CSF Working Paper Series No. 1

Governance of Digital Technologies in South Asia: An Overview and Analysis

May 2022

Anushka Wijesinha
Gayani Hurulle
Anarkalee Perera

CENTRE FOR A SMART FUTURE

Table of Contents

ABOUT CSF

The Centre for a Smart Future (CSF) is an independent, interdisciplinary public policy think tank based in Colombo, with a network of researchers, policy professionals and industry leaders based around the world. This paper is produced under the 'Technology, Innovation and Development' thematic pillar of the Centre.

Website: www.csf-asia.org
Email: connect@csf-asia.org
Twitter: @csfasia
Instagram: @centreforasmartfuture
LinkedIn: 'Centre for a Smart Future'

DISCLAIMER

This is a working paper, and hence it represents research in progress. This paper represents the opinions of the authors and is the product of professional research. It is not meant to necessarily represent the position or opinions of the Centre for a Smart Future, or organizations that the authors are affiliated with. All information contained in this document are believed to be accurate at the time of preparation. Any errors and omissions are the authors' own. This paper was self-funded and did not have any financial remuneration from any private, government or non-government entity.

Governance of Digital Technologies in South Asia: An Overview and Analysis

Anushka Wijesinha[1], Gayani Hurulle[2] and Anarkalee Perera[3]

1. Introduction

Across the world, the rise of digital technologies has been accompanied by attempts to regulate the use of these applications and their impact on society. The growing salience of cybersecurity and data privacy, alongside concerns over content moderation and facial recognition, have highlighted the need for governments and businesses to adopt stricter regulations to address the ethical, political, and legal issues related to the use of digital technologies, while simultaneously harnessing their social and economic potential. Regulating the digital domain is arguably one of the most important cross-cutting issues facing governments, with wide-ranging implications for businesses, civil society organisations, and the public.

In this context, this paper seeks to understand the status of digital governance in South Asia, with a specific focus on Sri Lanka, India, Pakistan, and Bangladesh, which are the key Indian Ocean rim countries in this region. To that end, the research explores four major thematic areas - cybersecurity, data protection, artificial intelligence, and mis/disinformation - the choice of which is informed by their significance for South Asian countries. For instance, the region is among the most vulnerable to cyberattacks and all four countries have ranked among the top 10 markets exposed to malware threats in Asia Pacific (Microsoft Malware Infection Index, 2016)[4]. Cyber vulnerabilities threaten not only to destabilise critical infrastructure in sectors like banking and energy, but also to compromise the personal data of citizens, as evidenced by the hacking of India's biometric system in 2018 (Huffington Post,2018)[5]. The rise of internet banking, fintech, and social media applications further underscore the need for more robust data protection regimes, as well as for greater regulations on mis/disinformation and artificial intelligence. Recently, COVID-19 misinformation campaigns have stymied state efforts to crack down on the spread of the virus in Pakistan and have fuelled ethnic violence in India (Yadav et al, 2020)[6]. Indeed, these challenges are not unique to South Asia, but they serve as vital examples of the importance of analysing digital governance in the region. Annexure 1 summarizes current policies and legislation governing data protection, cybersecurity, artificial intelligence, and mis/disinformation in these select countries, based on publicly-available information.

2. Data Protection and Privacy

The growth of the digital economy has left policymakers around the world to find ways to ensure the safety of its citizens in a world with increased 'datafication' (Mayer-Schönberger & Cukier, 2013[7]), while creating an environment conducive to using data for economic gain and social good. Many countries have turned to developing and enacting personal data protection laws, which safeguards information that is related to an identified or identifiable

[1] Anushka Wijesinha is an economist and former senior government official from Sri Lanka. He is the Co-founder of the Centre for a Smart Future. Corresponding author – anushkaw@csf-asia.org

[2] Gayani Hurulle is Senior Research Manager at LIRNEasia, a regional think tank on telecoms and digital technology. She specializes in digital development and policy.

[3] Anarkalee Perera is a Masters student at Johns Hopkins University and was formerly with a public policy researchers for an Asia-based technology company.

[4] Microsoft Asia News Center (2016, June 7). Malware Infection Index 2016 highlights key threats undermining cyber security In Asia Pacific: Microsoft Report. Microsoft. https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016-highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoft-report/.

[5] Khaira, R.,Sethi, A.,Sathe, G. (2018, September 11). UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm. Huffpost.https://www.huffpost.com/archive/in/entry/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472.

