IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 28, Issue 11, Series 8 (November, 2023) 09-17
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Synergising Cyber Governance And Human Rights: An Exploratory Study Of The Indian Sub-Continent

Dr Navjeet Sidhu Kundal
Assistant Professor
VSLLS, VIPS, GGSIP University.

ABSTRACT
Cyberspace permeates all aspects of our lives as digital technologies form a critical part of the infrastructure of the modern societies. People engage in all sorts of activities through the use of cyberspace ranging from attracting customers, doing business, interacting with others to creating spaces for dialogue, discussion and dissent. Despite its extensive use by people and its ability to influence public opinions and state policies, there is no binding treaty or universal laws to regulate the conduct of these activities by people. Human Rights norms can, however, play an important role in guiding any legislative action on technology and cyberspace.
Technology and South Asia are no strangers. Most number of internet users are found in some of the leading South Asian economies. The coming in of Industrialisation 4.0 has prompted most Asian States to revamp their governance models and regulate cyberspace. The last few years have seen States implementing data protection laws, intermediary regulation laws, social media liability rules.It should be seen, however, that any effort to draw a regulatory mechanism should account for human rights norms and standards. Privacy, freedom of speech and expression, right to health are human rights standards which can guide the governments and different actors that are involved in regulating cyberspace.
The paper aims to map the shifting modes of cyber regulation in South Asia and explore some of the recent laws passed in jurisdictions like Sri Lanka, Bangladesh and India to regulate cyberspace. It will also look at how far these models of governance have kept the human rights norms and principles in consideration. The paper highlights the need to review the existing regulations, as well as to provide a more comprehensive set of regulation to internalise human rights principles in cyber governance. This paper explores the application of Human Rights regime to cyberspace governance.
Key Words: *Cyber-governance, Free speech, Human Rights, South Asia, Data regulation*

Date of Submission: 11-11-2023 Date of Acceptance: 20-11-2023

I. Introduction

Cyber space is not limited merely to computer operations these days. It encompasses virtually the entire spectrum of social activities which are undertaken with the help of information and communication technologies.[1]Recent years have seen tremendous impact of cyberspace on our daily social, political and economic interactions. South Asia has become an Internet hub as it has amongst the highest users of Internet in the world. Peculiarly in South Asia, the liberating effect of the internet coexists with a heightened concern about State control of information. While Internet penetration has deepened in Asia owing to abundance of cheap mobile phones, however, cyber space has evolved into a space for contestation of power between the state and its societal opponents.[2] The interconnectedness of the global economy and the vulnerable environment of cyberspace in Asia ensures that whatever choices the region makes to regulate cyberspace, will impact the lives of coming generations.

Unlike the West, Asia has been rising amidst the information revolution. In today's world, economy is defined more by data management and intellectual capital than traditional forms of agriculture and manufacturing. Asian leaders know they must build a knowledge-based economy if their populations are to compete and continue

[1]Cees. J. Hamelink, "Human Rights in Cyberspace" (31-46) in Leen D' Haenens (Ed) *Cyber Identities Canadian and European presence in cyberspace* University of Ottawa Press, Ottawa, 1999.
[2]Aim Sinpeng, "Southeast Asian Cyberspace, politics, censorship polarisation", *News Mandala available* at https://www.newmandala.org/southeast-asian-cyberspace-politics-censorship-polarisation/ accessed on 3 June, 2023.

their transition toward middle income status. Political leaders across the region thus have invested in initiatives to digitize their economies, from Digital India to Singapore's Smart Nation Initiative.[3]

Because of the growing interconnectedness and cyber concerns peculiar to Asia, the kind of choices that Asian countries are going to make over the next few years is going to significantly affect the lives of millions of young and old people. Needless to say, the Asian response is going to mirror the western on some aspects, however, it will also take into account the new challenges and risks posed owing to the perceptibly different political environment. This, therefore, presents a unique opportunity for Asian countries to become path-bearers of a safe and secure internet. This will go a long way in incentivising the use of the internet for millions in Asia.[4]

It is imperative to look into the evolving nature of regulatory framework in jurisdictions like India, Bangladesh and Sri Lanka in the light of comprehensive push by the governments to control access to information and right to privacy. This discussion will contribute to existing literature and help future researchers in their research on cyber-governance in South Asia.

