BAUET JOURNAL
Published by
Bangladesh Army University of Engineering & Technology
Journal Homepage: http://journal.bauet.ac.bd
https://doi.org/10.59321/BAUETJ.V4I1.23

Comparative Analysis of Data Protection Laws Among the SAARC Countries: An Appraisal

Ahmed Adib[1], Mehrab Hasan[2]

[1]*Advocate, Supreme Court of Bangladesh*
[2]*Advocate, District & Sessions Judge Court, Dhaka*

Abstract: Undergoing the blessings of globalization, the seemingly less developed countries are also coping with digital cultures and industries. As economic and social events, at a large scale, are moving online; the importance of data and privacy protection is being recognized accordingly. Unfortunately, the current law and structure for data protection are incompetent and vividly fragmented with global, regional, and national approaches. In these circumstances, this qualitative research, considering the international laws and standards, especially the 'General Data Protection Regulation (hereinafter "GDPR")', has attempted to review the present laws and to analyze probable roadmaps for making efficient data protection strategies for the 'South Asian Association for Regional Cooperation (SAARC)' (hereinafter "SAARC") countries. The findings and outcomes of the study, pondering over the absence of effective laws and lacunas or loopholes in the existing regulations to shield the privacy of the citizens in the era of fourth industrial revolution (4IR), aim at paving the way for improving the much-needed framework to enact and implement data protection enactments in the SAARC region.

Keywords: *SAARC, Data Protection, Privacy, Information, GDPR.*

Introduction: Data means information, i.e., information about persons, things or institutions; or facts or numbers collected to check; or information in an electronic form [1]. In other words, Data is information or facts which are stored in electronic form and collected to peruse or examine [2]. Personal data commonly refers to the data or information that is related to a person who can easily be identified by the information or data, whether collected and accumulated by any government or any organization (being either public or private) or authority [3].

Data protection means the process of safeguarding data from data breach, corruption or loss. It aims to protect information relating to the person, i.e., name, birth date, photo, email address, mobile number, etc. It ensures that information does not go to the wrong hand and is not exchanged with the third party without the consent of the individuals [3]. Data protection is a species of privacy laws and policies that aims at minimizing breach of one's privacy by means of collection and storage; transfer of personal data or information [3].

Data protection is a novice form of right to privacy as earlier traditional eavesdropping or wiretapping was mostly the only tool used for the violation of the right to privacy [4]. Laws and circumstances have changed over the lapse of time. Developed countries, i.e., states of the EU and the US, started modifying their privacy and data protection enactments by inserting provisions regulating data protection since 1970s.

Such privacy laws are titled differently in different states. As for instance, the 'Digital Security Act' of Bangladesh is called 'Cyber Security Act' in other countries. Moreover, sometimes the same is termed as 'Prevention of Electronic Crimes Act' or 'Data Protection Act', etc. Regardless of the title of the Act, the preambles or the philosophies of the legislation remain almost identical all the time.

When computers became available and communication technologies started becoming familiar, the urge for data privacy was realized. The developed countries, saying more specifically – 'the westerners', tried their level best to enact laws relating to data privacy and enforce them. Such a phenomenon is, however, hardly observed in Asian countries and the SAARC countries are lagging far behind. The SAARC comprises eight countries, i.e., Afghanistan, Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan and Sri Lanka. Progress in privacy (and data) protection in South Asia has been delayed for many reasons, but there are, nowadays, some motives for optimism [5]. There is, unfortunately, no relevant regional progress resulting from the SAARC agreements, however, one of the most momentous regional factors is the possible implications of the decision made by the Indian Supreme Court on the (fundamental constitutional) right of privacy [5].

In this present global information economy, personal data (or individual information), has been converting into the fuel driving much of present online activities and movements since the inception of computers and other analogous revolutionary digital devices. Nowadays, as a result of developments in the field of Information and Communication Technology, a huge amount of information and data are uploaded online; collected, transferred and stored around the world. Financial, economic, educational activities including governmental services and activities; and social and religious events and activities, in developed and developing countries, have been made easier to be shared through internet connectivity and availability of mobile phones.