[6] Yadav, K., Thange, I., Ilhardt, J., Siwakoti, S., Shapiro, J. (2020, November 25). Old hatreds fuel online misinformation about COVID-19 In South Asia. Bulletin of the Atomic Scientists. https://thebulletin.org/2020/11/old-hatreds-fuel-online-misinformation-about-covid-19-in-south-asia/.

[7] Mayer-Schonberger, V., Cukier, K. (2013). Big Data: A Revolution that Will Transform how We Live, Work and Think. Houghton Mifflin Harcourt. https://books.google.lk/books/about/Big_Data.html?id=uy4lh-WEhhIC&redir_esc=y.

individual[8] including (though not limited to) a name, address, identification number, phone number and online identifiers (such as IP addresses).

Personal data protection legislation is often rooted in upholding the right to privacy. In India, landmark legal decisions such as the Puttuswamy Judgement[9], in which the Supreme Court reaffirmed a constitutional right to privacy, paved the way for the drafting of legislation. Discourse around such legislation, however, became commonplace with the European Union's (EU) publication of the General Data Protection Regulation (GDPR) in 2016, and its enforcement in 2018. The impacts of GDPR have transcended regional boundaries, influencing progress made by South Asian countries in several ways. First, South Asian businesses that offer goods and services to the EU or monitor the behaviour of those residing in the EU (European Union, n.d)[10] have had to comply with GDPR to continue economic activity. Second, it provided a blueprint for other countries, including those in South Asia, to develop similar legislation – policymakers in India[11] and Sri Lanka[12] have explicitly noted that they referred to GDPR when developing their own legislation. It is with this economic lens that Pakistan, in a 2020 revision of their 2018 draft of the Bill[13], has aligned the draft legislation more to GDPR, with a view on facilitating internationalisation of Pakistani business.

Noteworthy is that the widespread proliferation of personal data protection laws around the world has resulted in it being seen as a precondition for creating a suitable for foreign investment. In fact, policymakers in Sri Lanka had framed the lack of personal data protection legislation as being a key barrier to investment to build support for the legislation amongst key stakeholder groups[14].

At present, all the South Asian countries examined have draft personal data legislation in place, though (except for Sri Lanka) are yet to be passed into law[15]. Sri Lanka is the first in the region to pass the law in Parliament, in March 2022. India, in its latest draft has interestingly widened the scope of its legislation to include both personal and non-personal data - a seemingly unprecedented move. It is yet to be seen if any other countries, within South Asia or outside, will follow suit.

3. Artificial Intelligence

Advances in machine learning have propelled the development of Artificial Intelligence (AI) across the world, with countries racing to capitalise on the technology's transformative and disruptive potential. The benefits of early adoption have not been lost on states like the U.S. and China, which are spearheading global efforts on AI, as well as nations in Southeast Asia and Latin America, which are in the process of implementing national frameworks for the development and regulation of AI. South Asia, however, is currently playing catch-up. Sri Lanka does not yet have a national AI policy, though the apex industry body took initiative to formulate a draft framework in 2019 (Daily FT, 2019)[16]. Similarly, in Pakistan, the Presidential Initiative for Artificial Intelligence and Computing (2018) has sought primarily to promote AI research through the provision of educational opportunities. Beyond this, the Ministry of Information Technology and Telecommunications has announced plans to

[8] What is personal data?. Information Commissioner's Office. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.

[9] Justice K.S. Puttaswamy and Another v Union of India and Others (2017) 10 SCC 1 (India). https://translaw.clpr.org.in/wp-content/uploads/2021/12/Justice-K.S.-Puttaswamy-.pdf.

[10] Does the GDPR apply to companies outside of the EU?. (Date). GDPR. EU. https://gdpr.eu/companies-outside-of-europe/.

[11] Vidhi Centre for Legal Policy. (2022, January 22). From PDP Bill, 2019 to Data Protection Bill, 2021 and Beyond-A Roundtable Discussion [Video]. YouTube. https://www.youtube.com/watch?v=mk3HnNQp0Jc.

[12] The Chamber Academy. (2021, August 12). Discussion and Overview of the Data Protection Bill [Video]. YouTube. https://www.youtube.com/watch?v=yDHqFabiUrk.

[13] Personal Data Protection Bill 2019 (Pakistan). https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft_docx.pdf.

[14] The Chamber Academy. (2021, August 12). Discussion and Overview of the Data Protection Bill [Video]. YouTube. https://www.youtube.com/watch?v=yDHqFabiUrk.

[15] Note: Sri Lanka's Bill is to be debated in mid-March 2022.