At the root of all laws regulating Internet have been concerns specific to each nation. In particular, concerns regarding free speech, prohibition of unlawful content, appointment of grievance redressal officers by social media giants and regulation of cyber activities are being addressed through the laws. Although most of the laws stem from governance challenges of cyberspace, they also raise important questions with respect to Human Rights and settling of contours with respect to free speech. In addition to the challenges from overarching laws and rules & regulations, the Human Rights space is getting eroded by the use of latest surveillance technologies like Pegasus citing the alibi of national security.

Cyber Laws in Sri Lanka

Sri Lanka had close to 10.19 million internet users in January 2021 out of which 800 thousand users were added in the pandemic period. [5] To foster a trusting environment and to ensure safe internet access, the Government of Sri Lanka has brought in a number of legislations to prevent cyber attacks and protect the privacy of citizens. Notable amongst them are: the Computer Crimes Act ,2007, the Intellectual Property Act, 2003, the Right to Information Act 2016, the Banking Act of 1988, the Telecommunications Act of 1991 and the Electronic Transactions Act of 2009.[6] These legislations cover the area of computer related crimes and activities, and also address issues related to a person's privacy. To improve cybersecurity, the Sri Lankan Government introduced two more Bills in 2019. "Consequent to drafting its first Information and Cyber security strategy 2019-23, the Ministry of Digital Infrastructure and Information Technology (MDIIT) formulated the Cyber Security Bill and Data Protection Act , 2022. These act forms part of a drive to strengthen the regulatory framework dealing with emerging cyber-security and data protection challenges."[7]

Ministry of Digital Infrastructure and Information technology released the final draft of the bill in September 2019 and opened them for stakeholder comments through its website. Based on the inputs given by key stakeholders substantial modifications were made to them. Subsequent to this a review was made by an independent committee appointed by the government and the Bills were published in gazette. The bills were to come into force within a period of three years from the date after ratification by the Parliament.[8] The bills on Cyber Security aimed to protect vital information from cyber-attacks and empower the government to establish critical infrastructure needed for the same, the Data Protection Bill aims to protect personal data of individuals.

[3]Asian Development Bank, "Innovating Asia: Advancing the Knowledge Based Economy: The Next Policy Agenda,"10 Asian Development Bank' *available* at https://www.adb.org/sites/default/files/publication/59587/innovative-asiaknowledge-based-economy-pa.pdf accessed 22 May, 2023.

[4]Jonathan Reiber, Arun Mohan Sukumar, 'Asian Cybersecurity Futures: Opportunity and risk in the rising digital world' [https://cltc.berkeley.edu/wp-content/uploads/2017/12/asianfutures.pdf accessed 24 May, 2023].

[5] Digital 2021: Sri Lanka [https://datareportal.com/reports/digital-2021-sri-lanka accessed on 24 May, 2023].

[6] *Ibid*

[7] 'Introduction to Digital Security Laws in Nepal, Sri Lanka and Bangladesh', 9 August 2019. Available at [https://www.ikigailaw.com/introduction-to-digital-security-laws-in-nepal-sri-lanka-and-bangladesh/ accessed 26 May, 2023].

[8] Sri Lanka: Proposed Bill on Personal Data Protection, Jan 2020 [https://www.dataguidance.com/opinion/sri-lanka-proposed-bill-personal-data-protection accessed 12 May,2023].

Subsequently in March 2022 Srilanka became one of the first country in South Asia to pass an act on privacy and data protection. Out of these, the Data Protection Act is dealt in detail hereunder.

The Data Protection Act 2022

The Data Protection Act aims to protect personal data of individuals held by companies, banking institutions banks, operators, hospitals and other entities engaged in collecting personal data. "It aims to regulate the processing of personal data, designate a data protection authority, safeguard the rights of citizens referred to as 'data subjects,' and regulate the dissemination of unsolicited messages using personal data."[9] The Act provides for data to be processed for specified purposes only. An exception to that would, however, be processing of data in public interest for scientific, historical, research, or statistical purposes.