Article history:
Received on 25 March 2023
Received in revised form 12May 2023
Accepted 15 October 2023
Available online 15 November 2023

Corresponding author details: Ahmed Adib
E-mail address: aadib.law@gmail.com
Tel: +8801869113851

The research article aims to provide a basic guideline, to the lawmaker and the future researcher, to show the way how to develop privacy and data protection regime. The authors, to be specific, focused on highlighting the inadequacy of data protection laws, and scrutinized the enforced privacy and data protection laws compared to GDPR. Therefore, the upcoming lawmakers and researchers will be able to assess the importance and effectiveness of data protection laws in near future.

International Laws on Data Protection: As mentioned earlier, data protection is a new form of right to privacy. Before the emergence of computers, mobile phones, and other apparatus having the same effect, there was no terminology for 'data protection'. For a better understanding, we can consider 'right to privacy' as a genus and 'data protection' as a species.

Universal Declaration on Human Rights (UDHR), 1948 emphasizes the protection of privacy of a person, his family, home and correspondence [6]. The person shall be entitled to the protection of law enacted by the state. United Nations International Covenant on Civil and Political Rights (ICCPR), 1966 confirms the same [7].

UN Convention on the Rights of the Child (CRC), 1989 seeks the protection of the data of the child [8]. It prohibits unlawful interference with the right to privacy. The United Nations International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990 protects the information of the migrant worker from arbitrary and unlawful interference [9].

There are some regional conventions which ensure data protection as well. Cairo Declaration on Human Rights in Islam, 1990 denotes that every person has the right to privacy. It is prohibited to spy on anybody and to scandalize one's reputation [10]. The Asia Pacific Economic Cooperation Privacy Framework has established common sets of privacy protection and data peruse [11].

Overviewing the General Data Protection Regulation (GDPR), 2016: Data protection regulation titled 'General Data Protection Regulation (GDPR)' was enacted by the European Union (hereinafter "EU") in 2016 to protect and promote a regional strategy for data protection as a fundamental right. Personal data protection is one of the important rights of the citizen and it makes one feel safe from unlawful breach of his/her personal data [12]. The existence of the Regulation, 2016 will work as public international law and inspire the state to enact laws for the protection of privacy and data and to introduce legal frameworks providing remedy to the victim of privacy or data breach [13].

Nowadays, the use of information and communication technology has been increasing speedily. Therefore, people are sharing their personal data on vivid websites and they are concerned about their privacy and data breach. This crisis led to the introduction of a legal framework around the world. GDPR is the first step that has been taken by the EU for their party States [14]. GDPR upholds six prime principles as Fairness, Lawfulness and Transparency; Confidentiality; Accuracy; Data Minimization; Purpose Limitation; and Accountability [15].

The regulation is effective on organization or people all over the world storing and managing information of EU citizens and the EU States. The regulation sets rights including privacy protection [15, Article 15] and the right to forget personal data [15, Article 17] as well. A State is required to employ a data protection officer to manage the data and to inform data breach to the affected person within 72 hours [15, Article 33]. The officer will provide a report to the victim which must include the plan for the recovery of data and mitigating the consequences [15, Article 34]. The Regulation holds penal provisions as well. The organizations which violate the provisions of GDPR shall be liable to pay fines [15, Article 83, 84]. The maximum fine is 20 million Euros or 4% of the annual revenue of the organization, whichever is higher [15, Article 84(5)].

The GDPR sets standards that no organization or State would risk to ignore and other States will be inspired to enact national laws and policies to protect the data of the citizen. Now, a question may be raised as to whether the SAARC countries should comply with the provisions of GDPR or not. The EU sets that the State, while storing and managing data of EU citizens, must comply with the provision of GDPR. The SAARC countries while commencing business with EU countries must follow the regulation [16]. Japan has already expressed its will to enact laws similar to the GDPR. The UK is making efforts to make GDPR the norm in the post-Brexit era. The SAARC can take the GDPR as a directive while enacting laws and organizing legal frameworks to protect the privacy of the citizens [17]. It should, however, be borne in mind that Sri Lanka has already enacted laws regarding Data protection complying with the provisions of GDPR.