[16] Biyagamage, H. (2019, June 27). SLASSCOM launches Sri Lanka's first AI policy framework. Daily FT. https://www.ft.lk/Front-Page/SLASSCOM-launches-Sri-Lanka-s-first-AI-policy-framework/44-680805.

introduce the country's first AI policy, though early readings suggest that it will focus primarily on issues such as cybersecurity and protecting the country's critical data infrastructure (Daily Times, 2021)[17].

Bangladesh and India, on the other hand, have comparatively robust national AI policies, with specific plans for the use of AI applications in priority sectors such as education, transport, and healthcare. In addition, both countries' frameworks include plans for developing digital infrastructure and upskilling the workforce. A noteworthy unifying factor between the countries (and arguably across South Asia) is the focus on mobilising AI for economic development and inclusive growth. In Bangladesh, for example, the government hopes to specifically leverage artificial intelligence applications to meet the country's 2030 Sustainable Development Goals (National AI Strategy for Artificial Intelligence, 2020)[18]. Underlying these plans for harnessing AI for economic development have been calls for the establishment of R&D and innovation centres. If utilised correctly, these centres could promote regional collaboration on AI design, development, and deployment in South Asia.

The focus on AI's potential to gain a competitive economic edge has, however, left South Asian countries behind in select, yet vital, aspects of AI governance. Notwithstanding India's recent publication on "Responsible AI #AIforAll" (NITI Aayog, 2021)[19], and Bangladesh's terse acknowledgement of ethical principles in its national strategy, discourse on the development of a normative ethical framework for AI is still very limited. Admittedly, global conversations on AI ethics have also been criticised for a lack of consensus, technical-robustness, and accountability mechanisms (Marda, 2020)[20]. South Asian countries also face unique challenges to regulation given the "lack of maturity of its legal systems, governance standards, and the lack of institutional safeguards that exist in developed countries available in developed countries, such as the GDPR" (Natarajan and Murali, 2020)[21]. Additionally, the lack of enabling data ecosystems also poses a significant challenge to AI policy implementation in these countries. Addressing these cross-cutting issues will ultimately define whether South Asia can maximise the potential AI has to offer, while minimising its dangerous and high-risk applications.

4. Cybersecurity

Increased digitalization of economic activities, coupled with greater globalization of trade and business relationships, have led policymakers around the world to begin formulating national policy frameworks and laws to protect domestic interests against cyber threats. Ransomware attacks are increasingly successful, crippling governments and businesses, and the profits from these attacks are soaring (Microsoft, 2021). Guarding domestic infrastructure, networks, and organizations from domestic and foreign cyber-attacks have guided recent policy initiatives by South Asian countries. Yet, South Asian countries have adopted somewhat different trajectories to cybersecurity legislation. Bangladesh was the first to embark on policy formulation in this area, having incorporated cybercrimes provisions in its 2016 Information Technology Act. There are also some cybercrimes provisions in the newer Digital Security Act (2018), but this controversial law is seen more as a tool to combat online misinformation and extremism. Meanwhile, Sri Lanka drafted a Cyber Security Bill in

[17] Government to Introduce National Artificial Intelligence Policy Soon: Amin. (2021, December 6). Daily Times. https://dailytimes.com.pk/850869/govt-to-introduce-national-artificial-intelligence-policy-soon-amin/.

[18] Information and Communication Technology Division of the People's Republic of Bangladesh. (2019). National Strategy for Artificial Intelligence Bangladesh. https://ictd.gov.bd/sites/default/files/files/ictd.portal.gov.bd/legislative_information/c2fafbbe_599c_48e2_bae7_bfa15e0d745d/National%20Strategy%20for%20Artificial%20Intellgence%20-%20Bangladesh%20.pdf.

[19] NITI Aayog. (2021). Responsible AI #AIFORALL. https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf.

[20] Marda, V. (2020, July). India and Global Artificial Intelligence Governance. India and Digital Worldmaking. https://www.india-seminar.com/2020/731/731_vidushi_marda.htm.

[21] Natarajan, A., Murali, V. (2020, March). Regulating Artificial Intelligence in South Asia: Projections for the Future. ISAS and KAS. https://www.isas.nus.edu.sg/wp-content/uploads/2020/03/ISAS-KAS-AI-Special-Report.pdf.

2019 (with provisions to set up a 'Digital Infrastructure Protection Agency'), but in 2021 the government decided to draft two separate bills - one that is a 'Defence Cyber Commands Bill' and one that is 'a separate bill of cybersecurity laws outside the purview of defence'. Little is known about these at the time of writing, and they are yet to be presented to Parliament. Sri Lanka also has an Information and Cyber Security Strategy (2019-2023), and the banking regulator has stepped up efforts to combat cybersecurity threats on financial institutions[22].