The Act provides for setting up of a data protection authority, any public corporation, statutory body established by the government could be designated as data protection authority, such an authority would be responsible to handle all matters pertaining to data protection. The processing of data will be undertaken by a controller who would be "any natural or legal person, public authority, non-governmental organisation, agency, or any other body or entity which alone, or jointly with others, determines the purposes and means of processing personal data."[10]

Concerns

One of the essential aspects of the establishment of any supervisory authority, especially with respect to Data governance, is its ability to function with complete independence without outside interference, this helps safeguard the personal data of natural persons. Section 28(1) of the Data Protection Act, 2022, however, provides that the government will control the appointment of the Data Protection Authority. This is likely to interfere with the independent functioning of the body as an independent authority will be critical to balance the privacy of individuals and the right of the public to access information.[11]

Sections 6 and 9 of the Act covers exceptions in processing data. "This covers archiving of data for public interest, scientific research, historical research or statistical purposes, etc. The act does not recognize journalistic purpose as a legitimate purpose for processing of data. Data protection legislations in jurisdictions like EU, Singapore, Malaysia require data to be protected with due regard to Right to freedom of speech and expression including its processing for journalistic purposes"[12].

Further, the Act is not in consonance with the accepted global models of Data and privacy protection, including OECD guidelines. This "lack of international compatibility in privacy regulation creates many problems and restricts international trade and investments. Highly-fragmented, diverging global, regional, and national regulatory approaches make adoption cumbersome to most parties and places a high-cost burden. Data protection laws could act as a barrier for developing countries to trade internationally."[13]

The balance, or lack of it, between surveillance for national security purposes and privacy protection poses yet another challenge to data regulation laws.[14] Considerable threats are posed by mass surveillance by governments. These days, many states collect internet data to identify potential threats to national security. Although it can be argued that such programmes balance privacy needs against security concerns, reservations are bound to rise, given the large amount of personally identifiable data that the government ends up collecting. There are valid concerns about data leakage from screening programmes where data is aggregated in an algorithmic manner.[15]

Sri Lanka needs to draft laws in accordance with internationally accepted principles which have been recognised to facilitate the smooth cross border transfer of data. The countries where laws are not in place, the

[9] *Supra* Note 7.
[10] *Supra* Note 7.
[11] Personal Data Protection Act, 2022 available at [https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf] accessed 4 May, 2023.
[12] *Ibid*
[13] The Growing Need for Privacy and Data Protection in Sri Lanka available at [https://www.ips.lk/talkingeconomics/2020/01/13/the-growing-need-for-privacy-and-data-protection-in-sri-lanka/ 12 May, 2023].
[14] Supra Note 11
[15] *Ibid.*

UNCTAD recommends that "governments should aim for greater coverage in data protection, where gaps in coverage need to addressed, while, at the same time, balance is struck between surveillance and privacy".[16]

Bangladesh

As on January 2021, "Bangladesh was home to 47.61 million internet users, accounting for Internet penetration of 28.8%."[17] It is one of the fastest growing internet markets in South Asia. The erstwhile Information Communication Technology Act of 2006 was intended to provide a legal framework for giving recognition to Digital signatures, electronic records. This framework failed to address data privacy concerns therefore the Government took measures to enhance digital security through its Digital Bangladesh and e-governance project. It even came up with a long term vision in the form of National Cybersecurity strategy to strengthen the cyber-security framework.[18]

The Government came out with the Digital Security Act in September 2018 with the objective of "ensuring digital security and identification, prevention, suppression and trial of offences committed through digital device and for matters ancillary thereto"[19]. The Digital Security Act creates a wide range of cyber-crime offences and provides punishment for "propaganda or campaign against the Liberation War, the Father of the Nation, posting offensive content, cyber-terrorism and defamation, among others. Significantly, this Act has extra-territorial application"[20]. It also establishes a "Digital Security Agency, empowered to regulate content and request the Bangladesh telecom regulator remove/block the same. A number of provisions in the DSA penalize the dissemination of various types of information online, thereby limiting the enjoyment of the fundamental rights to speech, expression, and the press."[21]

