SIM Registration Law's passage. "The NTC and the telcos essentially did nothing to prevent the text scams except for advisories reminding the public to beware of such."

She pointed out that the telcos also stand to gain from the passage of the law as the collection and maintenance of personal information fall under their purview. "We all know that data is the new oil. They're going to profit and benefit from this."

"That's why the SIM Registration Law really is dangerous. It's not just the state that's violating our right to privacy. It has also allowed the private sector, particularly the big telcos, to use our data," she added.

To recap, the SIM Registration Law penalises the failure to register a SIM under Section 4 and its accompanying penalties stipulated in Section 11a, putting a burden on the majority of law-abiding citizens in the hopes of deterring scammers. It also impinges on the right to privacy and anonymity with the registration requirements detailed in Section 5 and the access, handling and use of this information allowed in Sections 9 and 10, leaving personal details vulnerable to data breaches and state surveillance.

Upon analysis using the three-part test, it appears that the SIM Registration Law does not stand any better than the ATL. Although the registration guidelines outlined in the law are succinct enough, its scope – the provision to law enforcement agencies of (1) tools to resolve crimes involving the use of SIMs and (2) a platform to deter the commission of wrongdoings – seems overbroad and can be interpreted in a myriad of ways. With this in consideration, the SIM registration fails the first test.

The law's stated aim also falls short of the exclusive list of legitimate aims set out by the ICCPR. The danger lies in the tension between the law's purported purpose and potential effects. If interpreted and implemented in tandem with other anti-terrorism measures, the enforcement bodies' track record and biases again come into play. The only requirement that comes in between a SIM user's data privacy and security from state surveillance is a subpoena based on a sworn complaint that their number was and is being used in the commission of a crime, which can include the laundry list of terroristic activities enumerated in the ATL.

The SIM Registration Law fails the third test in that its criminal penalties, imprisonment and onerous fines, are disproportionate when juxtaposed with the glaring lack of evidence of the efficiency and effectivity of SIM registration in preventing the crimes it was legislated to combat.

Conclusion

Grounding the protection of digital rights as inextricably integrated with the full realisation and exercise of basic freedoms has always been imperative. Access to and use of digital spaces and technologies will be for naught if it does not expand the collective's capacity to enjoy rights to freedom of expression and privacy, which are enablers of other human rights and are a cornerstone of democracy. It is tragically ironic then that our democratic rights are being infringed upon and our civic spaces constricted through digital routes.

The Anti-Terrorism and SIM Registration Laws not only engender a chilling effect because of their criminal penalties of fines and imprisonment but also endanger actual lives with the state surveillance that they facilitate. The ATL effectively sharpens the hunting tools for the state's targeted "terrorists" while the SIM Registration law casts a net that catches all, even enemies yet undesignated. Digital spaces have become the hunting ground. And we are all in the crosshairs.

Although anyone can fall victim to the threat to life and liberty posed by these two laws, we cannot act like prey. Human rights advocates and the general public need to confront these challenges and reclaim these civic spaces, both online and offline.

Recommendations

For government

- Center human rights in the legislation and execution of policies: In practice, this can be done by creating more spaces for civil society participation and public deliberation, and maintaining healthy channels for multi-sectoral dialogue and feedback to ensure strong accountability measures and oversight mechanisms.
- Foster a climate of trust: The government needs to do its best to assuage public anxiety about data breaches by beefing up its data privacy accountability and resilience, specifically by strengthening the Data Privacy Act and giving additional powers to the National Privacy Commission. It should also take the necessary steps to decriminalise libel by amending the Revised Penal Code and the Cybercrime Prevention Act. Lastly, the government could look into principles put forth by digital rights advocates in the Filipino People's Digital Justice Declaration and use the Philippine Digital Rights Agenda as a "checklist of priority issues" that need to be addressed to ensure "a robust digital environment" in the country.