The emerging modern technologies, nowadays, are generating a huge amount of data, and it is significant to take steps to secure the collection, processing, transmission and access of data [18]. As a huge number of data is being created daily, it will create conflict within the process of collection and protection of data, especially in terms of privacy. Undoubtedly, the GDPR has an impact on how data is stored and managed within and outside the EU and the regulation plays a significant role in enacting data protection legislation worldwide [18]. The regulation can be regarded as a 'privacy law model' practiced all around the world.

The GDPR is effective for the majority of organizations all over the world that collect and store the EU's personal data. If the SAARC States conduct business with the EU residents or organizations and offer them options to sign up for services, the SAARC states will be a subject of the GDPR. Moreover, the SAARC countries' business will be bounded by the GDPR for many reasons, such as the contractual relations and obligations to the EU or their responsibilities to suppliers or allies. Moreover, the functions of data controllers or data processors are significant. Accordingly, SAARC countries' companies will fall within the

ambit of the GDPR while processing activities of their co-data controllers or processors. Furthermore, non-compliance with the GDPR outside the EU will disapprove the business relations among the parties. The same will be applied to the Controllers or Processors in the SAARC countries [19].

Initiatives Taken by the SAARC Countries:

Bangladesh: The notion of data privacy and the underlying protection requirements and rights are new in the context of our country. Moreover, it has, in this era of digitalization, hardly emphasized ICT development, artificial intelligence, electronic communication, social networking, cyber-crimes, and to aware users about privacy protection [20]. Recently, (along with the Constitution of Bangladesh) the Digital Security Act, 2018 and the Information and Communication Technology Act, 2006 have started guaranteeing the right to privacy and making framework for data protection [20].

The Constitution [21] of Bangladesh safeguards citizens' privacy of communication and correspondence; however, this provision is not exhaustive to prevent the breach of privacy caused by individual or by an institution [22]. The ICT Act [23] of Bangladesh was envisioned to provide the legal recognition and framework for digital signatures, controller of certifying authorities and electronic records [22]. It was not projected to deal with data privacy or protection and nowadays it is not supposed to protect data privacy as well [22]. Nevertheless, the Govt. has enacted the Digital Security Act 2018, which is commonly recognized as the Cyber Security Act in other countries and jurisdictions, aims at promoting confidentiality, availability and integrity of public and private information networks (and systems) to protect individuals' rights, freedoms and privacy, economic and financial interests and security in cyberspace [22]. Consequently, the intrinsic purposes of the Digital Security Act, 2018 and the ICT Act, 2006 are not completely identical.

On the contrary, the EU, having an effective and operative data protection and privacy legal framework, has recently allowed its courts to decree that one of the giant data companies, i.e., Facebook Inc., violated and dishonored its citizens' privacy for assisting the indiscriminate and mass surveillance carried out by the intelligence services of a highly influential state [24]. Without proper shield or protection in action, a least developed country like Bangladesh may not be aware of how fatal the future of its citizens could be [24].

India: Right to privacy, in India, is promised to be protected as a constitutional right which includes right to personal liberty, right to life, freedom of expression. However, the issue has extended a debate questioning its nature and scope; whether it is judicially enforceable or not [25]. In August 2017, in ***Justice K S Puttaswamy and Anr. v. Union of India and Ors*** [26]**,** a judgment rendered by ("Puttaswamy") a bench of nine judges of the Supreme Court of India (hereinafter as "the Supreme Court"), unanimously opined that the right relating to privacy was an intrinsic comp0onent of the promise of the right to life and right to personal liberty as protected under the ambit of Article 21 of the Constitution of India that encompassed, at its core, a negative obligation of not violating the right to privacy and a positive obligation of taking all necessary measures to protect the rights relating to privacy [25]. *Puttaswamy* has modified the outlines of Indian privacy law, added a new interpretation of the existing privacy rules, and also raised the spectre of a (robust) common law tort for the breach of the right to privacy, independent of statutory guidelines and rules [25]. The Supreme Court has further clarified that any law encroaching upon the right to privacy would be an issue of (Constitutional) scrutiny, and would have to satisfy the three-fold prerequisite: legality; necessity; and proportionality [25].