India does not have specialised cybersecurity laws yet, only a policy framework on cyber security adopted in 2013 by the Department of Electronics and Information Technology. It is the current Information Technology Act (and its 2008 amendment) that contain provisions on 'cyber contraventions' and 'cyber offences'. Indian authorities are now considering a stand-alone law, and are looking at similar laws in the US and UK for inspiration. They have acknowledged that India's focus will be on national security as well as 'financial considerations'[23].

Pakistan recently adopted a National Cyber Security Policy in 2021, and interestingly, its formulation was led not by the defence establishment or by the Ministry of Information Technology, but by Pakistan Telecommunications Authority. This new policy is aimed at both data protection and prevention of cybercrimes and provides for the establishment of a new Cybersecurity Agency. By design, the policy covers both public and private institutions, including national information systems and critical infrastructure. Steps to adopt a law around it are unknown at this stage. Additionally, Pakistan's Prevention of Electronic Crimes Act (PECA) of 2016 also deals with certain aspects of cybersecurity, and stipulates methods of prosecution, investigation, and adjudication for cybercrimes. Digital rights groups contest its misuse by law enforcement agencies on the grounds of protection of civil liberties and freedom of expression. PECA 2016 is gaining prominence with the rapid growth in digital users and social media platforms in the country.

5. Social Media

Discourse on how to govern social media has risen with the ubiquity of the platforms, and mounting reports of harms associated with its use. Many of the harms associated with social media such as hate speech and misinformation, broadly referred to as the information disorder (Warbler & Derakshan, 2017)[24], have roots in offline spaces. While the accepted convention in many types of digital governance is that the onus of regulation lies primarily with the government, responsibility seems to be shared more evenly with platforms in social media governance. This was most evident in how Facebook was held responsible for the platform being used to spread hate and cause harm in Myanmar. However, self-regulation is thought not to be sufficient.

Governments in South Asia have used a wide variety of tools to restrict activity on social media platforms including internet shutdowns, which are the most extreme. Internet shutdowns are common in India. Historically, they have been triggered by various events ranging from farmer protests to school exams (Access Now, 2018[25]). Some shutdowns have been imposed in conjunction with strategic geopolitical decisions, such as the 2019 decision

[22] Sri Lanka now has a sector-specific cyberthreat agency - the Financial Sector Computer Security Incident Response Team (FinCSIRT).
[23] Bhardwaj, D. (2021, October 27). Centre planning separate cybersecurity policy. Hindustan Times. https://www.hindustantimes.com/india-news/centre-looks-at-making-cybersecurity-an-independent-law-may-include-focus-on-emerging-tech-101635274397673.html.
[24] Warbler & Derakshan (2017) describe 3 types of information disorder, characterized through intersections of falseness and harm. all of which are relevant to social media governance. They are (1) misinformation (information that is false, but not created with the intention of causing harm.), disinformation (information that is false and deliberately created to harm) and malinformation (Information that is based on reality, used to inflict harm).

[25] Taye, B. (2018, July 23). India cuts internet access for school exams, doubles down on rights-harming shutdowns. accessnow. https://www.accessnow.org/india-cuts-internet-access-for-school-exams-doubles-down-on-rights-harming-shutdowns/.

to abrogate Article 370 of the Indian constitution and bifurcate Jammu and Kashmir into two union territories[26]. Some other South Asian countries have favoured blocking select social media platforms over complete shutdowns, as seen in Sri Lanka in the aftermath of the Easter Sunday Bombings (Netblocks, 2019[27]) and anti-government protests in 2022 (Netblocks, 2022[28]) and in Bangladesh in conjunction with protests in Dhaka over Indian Prime Minister Modi's visit (Netblocks, 2021[29]). In 2021, the Parliamentary Panel on Communications and IT of India recommended that the country also explores similar measures[30].

Several South Asian countries have also introduced new regulations relating to social media governance. Pakistan, in a move widely criticised by industry (Asia Internet Coalition, 2020[31]; Asia Internet Coalition, 2021[32]), introduced Rules[33] which requires social media companies with significant presence to register in the country, establish physical country offices and engage in data localization. It also enforces a fixed turnaround time to block content as per directions from the government, a condition India too has introduced, compelling platforms to remove or disable access within 36 hours of receiving a directive from government to remote content (Ministry of Information & Broadcasting, 2021). Sri Lanka, on the other hand, is considering introducing laws to regulate online falsehoods, modelled after Singapore's Protection from Online Falsehoods and Manipulation Act. Experts have expressed concerns about importing laws from Singapore, which has a vastly different nature of state and history of how policies are used[34].