For advocates

- Deepen rights education at the grassroots: The best counterbalance to a government's overreach is an informed and empowered public. Human rights education can be further deepened by continuing efforts at the grassroots level. There is also an emerging need to mainstream discussions on the right to be forgotten, right to privacy, and right to anonymity, and to include these in digital rights and media literacy efforts.
- Nurture networks of civil society cooperation: An important part of mainstreaming rights advocacy is the maintenance of robust relationships among civil society actors that would be a fertile bedrock for cross-sectoral and intergenerational network-building initiatives. Aside from being an infrastructure of support and protection when facing attacks, these networks can also make concerted efforts in recording and responding to complaints and controversies related to the two laws.
- Strengthen the campaign for the repeal of both laws: At the maximum, the repeal of both laws should be the centre of campaigning efforts. At the minimum, amendments should be pushed to curb the discretionary powers of the ATC and install accountability provisions in the ATL; and introduce in the SIM registration law a stricter requirement, such as a judicial warrant, for the access of personal details by authorities, instead of just a subpoena.
- Proactively lobby for policies for the protection of human rights defenders and other at-risk groups: The campaign for the passage of the Human Rights Defenders bill, which has been pending since the 17th Congress, should be revitalised. In addition, the adoption of a law prohibiting red-tagging should also be supported. Discussions on the Magna Carta for Internet Freedom can also be revived.

For the general public

- Look out for members of your community: It's not just about knowing what you can do, but also where you can do something. Extending concern and compassion to people in our immediate vicinity is becoming exceedingly necessary considering the trend of social atomisation. Being critical consumers of digital content is not enough to counter the erosion of democratic rights and spaces. We also need to build, if not join, support groups of mutual care and responsibility, embedded in the wider web of networks for the defence of democracy.

This report draws from interviews with the following:
Prof. Danilo Arao
Atty. Mack Hale Bunagan
Ms. Ronalyn Olea
Mr. Wilnor Papa
Ms. Sunshine Serrano

SRI LANKA

HASHTAG GENERATION

As of January 2022, 11.3 million Sri Lankans are internet users – roughly half of its 21.5 million population. The number of social media users has steadily grown to 8.2 million users, up from 2 million users in 2014. Of this figure, over 98% access social media platforms using mobile devices. The country's two key institutions that govern the internet space are the Telecommunications Regulatory Commission (TRCSL) established in 1996 and the Information and Communications Technology (ICTA) established in 2003.

After undergoing a protest-driven political regime change in 2022 and being faced with a severe economic crisis, Sri Lanka is in a state of instability. Social media played a key role in this regime change as a tool of mass-scale mobilisations and brought the collective dissent of people to light. The local government elections, the first island-wide election since the new president took over, had earlier been announced but were postponed due to lack of funds. The 2023 budget, which was approved last year to address the country's economic meltdown, included a proposal to improve the digital economy and the establishment of a Data Protection Authority.

Freedom of speech, assembly, and association[1] are fundamental rights guaranteed in the Sri Lankan Constitution with limited restrictions[2]. Landmark judgements over time have expanded the right[3] and interpreted the limitations to these restrictions[4]. However, successive governments have used the tactic of cracking down on dissent whenever there is a possibility for public unrest. During the anti-Muslim riots in 2018, Easter Sunday attacks in 2019, COVID-19 lockdown in 2020/21 and public protests in 2022, the government restricted internet access, blocked social media platforms, and arrested hundreds of people, citing ICT laws related to material shared on the internet and social media platforms. In January 2023, the President expressed his willingness to introduce laws to restrict social media content following the Singaporean model.

Against this backdrop, this report, drafted in consultation with key stakeholders, reviews the Computer Crimes Act No 24 of 2007 and the Personal Data Protection Act No 09 of 2022 in detail. The former has been used by law enforcement in conjunction with other laws to restrict digital space and the latter includes provisions that could further shrink the digital rights space and limit press freedom. In addition, the report in brief reviews the implications of the ICCPR Act No 56 of 2007, Emergency Regulations, and the proposed Cyber Security Bill, considering their impact on citizens and their everyday lives.

The report recommends that the government maintain access to internet services, digital platforms, and circumvention technology, particularly during elections, protests, and periods of uncertainty while inviting international partners to help strengthen digital-related laws to comply with international human rights laws.

.

1. Article 14
2. Article 15
3. Amaratunga vs Srimal and Others (1993) 1 SLR 264 and Gunewardena vs Perera and Others (1983) 1 SLR 305
4. Sunanda Deshapriya vs Municipal Council Nuwara Eliya (1995) 1 SLR 362 and Sunila Abeysekera vs Ariya Rubasinghe (2000) 1 SLR 314

Computer Crimes Act No. 24 of 2007 (CCA)

After the introduction of the internet to Sri Lanka in the 1990s, the government sought to introduce corresponding legal provisions to match advancements in the ICT field and the safety of its users. A proposed law to prevent computer crimes was in consideration since the late 1990s. After a long consultative process, the Computer Crimes Bill was submitted to Parliament and debated in August 2005. The initial bill underwent a series of amendments and was finally approved in May 2007.