Furthermore, the Supreme Court has made an obligation on the Govt. to enact laws that adequately protect privacy relating rights. Several High Courts are recently dealing with data and privacy protection issues that include but are not limited to the export of data, adequacy of consensus or consent from a post-*Puttaswamy* viewpoint and transmission of data/information between group companies. While a vibrant judicial movement cannot be identified, it is palpable that data collection, managing and processing efforts in India must assess and anticipate the influence of *Puttaswamy* on Indian laws relating to data [25].

The Indian Govt. wants Facebook and Google, the global tech giants, to store and accumulate sensitive data/information of users locally, but critics opine that such actions might make users more permeable to official surveillance [27]. However, a (public) debate on the Indian government with a view to accumulating personal or private information for biometric characterization, i.e., Aadhaar along with ponderings over the EU data protection strategies are, however, continually pushing the state to espouse a Personal Data Protection (hereinafter as "PDP") legislation [27]. It is projected that the bill (of the legislation) will be passed by the parliament without any inordinate delay and will eventually be an enactment. Moreover, aficionados of the bill have been considering it timely and appropriate legislation which will be analogous to the (privacy) laws that are in existence in the European Union and in the United States [27].

Pakistan: The Constitution of the Islamic Republic of Pakistan incorporates the fundamental right to privacy under Article 14(1) of the Constitution which safeguards the 'privacy of home' and in **M.D. Tahir versus the Director, State Bank of Pakistan, Lahore and 3 others** [28], judgment was rendered by the High Court of Lahore mentioning that the assemblage of personal (or

private) information sans any allegation of misconduct or unauthorized work done by people (from all walks of life) is an unwarranted breach of (the fundamental) right to privacy [29].

The Prevention of Electronic Crimes Act, 2016 (hereinafter "PECA") is a primary legislation dealing with protection of data in Pakistan. The PECA, being promulgated on 18th August 2016, aims at controlling and preventing offences (or unauthorized activities) regarding information technology or systems. Furthermore, the (seemingly both substantive and procedural) law deals with provisions for mentioned offences along with the procedures of investigation and prosecution for the crimes. Interestingly, international cooperation to confront electronic crimes collectively is also incorporated by the same [29]. At present, however, there is no definite law relating to data protection in Pakistan. However, the Ministry of Information Technology and Telecommunication in April of the year, 2020 issued a (consultation) draft on Pakistan Personal Data Protection Bill, 2020 [30]. After successful completion of the discussion phase, all necessary endeavors will be taken and the bill will be placed (for debate and passage) before the Parliament. The enactment will hopefully be promulgated soon through the assent of the President subject to being passed by the Parliament [30].

Sri Lanka: The Constitution of Sri Lanka, enacted in 1978, did not hold any provision to protect the right to privacy as a constitutional right in Chapter three of fundamental rights [31]. Nevertheless, the revised Constitution of the Democratic Socialist Republic of Sri Lanka (as amended in 2015) through Article 14A has mentioned privacy considerations within the periphery of restrictions to the right to 'access to information' [31]. The Constitution of Sri Lanka, as per Article 14A, ensures the citizen's right to access to information, provided by the citizens for the exercise and protection of citizen's rights, which is stored by the State, the ministry, any other department of the state, or local authority, or any person [31]. However, the State can impose restrictions on such right if the exposure of the information is likely to destroy public peace, state security, public health and morals, and it is necessary for the prevention of contempt of courts, parliamentary privileges and confidentiality, and to uphold the dignity and impartiality of the Judiciary [31].