6. Prospects for Regional Cooperation

South Asian and Indian Ocean regional cooperation in digital technologies have lagged far behind cooperation in areas like trade, agriculture, finance and fisheries. Some regional and sub-regional initiatives in cybersecurity are underway, but not more broadly on the digital economy. The SAARC Secretariat has acknowledged cybercrimes as an emerging focus area, but this too in the context of transnational crime. The regional bloc has also set up a SAARC Cyber Crimes Monitoring Desk. In August 2021, India, Sri Lanka, and the Maldives agreed to jointly work on cybersecurity (among three other pillars of security - marine security, human trafficking, and counter-terrorism)[35]. Interestingly, there are some regional cooperation in the wider region being driven by technology companies themselves, most notably Microsoft Corporation. In 2021, the US-based tech giant launched the 'Asia Pacific Public Sector Cyber Security Executive Council', which brings together policy makers from 15 countries (none of whom are from South Asia) and technology and industry leaders. There has been some cohesion from the wider Asia-Pacific region in the personal data protection space. For instance, all 21 member economies of the Asia-Pacific Economic Cooperation (APEC) developed Cross-Border Privacy Rules (CBPR), a data privacy certification that companies can join to demonstrate compliance[36]. It is, however, an approach that promotes

[26] 145 days of internet shutdown in Kashmir, no word on service restoration. (2019, December 27). The Economic Times. https://economictimes.indiatimes.com/news/politics-and-nation/145-days-of-internet-shutdown-in-kashmir-no-word-on-service-restoration/articleshow/72996839.cms?from=mdr.

[27] Sri Lanka blocks social media for third time in one month. (2019, May 13). Netblocks. https://netblocks.org/reports/sri-lanka-blocks-social-media-for-third-time-in-one-month-M8JRjg80.

[28] Social media restricted in Sri Lanka as emergency declared amid protests. (2022, April 2). Netblocks. https://netblocks.org/reports/social-media-restricted-in-sri-lanka-as-emergency-declared-amid-protests-JA6ROrAQ.

[29] Facebook services restricted in Bangladesh amid anti-Modi protests. (2021, March 26). Netblocks. https://netblocks.org/reports/facebook-services-restricted-in-bangladesh-amid-anti-modi-protests-JA6pqEyQ.

[30] Shrivastava, R. (2021, December 1). No internet shutdown, have selective ban on FB, Whatsapp during unrest: Parliamentary panel to Government. India Today. https://www.indiatoday.in/india/story/no-internet-shutdown-selective-bans-on-fb-whatsapp-during-unrest-parliamentary-panel-1883026-2021-12-01.

[31] Asia Internet Coalition. (2020, December 5). Removal and Blocking of Unlawful Content (Procedure, Oversight and Safeguards) Rules 2020. https://aicasia.org/wp-content/uploads/2020/12/Industry-letter-to-the-Prime-Minister-Removal-and-Blocking-of-Unlawful-Content-Procedure-Oversight-and-Safeguards-Rules-2020.-1.pdf.

[32] Asia Internet Coalition. (2021, June 28). Industry comments on the Amendment - Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules.https://aicasia.org/wp-content/uploads/2021/06/Asia-Internet-Coalition-AIC-Industry-comments-on-the-Amendment-Removal-and-Blocking-of-Unlawful-Online-Content-Procedure-Oversight-and-Safeguards-Rules_28-June-2021.pdf.

[33] Ministry of Information Technology and Telecommunication (Pakistan). (2020, October 20). Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards), Rules 2020. https://moitt.gov.pk/SiteImage/Misc/files/Corrected%20Version%20of%20Rules.pdf.

[34] Nathaniel, C. (2021, June 7). Sri Lanka to curb fake news on social media. Daily News. http://www.dailynews.lk/2021/06/07/local/251037/sri-lanka-curb-fake-news-social-media.

[35] Srinivasan, M. (2021, November 28). India, Sri Lanka and Maldives to collaborate on security. The Hindu. https://www.thehindu.com/news/international/india-sri-lanka-maldives-to-collaborate-on-security/article61432937.ece.