The purpose of the CCA is to identify computer crimes and to provide procedures to investigate and prevent such crimes. The law categorises the following as offenses: accessing a computer or information held in a computer (S. 3 and 4); causing a computer to perform a function without lawful authority (S. 5); causing an offense using a computer putting national security, national economy and public order in (potential) danger (S. 6); dealing with unlawfully obtained data from a computer (S. 7); illegal interception of data (S. 8); making a device available to commit an offense under the act (S. 9); and unauthorised disclosure of information (S. 10).

In addition to sentencing and fines, the Act also provides for financial compensation (S. 14) for aggrieved parties. All offenses committed under this act are cognisable, (S. 16) meaning that the alleged perpetrators can be arrested without a warrant. To carry out an investigation, enter any premises, or access any information, a police officer of the rank of Sub-Inspector or above should be accompanied by an expert (S. 17). These searches could be carried out without a warrant if there is urgency (S. 18). The minister in charge of information technology appoints the expert (S. 17). How the investigation should be conducted without hampering the ordinary use of a computer (S. 20) and breaching the confidentiality of information (S.24) is specified in the Act. The jurisdiction to hear and prosecute offenses under the CCA is vested with the High Court (S. 25).

Even though the CCA provides an effective mechanism to deal with computer crimes, it has become inadequate to address online crimes amid the ever-evolving nature of online space and technology.

The CCA has a few provisions (S. 3, 8 and 10) to protect the right to privacy. However, in contradiction, S. 18 in the same Act permits an expert, or a police officer involved in the investigation, to tap any "wire or electronic communication" or obtain any subscriber information from any internet or digital service provider. S. 22 empowers a police officer to seize electronic equipment and devices, creating the possibility of a serious breach of privacy for a suspect or an alleged offender.

Over the years, CCA has been used by law enforcement authorities to stifle freedom of speech, especially in the era of social media, citing Section 6 of the Act which reads:

> Any person who intentionally causes a computer to perform any function, knowing or having reason to believe that such function will result in danger or imminent danger to — (a) national security; (b) the national economy; or (c) public order, shall be guilty of an offense and shall on conviction be punishable with imprisonment of either description for a term not exceeding five years.

This section criminalises using a computer in a manner that results in danger or imminent danger to national security and public order. With these broadly-interpreted terms, law enforcement authorities may argue in bad faith that the dissemination of false content poses a danger to public order and that criticising the government is a danger to national security. Arrests can be made without a warrant, based on the suspicion of an offense being committed under this Act – expanding the power of law enforcement to utilise this provision to curb dissent. This has created a climate of increasing fear and self-censorship among civil society actors and opponents of the government.

However, a holistic reading of the CCA suggests that Section 6 applies to actions that affect the software or hardware of a computer system. The intention here is to protect computer systems encompassing, for example, a defence system, an aviation system, or the stock exchange. It is actions such as embedding spyware in a computer system for espionage that is envisaged by this Section.

Section 6(2) provides that in a prosecution for an offense under subsection (1), certificates from the relevant ministers of defence and finance attesting to the existence of the national security, national economy, or public order concern shall be admissible in evidence and shall be prima facie evidence of the facts stated therein. This section reverses the burden of proof in that the burden is shifted to the defence to prove that there is no such threat as is envisaged by the certificate. Proving the negative is admittedly a higher burden. The Computer Crimes Division (CCD) of the Criminal Investigation Department (CID) of Sri Lanka Police recognises that, for example, the defence secretary has more information concerning threats to national security; therefore, any information that is relayed to the CCD by the defence secretary should be given due consideration.

The CCA does not contain draconian provisions akin to those contained in the Prevention of Terrorism Act (PTA) No 48 of 1979, for example. However, the problem is in its implementation. If law enforcement officers are concerned with the intention of the government, they may not be concerned with the mischief that the offenses under the CCA are intended to counter, but would rather look at the CCA as a tool to give effect to the intention of the government. The PTA has terrorism-specific offenses so the CCA need not replicate the same. But the offenses under the CCA are broad enough to encompass terrorism-related offenses as well. No law should be looked at in isolation.