Even though Sri Lanka does not have any definite laws for the protection of the right to privacy or data protection, certain provisions of law may be considered relevant to privacy rights in cyberspace. However, there are a few data protection-enabled legislations which are industry-oriented. Such legislations do not even define the term 'data' nor do have any specific provisions for its implementation. Other laws regulating and protecting privacy and data protection include: The Banking Act [32]; The Telecommunications Act [33]; The Intellectual Property Act [34]; The Electronic Transactions Act [35]; The Computer Crime Act [36]; The Right to Information Act [37]. Particularly, the Computer Crime Act, through penal sanctions, addresses a matter that encompasses data that has been obtained without due course of law, the unauthorized collection and unconsented disclosure of data [31]. In addition, following the standards set by the UN Commission on International Trade Law (UNCITRAL); the Model Law on Electronic Commerce, 1996 and the Model Law on Electronic Signatures, 2001, the Electronic Transaction Act was drafted. Afterwards, the Act came into force, being acknowledged by Gazette Extraordinary No. 1516/25, on September 27, 2007 [31].

Notably, the Legal Draftsman's Department (LDD) and the Ministry of Digital Infrastructure and Information Technology (MDIIT) have launched a draft bill for an Act to Provide for the Regulation of Processing Personal Data 2019 [38] which provides data protection and fundamental principles of privacy.

Nepal: The following are the existing laws in Nepal that regulate the issues regarding privacy: Constitution of Nepal [39]; Individual Privacy Act, 2018; The Civil Code, 2017; The Criminal Code, 2017 [40]; The Labour Regulations, 2017.

The Government of Nepal (hereinafter "GON") has recently drafted a bill relating to information technology and placed the same before the Parliament for discussion [41]. The provisions of the proposed bill, however, are subject to modification before its enforcement as an enactment [41]. Moreover, the govt. is yet to enact a regulation corresponding to the Act.

In ***Sapana Pradhan Malla v. Office of the Prime Minister and Council of Ministers & Others*** [42], the Supreme Court ruled that the right to privacy as guaranteed by the Constitution must be protected and an exception to this well-established general rule, i.e., information sharing with third parties, can only be made where prior consent has been obtained from the person concerned [41].

In Baburam Aryal ***v. GON*** [43], the Supreme Court held that the right to privacy, being a fundamental right, is guaranteed by the Constitution and should not be violated by the State or by any third party. The Supreme Court further added that under the ambit of the right to privacy, things relating to a person's body, communications, character, documentation, data, residence and property are inviolable except as otherwise permitted by any law. An entity (that may be either a natural or legal person) that collects and assembles information, has undertaken an obligation for such information and such information shall not be used whimsically at its discretion [41]. Instead, such an entity or department must shield such a 'data bank' of information by hook or by crook. The Supreme Court also laid down that the entity must not allow unwarranted and unauthorized access to such a 'data bank', even as a special case in the absence of a lucid legal basis [41].

Bhutan: Bhutan enacted the Information, Communications and Media Act of Bhutan 2018 [44] in 2017 which came into force in mid-2018 [45]. Even though the data protection principles incorporated in the Act are stated summarily, they are doing more than giving Bhutan a nominal data privacy law because they contain seven of the ten 'second generation' principles enshrined in the 1995 EU Data Protection Directive and thus form moderately strong legislation for the Asian region [45].

Chapter 17 of this Act deals with 'protection of offline or online privacy' which requires organizations to shield personal information taken from consumers or users, as well as sensitive personal/private information (that is defined) [46]. The organizations must have a practical privacy policy that encircles the purposes for which data or information may be received, collected and used. Any type of collection, disclosure and use is restricted to a reasonable person who is considered fit and appropriate in any specific circumstances. Users and consumers can require information or data to be removed [45].