[36] What is the Cross-Border Privacy Rules System?. (2021, October). Asia Pacific Economic Cooperation. https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.

lesser harmonisation in legislation, than that taken by the African Union through the Malabo Convention on Cyber Security and Data Protection[37]. Track II regional cooperation - sharing insights from ongoing domestic legal and regulatory initiatives, and lessons learnt in digital technology governance, as well as Track II dialogue among civil society and think tanks, would be an important focus area in the coming decade. SAARC should adopt the digital economy as a key topic for future summits, and IORA could include digital technology discussions in their Working Group on Science, Technology, and Innovation.

Ultimately, governance of digital technologies in Sri Lanka, India, Bangladesh, and Pakistan needs to be anchored to domestic socio-economic and institutional realities and regional imperatives, even while they are informed by global good practice and international frameworks. Crafting an effective regional voice through collaborative endeavours should be explored by policymakers and institutions involved in regional cooperation.

-END-

[37] African Union Convention on Cyber Security and Personal Data Protection. (2014, June 27). https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

7. Annexure 1: Summary of South Asian Countries Digital Technology Governance Initiatives

Sri Lanka

Data Protection		Artificial Intelligence		Online Misinformation		Cybersecurity	
Document	**Status & Remarks**	**Document**	**Status & Remarks**	**Document**	**Status & Remarks**	**Document**	**Status & Remarks**
Personal Data Protection Bill 2022	Passed in Parliament in March 2022, after several years of amendment and stakeholder consultation, led by the ICT Agency. Anchored largely to GDPR framework.	AI Policy Framework	Published by SLASSCOM (IT/BPM industry body) in 2019. SLASSCOM began spearheading an initiative to develop an AI Strategy. No government-level official initiatives yet.	Online Falsehood and Manipulation Bill	In October 2021, Minister of Justice Ali Sabri told Parliament that a Cabinet Paper on the Online Falsehood and Manipulation Bill was in the final stages of drafting and was to be introduced soon to control publishing of false information on social media.	Defence Cyber Commands Bill and Cybersecurity Bill	A Cyberseucrity Bill first drafted in 2019. But the President subsequently submitted proposed 2 separate bills be drafted -- a 'Defence Cyber Commands' bill and a separate bill of cybersecurity laws outside the defence purview. Meanwhile a Cybersecurity Strategy has been drafted

Bangladesh

Data Protection		Artificial Intelligence		Online Misinformation		Cybersecurity	
Document	**Status & Remarks**	**Document**	**Status & Remarks**	**Document**	**Status & Remarks**	**Document**	**Status & Remarks**

Personal Data Protection Bill	In drafting stage, as of September 2021	National Strategy for Artificial Intelligence Bangladesh	Published in March 2020	Digital Security Act	Act came into force in October 2018	IT Act 2016	

Pakistan

Data Protection		Artificial Intelligence		Online Misinformation		Cybersecurity	
Document	**Status & Remarks**	**Document**	**Status & Remarks**	**Document**	**Status & Remarks**	**Document**	**Status & Remarks**
Personal Data Protection Bill 2020	In draft stage, stakeholder feedback received, final Bill yet to be submitted to Parliament. It governs collection, storaging and processing of data, similar to many others. Revised Bill from a previous Bill in 2018, and the new draft is much more aligned to EU GDPR, with a view on facilitating internationalization of Pakistani business. Under the proposed Act, a new body -	Presidential Initiative for Artificial Intelligence and Computing	Established in 2018. Primarily an national programme under the President's leadership to promote AI research, knowledge and adoption, and has little focus on policymaking	Citizens Protection (Against Online Harm) Rules 2020	Regulations issued in January 2020 under two Acts Pakistan Telecommunication (Re-organization) Act, 1996 and the Prevention of Electronic Crimes Act, 2016, aimed at "exercising greater control" over digital content produced by Pakistani citizens, particularly on social media. International and domestic NGOs have criticized the government for tightening of control over online social media content	National Cyber Security Policy 2021	Approved by Cabinet of Minister in 2021, following submission by Pakistan Telecommunications Authority. It also provides for the establishment of a new Cybersecurity Agency. As this is a very recent policy, implementation status is to be seen. The new policy aims to support both public and private institutions, including national information systems and

	Data Protection Authority of Pakistan - will be established.				through these Rules.		critical infrastructure.
Prevention of Electronic Crimes Act 2016	Already legislated and in force. Contains significant provisions on data protection. It is unclear how the new Bill's provisions will interplay with this existing Act	National Center of Artificial Intelligence (NCAI)	Established in 2018. A government-supported body functioning as a hub of innovation, scientific research, knowledge transfer to the local economy, and training in the area of Artificial Intelligence (AI).			Prevention of Electronic Crimes Act	Act passed in 2016. Prevention of crimes, defamation and frauds committed through the use of internet-based platforms and employing digital identity Digital Rights groups contest its misuse by law enforcement agencies on protection of civil liberties and freedom of expression using transnational digital platforms