Concerns

Section 8 of the Digital Security Act gives power to the Director-General of the Digital Security Agency to decide if any information published or disseminated through digital media constitutes a threat to the digital security of the nation. If the Director-General recognizes anything as a threat, then he can request the Bangladesh Telecommunication Regulatory Commission (BTRC) to remove or block such information.[22] Sub-section (2) of Section 8 authorizes the law enforcement agencies to approach the BRTC to remove or block any information published on social media on the ground of threat to security of the nation, causing hatred and disaffection amongst people. Vesting this kind of power in the agency gives a lot of subjectivity to its work and also risks allowing the suppression of different views on critical governmental policies. [23]

Another problematic provision is with respect to Section 21 of the Act which makes it an "offence to use digital platforms to spread or run a propaganda campaign, or assist in running propaganda campaigns against the Liberation War of Bangladesh, the Father of the Nation, National Anthem or National Flag"[24]. A hefty fine of 30 million Taka fine (approx. 300,000EUR) and/or life imprisonment is stipulated for anyone who violates the provision of the Act. The law enforcement agencies can easily abuse these provisions. Further the Criminalisation of opinions about Historical Facts is a clear violation of ICCPR.[25]

Section 28 and 31 prohibit publication and circulation of any information which hurts religious values or creates hostility and animosity among different class of communities. It is unequivocally true that the State has

[16]'The Growing need for Privacy and Data Protection in Sri Lanka' available at [https://www.ips.lk/talkingeconomics/2020/01/13/the-growing-need-for-privacy-and-data-protection-in-sri-lanka/ accessed 26 May, 2023].

[17]Digital 2021: Bangladesh, [https://datareportal.com/reports/digital-2021-bangladesh accessed 24 May , 2023}.

[18] *Supra* Note 16.

[19] Digital Security Act 2018, Preamble

[20] *Ibid*

[21] M. Ehteshamul bari and Pritam Dey, 'The Enactment of Digital Security Laws in Bangladesh: No Place for Dissent' in *The George Washington journal of international law and economics*, Vol 51, December 2019.

[22] Digital Security Act 2018, No. 46 of 2018, § 8, The Bangladesh Gazette Extraordinary, Oct. 8, 2018 (Bangl).[https://basis.org.bd/public/files/policy/5e1653db166e8Digital-Security-Act-2018-English-version.pdf accessed 29 June ,2023].

[23] *Ibid.*

[24] *Ibid*

[25] Human Rights Committee, General Comment No. 34: Article 19 Freedom of Opinions and Expression [https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf accessed 29 May, 2023].

the power make laws to promote tolerance and religious harmony. In the absence of any guidance or moderation/restraints on these Sections, however, the provisions can be easily misused.[26]

Further, in the garb of protecting state secrets, Section 32 imposes a heavy fine and a jail term for the commission of an offence under the Official Secrets Act. This is clearly going to stifle all kinds of fair investigation on the part of journalists.[27]

Section 43 of the Digital Security Act, 2018 allows for police officials to "enter and search any property, seize computer systems, gather data, information or other related objects, and arrest any person present on the property without a warrant, merely on suspicion that an offence under the Act has been, or will be, committed"[28]. Further, the Act provides immunity to those who conduct surveillance on the Government's behalf, by stating that any "person, entity or service provider, who gives or publishes information for the interest of investigation, cannot be investigated under civil or criminal law".[29]

Significantly, the Digital Security Act provides safe harbour protection for intermediaries, and penalizes illegal use of "identity information".[30]

Frontline defenders a human rights organisation based in Dublin observes that the government of Bangladesh passed the act in spite of strong wave of criticism from the civil society groups and human rights organisations. The Act contained vague and cryptic provisions leading to legal uncertainty and confusion. It criminalises legitimate dissent and grants absolute powers to the state to initiate action against anyone whose activities are considered suspicious by the law enforcement agencies. It also allows broad power to the government to remove or block any data from the internet, indirectly stifling dissent and silencing any voice critical of the policies of the state. It permits invasive surveillance by allowing government access to data through the intermediaries without sanction of the law. This move is considered a major blow to the creation of an enabling environment for protection of human rights in the country.[31]

Citing data from Bangladesh's Cyber Crime Tribunal, Amnesty International reports that nearly 2,000 cases have been filed under the draconian DSA, with journalists often targeted. Ten newspaper editors faced legal charges under the act for critical reporting on leaders of the ruling Awami League party in 2020.[32]

The understanding and concerns of International Academia is summed up in the lament of Ali Riaz, distinguished Professor of Political Science at the Illinois State University in the US, who published a scathing attack on the act in his research titled 'the unending nightmare' that the provisions of the act pose a threat to fundamental rights enshrined in the Bangladeshi constitution and international standards of freedom of expression.