Chapter 21 of the Act states that 'Data Protection' encompasses quite a comprehensive data privacy code that in some cases repeats what Chapter 17 mentions, but in a more rigid and strict form, and with more lucidity concerning offences and compensations. The heading of the chapter seems to bound it to data collected electronically [45]. Collection, disclosure and processing of personal information necessitate written permission, agreement or authority of law. In case of failure to protect information or data by judicious security practices, unlawful or unwarranted disclosure of data, and unethical copying of data, all constitute offences and liabilities to pay compensation or fine [45]. The Act has also established an independent "Bhutan Infocomm and Media Authority", and an 'office of consumer protection', which have the authority to investigate and deal with complaints, with the rights to appeal to an appellate tribunal and also to the courts [45].

Afghanistan: The people of Afghanistan have been increasing the use of technologies and making different ways of life. Therefore, it is important to enact specific laws and establish a legal framework to store, manage and protect the data [47]. The constitution of Afghanistan ensures the rights of the citizen to protect their privacy and confidentiality while using telecommunications [47]. It ensures the protection of letters and information from intrusion. The constitution of Afghanistan was enacted in 2004 and it addresses the aspects of protecting data including freedom of expression [48]; confidentiality of conversation, correspondence and communication [48, Article 37]; personal liberty and dignity [48, Article 24]; right to access to information [48, Article 50] in the state departments. However, there is no specific law protecting the data of the citizen. Therefore, it is yet to take steps to develop privacy laws. Moreover, the state is undergoing war and it is unrealistic to have any prospect of privacy laws [49]. However, the unending war does not resist a person from his inalienable right to data protection *per se*. The state should tend to shield the privacy rights of its citizens.

Maldives: The constitution of Maldives and the penal code of the country hold the provision relating to the protection of privacy. The penal code forbids acquiring and disclosing personal information, and important information without prior license or authority [47]. The Ministry of Economic Development of the Maldives in 2016 declared that it would enact a new law to protect the data [50]. The main purpose of the law was to develop the business sector and e-commerce and to the information of the customers. The bill has been drafted in 2017 but is yet to be an Act [51]. The limitation of the bill is that it has no penal provision for non-compliance with the provisions.

Appraisal of the SAARC Countries Compliance with the GDPR, 2016:

Afghanistan: In Afghanistan, there is no law that complies with the GDPR, 2016. The State enacted the Access to the Information Law as per Article 50 of the Constitution in 2018. The law ensures the denial of access to information to protect privacy [52]. In effect, the state has to walk a long way to comply with the GDPR.

Bangladesh: In Bangladesh, Article 43 of the Constitution ensures the right to privacy in the home, correspondence and communications. Another article protects the right to life and individual liberty [21, Article 32]; the Penal Code, 1860 protects the modesty, and privacy of women [53]; the Information and Communication Technology Act, 2006 [54] protects privacy from disclosures and holds the penalty provision of imprisonment up to 2 years, or fine of 2 lac or both; the Digital Security Act, 2018 prohibits the illegal transfer of personal data [55]. However, there is no law similar to the GDPR. The state has drafted a bill titled 'Data Protection and Privacy Rules, 2019' to protect privacy and data. The law was drafted to fulfill the aim of section 60 of the Digital Security Act, 2018. It does not comply with the standard of OECD (Organization for Economic Co-operation and Development) guidelines. As it is a bill, the government can review it at any time. Therefore, the state's privacy law is still in its infancy [56].

Bhutan: Bhutan has enacted the Information, Communication and Media Act, 2017 which has been enforced since 2018. The law has highlighted the principles of GDPR, 2016, definition of data [57], State's responsibilities to protect data [57, Section 179] and e-governance [57, Section 271], online privacy [57, Section 336-43], security of payment and information [57, Section 344-46], email [57, Section 347], information of children [57, Section 348-51], breach of confidentiality [57, Section 391], and vivid offenses and punishments. Therefore, there is a data protection regime in the State.