During the COVID-19 lockdown in Sri Lanka, the CCA was used to arbitrarily arrest and detain people who were critical of the government's response to the pandemic. This was done in the name of countering disinformation and fake news: a disproportionate response to the infodemic at the time. During the first wave of COVID-19, the police made several arrests for spreading fake news on social media about the virus, citing the provisions of the CCA. S. 6 above was interpreted by Sri Lanka police to include false rumours regarding the head of state, as seen in the case of a woman who was arrested for allegedly spreading a rumour that the President had tested positive for the virus. In a bid to maintain public order and avoid unnecessary panic, the Inspector General of Police issued a circular in April 2020 to arrest anyone criticising public officials and pointing out “minor issues” in the pandemic response efforts. An educational administrator was arrested for insisting on a higher

fatality rate on a post on his Facebook profile. A man was arrested for allegedly creating false propaganda about the virus and sending it to 5,000 people on Facebook; the basis of the arrest was that this act harms national security and public peace.

Similarly, many attempts were made to prevent public mobilisation via social media during the large-scale protests against the incumbent President and his government in 2022. The CCA was used frequently when peaceful protestors retaliated against violent mobs in May 2022, during which riots erupted and resulted in the death of several individuals. In response, the President ordered strict enforcement of the law against the rioters, which included a crackdown on social media using the CCA. The police started investigations into 59 groups on social media in this regard, while the CID looked into alleged threats to Members of Parliament via social media. A journalist was summoned for questioning over content on his YouTube channel that allegedly created public unrest when he spoke of the ongoing economic crisis and attempted to hold the government accountable.

Law enforcement used tactics to threaten and instil fear among those arrested. It was observed that individuals were targeted more than media pages with a high number of followers. There is a concern among activists and political opponents that the content they share online could be misinterpreted by law enforcement and used as a basis to arrest and silence them for political purposes. This may also lead to self-censorship and a chilling effect on the public when showing dissent or expressing themselves freely.

Resorting to CCA to infringe on the digital rights of the people beyond its initial purpose of safeguarding users of computer crimes is a growing concern in Sri Lanka. Dr Gehan Gunatilleke, commenting on the severity of this issue, spoke of the possibility of CCA being used by law enforcement to avoid the requirement of obtaining a search or arrest warrant as the offenses under the Act are cognisable.

Section 18(4) of the CCA provides that the Minister may, by regulation, "prescribe the manner in which and the procedures required to be followed in respect of, the retention and interception of data and information including traffic data, for the purposes of any

investigations under this Act." However, after being in force for over 15 years, no such regulations have yet been published.

When evidence concerning an offense under the CCA is produced in court, the CCD of the CID is compelled to produce all the data they retrieve from a computer system instead of restricting it to the evidence that is referable to the offense. This is intended to maintain the credibility of the evidence produced. Given the public nature of court proceedings, there is an obvious threat to the privacy of the parties involved. A judge can play a role in protecting the privacy of an individual by, for example, retracting private information from appearing in the judgment.

Section 21(2) of the CCA provides that no police officer shall access any computer for an investigation unless the Inspector General of Police has certified in writing that such police officer possesses adequate knowledge and skill in the field of information communication technology. This is intended to safeguard the credibility of the investigator who retrieved the evidence. The prosecution can establish that evidence retrieval was conducted by competent personnel. The officers of the CCD of the CID, however, do not go through an identified training course to qualify for this certification. The officers are also not required to carry this certification with them when extracting evidence. Such certification is only to be submitted to Court or an expert recognised under the CCA. To address this concern and to make sure that the officers have the required expertise to avoid tampering with the privacy of individuals, they should be given the required training in computer forensics. This could be done in collaboration with ICTA and the state universities.

Personal Data Protection Act No. 09 of 2022 (PPDA)

With our daily lives increasingly being online, the issue of data privacy has grown more important. The country lacked a sufficient data protection legal regime to protect consumers, and the PPDA was introduced to address this gap following a long process of consultations. After the law's enactment in March 2022, Sri Lanka became the first South Asian country to have comprehensive data protection legislation.

The Bill was gazetted in January 2022 and was subsequently challenged in the Supreme Court for its constitutionality. It is important to note that any aggrieved party only had two days to challenge the Bill as the gazette was published on the website for public access five days later. The 20th Amendment to the Constitution reduced the number of days available to challenge a Bill from 14 to seven[5]. Since a law can only be challenged at the Bill stage[6] according to the Constitution, this limitation, along with the above procedural error of not having timely access to the gazetted Bill, is noteworthy. Furthermore, the petition challenging the bill was dismissed without being taken up due to a technicality. The grounds on which the bill was challenged will be discussed in detail shortly.