The law has not been made to protect the citizens, but rather to serve the interests of the ruling party and the government," he expressed with anguish. He further observes, "It has deliberately incorporated vague and ambiguous concepts, which allow the government to interpret them as they wish and use as pretext to silence any critical voice.[33]

The Act is an attack on freedom of speech and expression and is repressive. The provisions of the Act are vague and broad and can be easily sed to silence and imprison journalists and social media users and carry out invasive forms of surveillance.[34] In the past few years, the Bangladesh government has used the Act to arrest more

---

[26] *Ibid* p;17.

[27] *Ibid* p; 17.

[28] Section 43, Digital Security Act, 2018.

[29] 'Two years since coming into force, Bangladesh's Digital Security Act continues to target human rights defenders and suppress free speech', 8 October 2020 available [https://www.frontlinedefenders.org/en/statement-report/two-years-coming-force-bangladeshs-digital-security-act-continues-target-human 30 May , 2023].

[30] Introduction To Digital Security Laws In Bangladesh [https://www.mondaq.com/security/880248/introduction-to-digital-security-laws-in-bangladesh accessed 29 May, 2023].

[31] *Ibid.*

[32]'Bangladesh: Escalating attacks on Media must stop' 8 October 2020. [https://www.amnesty.org/en/latest/news/2020/10/bangladesh-escalating-attacks-on-the-media-must-stop/ accessed 1 June, 2023].

[33] 'How is Bangladesh's Digital Security Act muzzling free speech?' [https://www.dw.com/en/how-is-bangladeshs-digital-security-act-muzzling-free-speech/a-56762799 accessed 1 July,2022].

[34] 'Bangladesh: New Digital Security Act is attack on freedom of expression', November 12, 2018. Available at [https://www.amnesty.org/en/latest/news/2018/11/bangladesh-muzzling-dissent-online/ accessed 1 June, 2023].

than a thousand people. The Act contains ambiguous provisions without clear definitions, explanations and exceptions including non-bailable penalties for several offences.[35]

According to Section 21 of the Act, "any person making any kind of propaganda or campaign against liberation war, spirit of liberation war, father of the nation, national anthem or national flag shall be punished with imprisonment for life and a fine not exceeding 3 crore rupees."[36] Section 25 proposes to punish any person "if he or she publishes or propagates or abets to publish or propagate any information, as a whole or partly, which he knows to be propaganda or false, with an intention to affect the image or reputation of the country, or to spread confusion."[37] This bestows sweeping powers to the state to punish any person for expressing his/her legitimately. The Act also arms the apex Digital security agency of the country with wide powers to initiate investigations and arrest anyone without a warrant on the mere suspicion of the commission of a digital offence.

Most recently, Mushtaq Ahmed died in a prison in Dhaka 10 months after he was arrested under the Digital Security Act for his comments on facebook criticizing governmental failure in handling the Coronavirus pandemic.[38] According to a report by Amnesty International as of July 2021, around 433 people have been imprisoned in Bangladesh under the act. The Act confers arbitrary power of arrest, search and seizure of devices on the enforcement agencies. They can arrest an individual without a warrant for sharing anything online.[39]

Amnesty International has found that Bangladesh authorities are weaponizing the Digital Security Act through its Sections 25 (Transmission, publication, etc. of offensive, false or threatening data information), Section 29 (Publication, transmission, etc. of defamatory information) and Section 31 to target voices of dissent. The organization has urged the government to end repression on people's right to free speech and expression online and repeal the harsh and oppressive act.

India

Having the (in)glorious distinction to be the second most populated country in the world, rapid changes in the technology sector and resultant increase in usage of cyberspace has huge repercussions for a growing economy like India. Unprecedented adoption of new age technologies, young tech-savy population and affordable internet services have pushed India into digitization. The main legislation governing cyber space in India is the Information Technology Act of 2000 which continues to be the mother legislation to govern activities in cyberspace. It has undergone two amendments: once in the year 2008 and the second in 2017.