India: Article 19(1) and 21 of the Constitution of India states that privacy is a constitutional right of the citizen. Another law 'the Information Technology Act, 2000' holds provisions including the right to privacy, personal data and data protection [58]. The Information Technology Rules, 2008 have privacy-related issues that include personal data [59] and protection of sensitive data [59, Section 2]. However, there is no law equivalent to GDPR. The state has drafted a bill, i.e., 'Personal Data Protection Bill, 2019' in which there is a lacuna that it excluded the central government from the scope of the Act. On this point, Justice B. N. Srikrishna quoted that it would make India an 'Orwellian Country'. However, the Personal Data Protection Bill 2019 is a beginning for India to a successful step in the regime of data protection [60].

Maldives: In 2006, Maldives ratified the ICCPR and signed its Optional Protocol. So, the state has to comply with Article 17 of the convention to address the privacy of the citizens. Though the constitution of Maldives safeguards the right to privacy, the same is, however, not enforceable by a court of law. The Right to Information Act, 2014 is the only Act that grips the provision relating to privacy protection [61]. The state has drafted a bill titled 'Privacy and Data Protection Bill' which aims to promote e-commerce and medium enterprise [62]. No law there complies with the provisions of GDPR and the country, thus, has a feeble data protection legal framework.

Nepal: Though the Constitution of Nepal ensures right to privacy and the right to information, there is no legislation similar to the GDPR except the Privacy Act, 2018. However, the Act has recognized privacy protection including personal information, protection of body and family, residence, property, document, data, [63] etc. but failed to address the problems relating to email address, IP address, social media and personal website.

Pakistan: The Electronic Crimes Act, 2016 contains the provision regarding the right to privacy and personal information. However, there is no law in line with the GDPR, except the Personal Data Protection Bill, 2018 [64]. It incorporates various provisions, including the definition of personal data [65]; sensitive personal data [65, Section 2(n)]; protection of personal data [65, Section 12]; right of access to personal data [65, Section 15]; right to correction of personal data [65, Section 23]; processing of sensitive personal data [65], etc. In comparison with GDPR, the Personal Data Protection Bill, 2018 only applies to personal data processing relating to business transactions. The bill does not include biometric and genetic data [64]. Therefore, its scope seems to be limited. Moreover, it has not dealt with comprehensive rights of data and privacy protection, and omitted institutional framework to enforce the law.

Sri Lanka: Sri Lanka enacted the Computer Crimes Act, 2007 which contains vivid crimes regarding data protection and compensatory clause for violation of provisions [66]. The Act contains provisions including unlawful entry issues; unapproved modifications; unlawfully obtained information; unauthorized interference, and other related crimes [66]. The state has enacted the Personal Data Protection Bill, 2019 which amended the Data Protection Framework. The bill, being influenced by the EU GDPR, became an Act in 2022 titled the 'Personal Data Protection Act, 2022'. Sri Lanka, thus, became the first SAARC country to enact complete privacy legislation [67]. There are, however, also dissimilarities between the Act of 2022 and the GDPR, 2016. The Act does not tend to protect sensitive personal data and imposes lesser punishment [67].

Findings and Recommendations: From the discussion above, it is conclusive that there is less progress within the SAARC countries regarding data privacy laws. SAARC countries' data privacy regimes have not matured enough, but have just started with significant shortcomings. In most cases, being contrary to international norms, SAARC countries do not have adequate data privacy legislation. Both Bhutan and Nepal have weak special laws in South Asia, while India and Pakistan are seeking to pass data protection bills. Though the Personal Data Protection Act, 2022 has lacuna, Sri Lanka has eventually managed to enact a complete legislation [68]. Bangladesh is committed with a view to adopting a privacy and data protection law shortly [69], while there is no substantial progress in Afghanistan and Maldives. The EU's approach to data protection laws, currently promoted by the GDPR, is the right option for the SAARC countries.