The PPDA follows the EU Data Protection Regulations and has significant implications consisting of both legal and compliance obligations for any entity that processes personal data. The law empowers users with a wide range of data subject rights to give them more control over their own data. Considering the range of actions that data processing entities should take to ensure compliance with the PPDA, the Act will come into operation fully in 18 to 36 months and is expected to be operationalised between September 2023 and March 2025.

.

5. Article 78(1) - Every Bill shall be published in the Gazette at least seven days before it is placed on the Order Paper of Parliament

6. Article 80 (3) - Where a Bill becomes law upon the certificate of the President or the Speaker, as the case may be being endorsed thereon, no court or tribunal shall inquire into, pronounce upon or in any manner call in question, the validity of such Act on any ground whatsoever.

The Act applies to any processing of personal information that takes place in Sri Lanka as well as to controllers or processors that are domiciled in, incorporated in, or offer goods or services to persons in Sri Lanka (S. 2). The data controllers and processors are now restricted to processing data following principles of legitimacy, proportionality, accuracy, limited retention, integrity, transparency, and accountability (S. 5 - 12). It is important to note that the Act exempts the processing of personal information for personal, domestic, or household purposes. Data subjects (whose personal information is being processed) have the right to access (S. 13) and withdraw their consent or object to processing (S. 14); the right to rectify (S. 15) and to the erasure (S. 16) of data according to the PPDA. In case the data controller refuses S. 13-16 above, the data subject also has the right to review such a decision (S. 18 (1)). Ironically, this review is not permitted where, among other things, the data subject has initially consented to the automated data processing, which led to the decision (S. 18(2)). This limitation exists even for special categories of data and where such an automated decision was necessary for entering into or the performance of a contract between the data subject and the controller. This section, in contrast with the EU standards, gives less data protection to data subjects in Sri Lanka, as the EU provisions allow data subjects to review consented automated data and allow no automated decision to be based on special categories of data.

Once a data subject makes this request, data controllers are mandated to respond within 21 days (S 17). Data controllers can refuse the request of a data subject for a variety of reasons, including national security, public order, data forming a part of an investigation or a legal procedure, and the prevention, detection, and prosecution of criminal offenses (S. 17(2)). The data subjects are also entitled to know if there has been any breach of data (S. 23). The PPDA requires all data processors to appoint a suitable Data Protection Officer (S. 20) to systematically monitor and process personal data and to avoid possible risks to the said data. To further strengthen data protection, if a public authority processes personal data, it should only be processed in Sri Lanka (S. 26). Exceptions are allowed only in limited circumstances.

Another key feature of the Act is the establishment of the Data Protection Authority (S. 28) managed by a Board of Directors (S. 29) to regulate the processing of personal data, safeguard and protect the privacy of data, and ensure regulatory compliance with the Act to facilitate growth and innovation in the digital economy (S. 31). Powers, duties, and functions of the Authority, including the power to impose fines to parties that violate the provisions of the Act, are listed in S. 32 and 33.

While the PPDA bridges a significant gap in the field of data protection in Sri Lanka, it also has provisions that are detrimental to free speech and the free flow of information. The Bill was challenged before the Supreme Court for these differences.

According to section 3 of the Act, the provisions of the PPDA prevail over any other written law in case of any inconsistency or discrepancy. The data protection guaranteed under the PPDA challenges citizens' right to access information under the Right to Information Act No 12 of 2016. The right to information, which is instrumental to exercising the right to free speech and expression, is affected. However, Transparency International noted in a press release that the preamble of the 2019 draft framework of the Bill referred to the right to information as a crucial right and recognised the need for the public interest to be balanced with the protection of personal data. But the Act that was enacted in 2022 has omitted this provision. In an environment of government secrecy and censored or partisan information, this blow to free speech is critical.

To facilitate media freedom, a balance should be maintained between private data protection and public interest. In the context of media reporting, not having an exception to the processing of personal data makes it extremely difficult for journalists and media institutions to use the personal data of public persons in their reporting as they are data controllers and processors within the purview of the Act. If the actual crime or offense exposed is greater than the offense of processing private data, a provision protecting the journalists should be included in the Act. The removal of the financial data and personal data relating to offenses/criminal proceedings and convictions from the special categories of personal data can ensure access to relevant information to keep political figures accountable and allows space for journalists to carry on with their reporting.