Given the growing digitization in India and the entering of goliath technology companies, the government is finalizing the Personal Data Protection Bill. The Ministry of Electronics and Information Technology also released guidelines in the forms of Information Technology (Intermediaries and Digital Media Ethics) Rules in 2021. These I.T. Rules have been promulgated under the Information Technology Act, 2000.

According to the Ministry of Information and Technology, "these Rules are intended to combat harmful content including the persistent spread of fake news and the rampant abuse of social media and are designed to empower ordinary users and hold platforms accountable."[40]

The I.T. Rules have been subject matter of criticism and concerns and objections have been raised against the legality of the rules.[41] Since they are mere 'guidelines', they do not have legislative backing and are considered to be ultra vires the parent legislation i.e. The Information and Technology law.

The I.T. Rules are divided into three parts. Part I of the rules contains definitions while Part II empowers the government to exercise control over intermediaries like Twitter, Facebook, Google and Whatsapp. Part III involves Code of Ethics & procedure and safeguards in relation to digital media.

---

[35] *Ibid.*

[36] Section 21, Digital Security Act, 2018. Available at [https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf 2 April , 2023].

[37] Section 25, Digital Security Act, 2018.

[38] 'How is Bangladesh's Digital Security Act muzzling free speech'?[https://www.dw.com/en/how-is-bangladeshs-digital-security-act-muzzling-free-speech/a-56762799 accessed 2 May , 2023].

[39] Bangladesh: End crackdown on freedom of expression online 25 July 2021 [https://www.amnesty.org/en/latest/news/2021/07/bangladesh-end-crackdown-on-freedom-of-expression-online/1 Aug, 2021).

[40] "Information Technology Rules, 2021 suggest big changes for big tech in India." April 27, 2021 [https://iapp.org/news/a/information-technology-rules-2021-suggest-big-changes-for-big-tech-in-india/ accessed 1 May, 2023].

[41] 'India wants to cut Big Tech down to size. Critics say the new rules may give the state too much power.' April 20, 2021[https://www.cnbc.com/2021/04/20/indias-social-media-law-puts-big-techs-power-into-states-hands-critics-say.html accessed 31 May, 2023].

A pertinent and disconcerting fact about these I.T. Rules is that they were passed without any discussion in the Legislature. The rules also raise grave questions pertaining to civil liberty. Part II has grave implications for civil liberty and right to privacy for users of Internet.

In particular, Rules 3(1)(b) and 3(1)(c) permit social media intermediaries such as Facebook to play the role of an arbiter by giving it powers to decide whether any content uploaded on the platform violates any law in force or not. This rule appears to be in direct violation of Supreme Court of India Judgment in Shreya Singhal's case. The court had held in the case that "intermediaries cannot be held liable unless they had proper information, and unless proper order is given by the requisite authority". It is presumptuous on the part of the Government to expect social media intermediaries like Google, Facebook, etc. to not only scrutinize the millions of entries but also adjudicate to ensure that the entries are true, legitimate and not likely to offend the sensibilities or cause resentment among the people.

Rule 3(2) of the enactment enjoins upon the social media intermediaries to establish internal grievance redressal mechanisms. These are required to be put in place to enable the users to lodge a complaint against any content posted on the Social Media Platform. The 'Grievance Office' designated by the intermediary is, then, expected to resolve the grievance. A study by the Centre for Internet Society points out that "such take down requests have a chilling effect on Freedom of speech and expression of all users."[42]

The Rules also enjoin upon the social media intermediaries the responsibility to trace the originator of the message. It is pertinent to mention that Rule 4(4) requires that each Intermediary develops an automated tool to censor content. With a formidable position at world stage in the field of Information Technology, India had the opportunity to regulate cyberspace in deference to Human Rights Principles like Freedom of speech and expression, privacy, legality, proportionality and necessity.[43]

The rules were passed without consultation with stakeholders and parliamentary deliberation. This is in direct violation of human rights principles of legality and openness. It is pertinent to note that "when states consider particular forms of online content sufficiently harmful so as to require regulation, they should be deliberated upon openly and defined through legislation, consistent with domestic law."[44]

The country has drafted the Digital Personal Data Protection Act 2023. The Act raises significant concerns for the digital infrastructure particularly with respect to extra-territorial application of the law, limited bases for processing data, data localisation and additional types of burdens imposed on certain types of data controllers and social media companies.[45]

A significant development vitiating the canvas of Right to Privacy is the manipulation of established procedures and protocols to justify the alleged use of Pegasus - a modern surveillance tool, to target hundreds of verified phone numbers of renowned Indian journalists, political leaders, constitutional heads, dissidents, activists and private individuals.[46] Its use notwithstanding, this has certainly raised pertinent questions about the extent to which the countries can use defence as an excuse for surveillance of its citizens. The deliberations and outcome of discussions on this issue will result in evolution of Human Rights and democratic ideals.