India

Data Protection		Artificial Intelligence		Online Misinformation		Cybersecurity	
Document	**Status & Remarks**	**Document**	**Status & Remarks**	**Document**	**Status & Remarks**	**Document**	**Status & Remarks**
Personal Data Protection Bill (PDPB)	Final draft presented to the Indian parliament in Dec 2021; likely to passed in the next session of parliament, in the first half of 2022. The scope of the Personal Data Protection Bill has undergone an expansion and will now cover both personal and non-personal data. Consent is a significant focus of the Bill, as are the data localisation requirments for businesses.	National Strategy on Artificial Intelligence	Implemented. In pursuance of the AI policy, NITI Aayog has adopted a three-pronged approach – undertaking exploratory proof-of-concept AI projects in various areas, crafting a national strategy for building a vibrant AI ecosystem. NITI Aayog has partnered with several leading AI technology players to implement AI projects in critical areas such as agriculture and health.	Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021	Commenced Feb 2021. Introduced under the Information Technology Act, 2000 ("IT Act")	Information Technology Act (2000)	Enacted in 2000. This law is old, but was updated in 2008

Information Technology Act (2000)	Enacted in 2000. Data protection in India is currently governed by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (“Data Protection Rules”) notified under the Information Technology Act, 2000 (“IT Act”).					National Cybersecurity Policy	There is some lack of clarity on this as this policy came out in 2013, but online information still says the old law governs cybersecurity.
Data Empowerment and Protection Architecture	Open for public comments in Nov 2021. Aims to build over existing regulation through which individuals will be able to share their financial data across banks, insurers, lenders, mutual fund houses, investors, tax collectors, and pension funds in a secure manner.					National Cybersecurity Strategy	Announced in 2020

References

145 days of internet shutdown in Kashmir, no word on service restoration. (2019, December 27). The Economic Times. https://economictimes.indiatimes.com/news/politics-and-nation/145-days-of-internet-shutdown-in-kashmir-no-word-on-service-restoration/articleshow/72996839.cms?from=mdr.

African Union Convention on Cyber Security and Personal Data Protection. (2014, June 27). https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

Asia Internet Coalition. (2020, December 5). Removal and Blocking of Unlawful Content (Procedure, Oversight and Safeguards) Rules 2020. https://aicasia.org/wp-content/uploads/2020/12/Industry-letter-to-the-Prime-Minister-Removal-and-Blocking-of-Unlawful-Content-Procedure-Oversight-and-Safeguards-Rules-2020.-1.pdf.

Asia Internet Coalition. (2021, June 28). Industry comments on the Amendment - Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules. https://aicasia.org/wp-content/uploads/2021/06/Asia-Internet-Coalition-AIC-Industry-comments-on-the-Amendment-Removal-and-Blocking-of-Unlawful-Online-Content-Procedure-Oversight-and-Safeguards-Rules_28-June-2021.pdf.

Bhardwaj, D. (2021, October 27). Centre planning separate cybersecurity policy. Hindustan Times. https://www.hindustantimes.com/india-news/centre-looks-at-making-cybersecurity-an-independent-law-may-include-focus-on-emerging-tech-101635274397673.html.

Biyagamage, H. (2019, June 27). SLASSCOM launches Sri Lanka's first AI policy framework. Daily FT. https://www.ft.lk/Front-Page/SLASSCOM-launches-Sri-Lanka-s-first-AI-policy-framework/44-680805.

Does the GDPR apply to companies outside of the EU?. (Date). GDPR. EU. https://gdpr.eu/companies-outside-of-europe/.

Facebook services restricted in Bangladesh amid anti-Modi protests. (2021, March 26). Netblocks. https://netblocks.org/reports/facebook-services-restricted-in-bangladesh-amid-anti-modi-protests-JA6pqEyQ.

Government to Introduce National Artificial Intelligence Policy Soon: Amin. (2021, December 6). Daily Times. https://dailytimes.com.pk/850869/govt-to-introduce-national-artificial-intelligence-policy-soon-amin/.

Information and Communication Technology Division of the People's Republic of Bangladesh. (2019). National Strategy for Artificial Intelligence Bangladesh.https://ictd.gov.bd/sites/default/files/files/ictd.portal.gov.bd/legislative_information/c2fafbbe_599c_48e2_bae7_bfa15e0d745d/National%20Strategy%20for%20Artificial%20Intellgence%20-%20Bangladesh%20.pdf.