Responding to the demands made by civil society actors and journalists to enable the media to process information without the restrictions of the PPDA, the Minister of Justice said during the Parliamentary debate on the Act: “There is nothing called journalistic rights in Sri Lanka. The rights of journalists and the rights of the citizens are one and the same. Journalists don't have anything beyond that, though they have a certain amount of privilege … Don't make a bogeyman out of this Act. There is nothing called a perfect law. Let us take this and move on”.[7]

Even though the PPDA does not prevent the government from establishing an independent Data Protection Authority, the significant control the government has over this Authority is likely to dilute its legitimacy as an expert body. For instance, the President has the power (S. 29 and 30) to appoint the Board of Directors (along with the Chairperson) of the Data Protection Authority, leaving a greater chance of abuse and partiality. This Authority’s power to interpret which data should be protected has an enormous bearing on journalists’ reporting when they attempt to uncover government irregularities and corruption or those affiliated with the President. The Authority is a non-judicial and non-independent body with the power to impose a fine of up to Rs. 10 million on the data controller/processor in case of non-compliance with a directive issued by them (S. 38). To make an appeal impossible, any party who is willing to appeal the fine by filling an application to the Court of Appeal should deposit in cash a sum of money equal to the imposed penalty (S. 38(9)). There is fear among media and civil society actors that the Authority would be used for political purposes and to silence critics.

.

7. Parliament Hansard dated 09th March 2023, Page 327 - https://www.parliament.lk/uploads/documents/hansard/1647331727024074.pdf

While Sri Lankan authorities are proud to be the first South Asian country and one of the few countries in Asia to enact personal data protection laws, it is important to reflect on why other countries like India are taking longer to balance the interests and rights of all stakeholders. Sri Lanka has a history of well-meaning laws being abused, such as the ICCPR Act No 56 of 2007 which will be discussed in the next section. This Act in practice could create a chilling effect on the media and among opponents of the government, creating a major blow to democracy.

After reviewing the digital rights implications of two national ICT laws, it is essential to ascertain the contribution of a few pieces of policies to the composition of the Sri Lankan digital landscape, without which this analysis would be incomplete.

International Covenant on Civil and Political Rights (ICCPR) Act No 57 of 2007

The ICCPR Act was enacted to incorporate the provisions of the International Covenant on Civil and Political Rights in 2007. After acceding to the Covenant in 1980, this was an essential step for Sri Lanka to incorporate its provision into the local legislation as a dualist nation. The ICCPR Act is brief and recognises the right of every person to be recognised before the law (S. 2), several rights of the child (S. 5), and the right of a citizen to access public benefits (S. 6).

Most importantly, S. 3 of the ICCPR Act prohibits persons from propagating war and advocating for national, racial, or religious hatred that may incite discrimination, hostility, or violence. Any offense committed under this section is non-bailable and cognisable (S. 3(4)). The High Court can impose a sentence of up to 10 years upon conviction (S. 3(3)) under the Act.

Although seemingly progressive towards countering dangerous speech, the Act has been used to restrict freedom of expression offline and online. Assessing its implementation record in the last five years, several instances of a collective restriction of free speech could be seen. For instance, a poet was arrested in April 2019 over a Facebook post allegedly inciting religious hatred when he spoke about homosexuality and child abuse in a Buddhist temple. He was kept in custody for over five months before being released on bail in August 2019. In May 2019, a woman was arrested for wearing a dress with the logo of a ship's helm that resembled a Dharmachakra. Another individual was arrested in April 2020 and kept in remand for over five months due to a Facebook post where he talked of an ideological jihad. In July 2020, authorities questioned an online activist after a Buddhist monk lodged a complaint regarding the activist's Facebook post connecting the origin of Buddhism to Jainism. In January 2023, a popular Youtuber was arrested over a comment he made about the sacred Tooth Relic of the Lord Buddha. In contrast, when a well-known rogue Buddhist monk called for boycotting Muslim shops in 2017 followed by similar incidents that are within the parameters of this section, these were overlooked by law enforcement. As of 2019, no person who has incited violence against a religious or racial minority group has been convicted under the Act despite major incidents of communal violence against people of the Islamic faith. This selective application of the ICCPR Act is infringing on citizens' right to expression, especially of minorities and opponents of the government.