A perusal of the Laws passed by Jurisdictions like India, Bangladesh and Sri Lanka shows that governments have passed laws hastily without adequate consultations with the civil society and other stakeholders. Such laws have scant regard for privacy, authorize censorship by state and increase surveillance.[47] The disregard for right to privacy compromises free speech and erodes the inherent right to express and hold one's opinion in clear violation of Right to Free speech enunciated in Article 19 of the United Nation's Universal Declaration of Human Rights (UDHR). "Governments are using the focus on data and national security to push misguided efforts to localize data and advance cyber laws that are not user-centred, do not keep data secure and effectively open the

[42] Intermediary Liability in India: Chilling Effects on Free Expression on the Internet, The Internet Centre for Society 27th April 2012 [https://cis-india.org/internet-governance/chilling-effects-on-free-expression-on-internet. 1 May, 2023].

[43] *Ibid*

[44] *Supra Note* 43.

[45] Transformation of Privacy Landscape in India, Jan 4 2021. Available at [https://www.mofo.com/resources/insights/210104-transformation-privacy-landscape-asia.html accessed August 3, 2022].

[46] Nishant Sirohi, 'Pegasus in the room: Law of surveillance and the national security alibi', August,7, 2021, Observer Research Foundation, [https://www.orfonline.org/expert-speak/pegasus-in-the-room-law-of-surveillance-and-national-securitys-alibi/ accessed 3 August, , 2022]'

[47] Government Policy for the Internet Must Be Rights-Based and User-Centred. [https://www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred accessed 5 Aug, 2022].

door to human rights violations"[48]. Laws that evolve in the background must keep respect for privacy at their heart and important rights recognised under all International Human Rights Instruments.

Can Human Rights Principles Show the Way?

As technologies evolve the need for regulation will continue to grow. International Law particularly Human Rights Law can be the only normative order which can prescribe rules and lay down foundational principles for safe Internet. States must align their laws in tune with Human Rights norms enshrined in the Universal Declaration of Human Rights, 1948 and International Covenant on Civil and Political Rights, 1966. The states must protect, respect and remedy any abuses that take place in the cyber space in tune with the UN Guiding Principles for Human Rights, 2011. States can progress only by facilitating a safe and accessible Internet for all.

Free Speech and Expression

It is not only preferable, rather it is imperative that the regulatory frameworks set up for cybersecurity and protection of data hinge upon universally recognised and accepted Human Rights parameters and principles. All laws that authorize surveillance must adhere to the standard of proportionality and necessity. United Nations calls upon all member states to uphold all the fundamental Human Rights in the online space as well.[49]

The development of a system of digital governance must be based on universally respected Human Rights as enshrined in United Nation's Universal Declaration of Human Rights. The United Nations Human Rights Council adopted a resolution for promotion, protection and enjoyment of human rights on the Internet affirming, thereby, that the rights that people have in the offline environment, must be protected online as well.[50]

A 2012 report of the special rapporteur on the promotion of free speech and protection of the right to freedom of opinion and expression underscores the importance of free flow of information in today's world and without any restrictions except in a few limited cases permitted under international human rights law.[51] The UN Human Rights Committee has sought to clarify the application of Article 19 para 3 of ICCPR to Digital Media and provides that "[a]ny restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3 of Article 19."[52]

The framework of International Human Rights Law remains as relevant today to new communication technologies as it was to traditional technologies. In this regard, Article 19 para 3 of International Covenant on Civil and Political Rights remains relevant in determining the type of restrictions that are in contravention of states' obligation to protect freedom of speech and expression.[53] Any restriction on free speech must pass the following tests of legality, legitimacy and necessity:

(a) "It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); and

(b) It must pursue one of the purposes set out in article 19, paragraph 3, of the Covenant, namely,

(i) to protect the rights or reputations of others, or

(ii) to protect national security or of public order, or of public health or morals (principle of legitimacy); and

Any legislation restricting the rights of citizens must only be applied by an independent body which is not under the influence of any political party, commercial enterprise or other influences which may compromise

[48] *Ibid*

[49] *Supra note* 47.