Justice K.S. Puttaswamy and Another v Union of India and Others (2017) 10 SCC 1 (India). https://translaw.clpr.org.in/wp-content/uploads/2021/12/Justice-K.S.-Puttaswamy-.pdf.

Khaira, R.,Sethi, A.,Sathe, G. (2018, September 11). UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm. Huffpost.https://www.huffpost.com/archive/in/entry/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472.

Marda, V. (2020, July). India and Global Artificial Intelligence Governance. India and Digital Worldmaking. https://www.india-seminar.com/2020/731/731_vidushi_marda.htm.

Mayer-Schonberger, V., Cukier, K. (2013). Big Data: A Revolution that Will Transform how We Live, Work and Think. Houghton Mifflin Harcourt. https://books.google.lk/books/about/Big_Data.html?id=uy4lh-WEhhIC&redir_esc=y.

Microsoft Asia News Center (2016, June 7). Malware Infection Index 2016 highlights key threats undermining cyber security In Asia Pacific: Microsoft Report. Microsoft. https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016-highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoft-report/.

Ministry of Information Technology and Telecommunication (Pakistan). (2020, October 20). Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards), Rules 2020. https://moitt.gov.pk/SiteImage/Misc/files/Corrected%20Version%20of%20Rules.pdf.

Natarajan, A., Murali, V. (2020, March). Regulating Artificial Intelligence in South Asia: Projections for the Future. ISAS and KAS. https://www.isas.nus.edu.sg/wp-content/uploads/2020/03/ISAS-KAS-AI-Special-Report.pdf.

Nathaniel, C. (2021, June 7). Sri Lanka to curb fake news on social media. Daily News. http://www.dailynews.lk/2021/06/07/local/251037/sri-lanka-curb-fake-news-social-media.

NITI Aayog. (2021). Responsible AI #AIFORALL. https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf.

Personal Data Protection Bill 2019 (Pakistan). https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft_docx.pdf.

Shrivastava, R. (2021, December 1). No internet shutdown, have selective ban on FB, Whatsapp during unrest: Parliamentary panel to Government. India Today. https://www.indiatoday.in/india/story/no-internet-shutdown-selective-bans-on-fb-whatsapp-during-unrest-parliamentary-panel-1883026-2021-12-01.

Social media restricted in Sri Lanka as emergency declared amid protests. (2022, April 2). Netblocks. https://netblocks.org/reports/social-media-restricted-in-sri-lanka-as-emergency-declared-amid-protests-JA6ROrAQ.

Sri Lanka blocks social media for third time in one month. (2019, May 13). Netblocks. https://netblocks.org/reports/sri-lanka-blocks-social-media-for-third-time-in-one-month-M8JRjg80.

Srinivasan, M. (2021, November 28). India, Sri Lanka and Maldives to collaborate on security. The Hindu. https://www.thehindu.com/news/international/india-sri-lanka-maldives-to-collaborate-on-security/article61432937.ece.

Taye, B. (2018, July 23). India cuts internet access for school exams, doubles down on rights-harming shutdowns. accessnow. https://www.accessnow.org/india-cuts-internet-access-for-school-exams-doubles-down-on-rights-harming-shutdowns/.

The Chamber Academy. (2021, August 12). Discussion and Overview of the Data Protection Bill [Video]. YouTube. https://www.youtube.com/watch?v=yDHqFabiUrk.

The Chamber Academy. (2021, August 12). Discussion and Overview of the Data Protection Bill [Video]. YouTube. https://www.youtube.com/watch?v=yDHqFabiUrk.

Vidhi Centre for Legal Policy. (2022, January 22). From PDP Bill, 2019 to Data Protection Bill, 2021 and Beyond-A Roundtable Discussion [Video]. YouTube. https://www.youtube.com/watch?v=mk3HnNQp0Jc.

What is personal data?. Information Commissioner's Office. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.

What is the Cross-Border Privacy Rules System?. (2021, October). Asia Pacific Economic Cooperation. https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.

Yadav, K., Thange, I., Ilhardt, J., Siwakoti, S., Shapiro, J. (2020, November 25). Old hatreds fuel online misinformation about COVID-19 In South Asia. Bulletin of the Atomic Scientists. https://thebulletin.org/2020/11/old-hatreds-fuel-online-misinformation-about-covid-19-in-south-asia/.