Emergency Regulations

The Public Security Ordinance of 1947 gives the President the power to proclaim an emergency for all or selected parts of Sri Lanka if s/he thinks that it is expedient to do so in the interest of public security and the preservation of public order or for the maintenance of supplies and services essential to the life of the community (S. 2). According to Article 155(2) of the Constitution, the Emergency Regulations under the Public Security Ordinance have the legal effect of overriding, amending, or suspending the operations of the provisions of any law except the provisions of the Constitution.

The only check on the President's power to declare an emergency is the requirement to get Parliament's approval within 14 days of declaring such an emergency; failing which, the state of emergency would expire at the end of one month. This law allows the detention of individuals and the search and takeover of private property without a warrant and empowers the President to call on the armed forces to maintain public order and restrict people's movement.

The latest state of emergency was proclaimed by the former President in April 2022 after protestors clashed with the police and military in front of his private residence in the course of increasing protests nationwide. Shortly after that, access to social media sites was blocked as part of attempts to control growing discontent towards the government. This was extended in May 2022, curbing the right to peaceful assembly and freedom of expression. The current President, who was acting president at the time, declared a state of emergency in July 2022 (the corresponding Emergency Regulations are accessible here). Regulation 15 was of particular concern when it comes to citizens' digital rights as it makes "communicating or spreading any rumour or false statement or any information or image or message which is likely to cause public alarm, public disorder or racial violence or which is likely to incite the committing of an offense via word of mouth or digitally (including social media)" an offense. When read carefully, even sharing true information can be considered an offense if it has the potential to cause public alarm. In August 2022, the UN Human Rights Experts condemned the repeated use of the state of emergency to crack down on protestors and stifle freedom of expression.

Proposed Cyber Security Bill

The Cabinet approved the proposal to draft a law to strengthen and improve cyber protection in October 2021. The draft framework of the bill was made available to the public in December 2019. It was drafted to ensure the effective implementation of the National Cyber Security Strategy to prevent, mitigate, and respond to cyber security threats and incidents effectively and efficiently, to set up the Cyber Security Agency, to empower the institutional framework to provide a safe and secure cyber security environment, and to protect the Critical Information Infrastructure (S. 2).

The Bill proposes three separate bodies (Cyber Security Agency, National Cyber Security Operations Centre, and Sri Lanka Computer Emergency Readiness Team) with overlapping functions to deal with cyber security, which would lead to systemic delays when reacting to cyber threats.

The definition provided in the Bill for a Critical Information Infrastructure is too broad (S 17). Under conditions of poor oversight, this regulatory control could cover media institutions, civil society organisations (CSOs), and private actors and could be used as a tool to control and criminalise politically inconvenient actions. This would have a disproportionate effect on freedom of expression. Further, the absence of a definition of "cyber security incident" in the Bill may lead to the term being arbitrarily defined in a manner that would restrict freedom of expression.

If the National Cybersecurity Agency referred to in the Bill remains independent without being subjected to manipulation by the government, it would strengthen the critical digital infrastructure systems. Otherwise, the Bill has the potential to restrict or tamper with the digital rights of journalists and civil society groups.

In August 2022, the Cabinet approved the implementation of the Cyber Security Policy formulated in line with the National Information and Cyber Security Strategy.

Attempts to criminalise fake news

Pursuant to the nine-day-long ban on social media platforms in the aftermath of the Easter Sunday attacks in April 2019, the Cabinet of Ministers approved a proposal to institute legal action against the dissemination of fake news and hate speech on social media, citing the surge in online disinformation narratives that allegedly manifested in real-world violence.

In April 2021, the Cabinet of Ministers approved a proposal to enact laws against the spread of fake statements and misleading assertions publicised through the internet. Commenting on this decision, the Minister of Justice said the government cannot allow social media posts to "paint the country in an unflattering light" and that they intend to base the Sri Lankan law on the Protection from Online Falsehoods and Manipulation Act of Singapore. While there is a need to effectively counter disinformation, this move was viewed as a disproportionate response by many lawyers and social media activists. Critics note this as a step taken by the government to further restrict freedom of expression, especially on social media.

In August 2018, addressing the Colombo Defence Seminar, then Prime Minister and now Executive President Ranil Wickremesinghe spoke extensively about the threats posed by the internet and social media to national interests. He referred to social media sites as global disruptive forces, indicating his intention to restrict social media and digital spaces. Continuing his vision, the President in January 2023 told heads of various media institutions that he has received a copy of Singapore's Social Media Regulation Act and intends to enforce a similar bill to regulate social media.