[50] United Nations Human Rights Council 20th Session Geneva Resolution on the promotion, protection and enjoyment of human rights on the Internet: resolution / adopted by the Human Rights Council. Available at [https://digitallibrary.un.org/record/731540?ln=en#record-files-collapse-header accessed 25 July, 2022].

[51] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, Human Rights Council, 29th Session available at [https://www.ohchr.org/en/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc accessed 21 July, 2022].

[52] Human Rights Committee, General Comment No 34, CCPR/C/GC/34, 12 September 2011, para 43 available at [https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf accessed 31 Aug, 2022].

[53] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, [https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf accessed on 3 Aug, 2022].

the independent judgment of the body. Further, the restrictions must not be arbitrary or discriminatory but reasonable, based on objective parameters and with adequate safeguards.

Proportional Liability of Intermediaries

The Internet began with a largely read-only Web space. The recent times have seen it evolve whereby users are able to create, share, collaborate and communicate their work with others, without any need of any web design or publishing skills without editorial review. This has come to be known as Web 2.0. This has been made possible due to protection of intermediaries from liability for third party content. However, it is disconcerting to see that the legislations aimed for cyber security and data protection, in effect, erode that protection of intermediaries. These laws aim to impose disproportionate liability on intermediaries if they fail to filter, remove or block user generated content which is deemed illegal by the governments. Such laws can lead to misaligned priorities amongst the intermediaries and would further incentivize invasive monitoring and lead to over removal of content.[54]

Right to Privacy

The Right is protected under Article 12 of the Universal Declaration of Human Rights and Article 17 of International Covenant of Civil and political Rights 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; (2) everyone has the right to the protection of the law against such interference or attacks."

In addition, the protection of personal data represents a special form of privacy. State parties are under an obligation under "Article 17(2) to regulate, through clearly articulated laws, the recording, processing, use and conveyance of automated personal data and to protect those affected against misuse by State organs as well as private parties. In addition to prohibiting data processing for purposes that are incompatible with the Covenant, data protection laws must establish rights to information, correction and, if need be, deletion of data and provide effective supervisory measures."[55]

The right to privacy can be restricted under certain exceptional situations. These may range from increase in state surveillance for improving criminal justice administration, combating terrorism and crime etc. However, these may only be permissible if internationally accepted human rights norms are adhered to. The conditions for limiting the right to freedom of speech and expression of an individual must be clearly laid down by law, measures limiting the right to free speech must be authorised by a recognised state agency, particularly the judiciary, for protecting rights of others, to prevent the commission of another crime with strict adherence to principle of proportionality. Given the above reasons, as and when the governments decide to regulate, they must build strong accountability and transparency in their efforts.[56]

II. Conclusion

The historically validated Human Rights principles can be used actively by governments to design laws that are less likely to infringe their international commitments while achieving effective results. The governments should realize that the foundations of good and effective cyber governance do not necessarily have to be built upon the burial of universally accepted and cherished ideals of Freedom of Speech, Expression and Privacy. By moderating cyber governance legislations on the touchstone of Human Rights Principles, governments can balance public and private responsibilities and foster trust and innovation while also respecting and building norms like transparency, openness, inclusivity, non-discrimination and equality.

Diclosure Statement

The author reports there are no competing interests to declare.

[54] 'Content Regulation and Human Rights Analysis and Recommendations', Policy Brief Global Network Initiative. [https://globalnetworkinitiative.org/wp-content/uploads/2020/10/GNI-Content-Regulation-HR-Policy-Brief.pdf accessed 31 Aug, 2022].

[55] Human Rights Committee, General comment No. 16 on Article 17 of the International Covenant on Civil and Political Rights, para. 10. [http://ccprcentre.org/page/view/general_comments/27798 accessed 3 Aug, 2022].

[56] *Ibid*; pp 55.