All groups, especially journalists and human rights defenders, should envisage the dangers that this move would pose to free speech and should continue to fight against restrictive laws proposed by the government.

Conclusion

While freedom of expression is a fundamental right in Sri Lanka, various laws and their implementation has imposed severe restrictions on free speech, including in the digital space. In 2022, global internet freedom declined for the 11th consecutive year. According to Freedom House, Sri Lanka scored 48 out of 100 on the Internet Freedom Index. 2022 was a significant year for the Sri Lankan civil advocacy space owing to unprecedented mass protests that resulted in the resignation of the popular leader Gotabhaya Rajapakse.

Social media played a critical role in this process as a tool to gather average citizens around a common goal, keep the spirits of the protestors high, capture international attention, and document the use of force on the protestors by law enforcement. A state of emergency was declared thrice in April, May, and July and access to social media was blocked to prevent protestors from using the platforms to mobilise people.

Activists, journalists, and human rights defenders were arrested, intimidated, and surveilled for the content they shared online. According to individuals who were arrested during this period, the judiciary played a key role in demanding evidence or proof from the CID before refusing to grant bail when produced in court. The offline and online mobilisation of the public, supported by the lawyers, made it difficult for the police to carry on with their usual methods of intimidation and fear.

From time to time, the incumbent President and his government have made their intention known in bringing in legal frameworks to curb online discriminatory, defamatory, and misleading speech. The recently-enacted PPDA will have far-reaching consequences for journalists and CSOs if implemented in bad faith. The proposed Anti-Fake News Bill and the Cyber Security Bill can be used as tools to curb dissent, silence opponents, and censor media channels. With a local-level election on the horizon, digital spaces would be increasingly used by politicians for their election campaigns and to spread disinformation and hatred for election gains.

The visible increase of dangerous speech online (disinformation, sexual and gender-based violence, hate speech) and the risks they pose are used as a justification by governments to impose arbitrary and restrictive laws. In reality, these laws aim to control alternative narratives, curb dissent, and limit the free flow of information.

Safety and freedom in the digital space are fundamental to exercising one's digital rights. If one is to be active in public discourse, make informed decisions, and contribute to the continuation of democracy as free and equal citizens, various stakeholders have a responsibility to take more initiative to guarantee freedom in digital spaces amid a context where new laws are enacted in a restrictive manner.

To that end, the report recommends the following:

To Government Actors

- Adopt a consultative process including civil society representatives, journalists, and social media experts when drafting laws that have implications for digital rights
- Amend the PPDA to include "journalistic purposes" to facilitate free and independent reporting
- Maintain access to internet services, digital platforms, and circumvention technology, particularly during elections, protests, and periods of uncertainty
- Adopt a clear and consistent policy environment that supports civil rights and is compatible with human rights standards
- Train law enforcement officers on fundamental rights and constitutional limitations to avoid the arbitrary use of power
- Strengthen the capacity of law enforcement officials to obtain Mutual Legal Assistance in prosecuting transnational crimes under the CCA and PPDA

To Journalists, Human Rights Defenders, and CSOs

- Be proactive in challenging Bills before the Supreme Court that can potentially restrict fundamental freedoms
- Advocate for the immediate release of those arrested and detained for online expression
- Urge the government to have a clear and consistent policy environment that supports and protects the digital public sphere
- Promote digital inclusion towards a free and open digital space by providing expertise to legal frameworks on digital rights
- Create awareness of the rights and remedies available to citizens when their digital rights are violated
- Improve digital literacy among the people
- Disseminate knowledge and skills to recognise and counter online harmful speech
- Create solidarity networks

To Social Media Intermediaries

- Adopt swifter systems to restrict online harmful speech on their respective platforms
- Recruit more content moderators with local expertise
- Maintain meaningful dialogue with the government to ensure that social media platforms remain available to the people, particularly in times of crisis

To International Partners

- Build resilience among journalists and CSOs to resist government crackdown and continue to strengthen free speech
- Engage civil society, partner countries, and technology companies in policy dialogues related to digital transformation and civic space
- Assist the government in strengthening digital-related laws to comply with international human rights laws

EngageMedia.org/
Greater-Internet-
Freedom