The SAARC countries' privacy regime does not comply with the EU standard as discussed earlier. Despite constitutional recognition, there is hardly any solid legal framework to protect data and privacy except in Sri Lanka. Moreover, it is lucid that South Asian culture is different than that of the EU and Western regions. But things (including cultures) are now changing today. The SAARC countries, failing to find any effective way out to combat the problem, i.e., breach of privacy or confronting various (legal or natural) persons to ensure data protection, have already started taking initiatives to enact data protection and privacy protection laws.

The private sectors must be very vigilant to shield their data and privacy upon which business actions are (being) taken [70]. It must include rigorous training of their employees on data security, application of secure technology, compliance with the preset data protection laws, assessment of the vulnerability and data breach response plan, etc. [58].

The SAARC states should take initiatives to implement a joint multilayered policy which will address privacy protection strictly, privacy breach impact assessment, and respond to data breaches as soon as possible and the States should, before exacerbating the situations, enact efficient data privacy laws and make people aware about it [71]. The state can, however, take interim measures, such as conducting research and showing a list of vulnerable sectors of data breaches and forcing industries and organizations to take licenses before collecting and storing data [72].

The SAARC countries must follow the GDPR standard to enact laws to protect the privacy and data of the citizens. The African, Caribbean, Latin American and even the ASEAN (ASEAN consists of ten Southeast Asian states – Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam – into one organization. ASEAN's success has facilitated support for regional security and affluence for over 50 years and it is uniquely placed to address grave regional issues) nations [73] have introduced privacy laws following the GDPR guidance and taken regional initiatives of the same types [74]. As no regional initiatives have been taken by the SAARC, it is necessary to adopt measures by the SAARC to shield the data protection rights;

In these circumstances, let the philosophies be pondered over while enacting legislation in the SAARC countries. The given principles, despite not being exhaustive, might, however, provide an overview of the periphery of expectations of data protection.

Data Protection Agency: The state should establish separate authority to deal with data collection and management. The authority shall protect the data from data breach and do all other related works as prescribed by the existing law.

Transparency and Accuracy: The citizens should have access to the data provided by them in any organization so that they can delete or amend the information at any time. Organizations must not abuse the data collected by them and share data with any unlawful authority, or without the consent of the data provider.

International Standard and Principles: The states should follow the international standard of data protection law, i.e., GDPR, OECD (Organization for Economic Co-operation and Development) guidelines and so forth. Amongst myriad well-established principles, a new dogma, i.e., the 'principle of inter-operational equity' can also be followed (at the time of enacting and applying data protection relating laws) because it refers to a solution towards sustainable data protection (particularly while bridging the gap between right to trade and right to data protection) [75].

Obligatory Data Breach Notification: The organization shall immediately notify the victim whose data has been breached and the notice shall contain a lay-out of recovering the data and mitigating the impact of data breach.

Prosecution: The individual or the organization shall be prosecuted in court for breach of data protection laws. There should be a special court to enforce the law and speedy trial of cases relating to the breach and violation of data protection law.

Penal Provision and Compensation: The data protection law must contain penal provisions for data breaches and violations of provisions of the law. The victim of data breach should be adequately compensated as well.

Regarding all the facts discussed earlier, the authors found that the people of the South Asian Region depend either on the mercy of the government or on the luck that their data and privacy shall not be breached. On the other hand, most of the constitutions of the states hold the Articles, directly or indirectly, to protect the data and privacy of the citizens. The judiciary of the states has, however, started emphasizing the protection of data and privacy of the citizens. The South Asian States, e.g., Maldives, India and Bangladesh are undoubtedly making greater efforts to enact data protection laws; but these laws are hardly appropriate regarding the standard of the GDPR.

Conclusion: If the rest of the countries of the world want to maintain relations, specifically economic and trade relations with the EU, they have to ensure effective data protection and privacy laws. Consequently, it is the global trend that the states follow the GDPR guidelines, and the South Asian States cannot supersede it. The South Asian States, unfortunately, failed to enact their data protection laws following GDPR compliance.

Ineffective data protection laws in the South Asian Region are indeed trampling the overall progress in the world. In this digital era, data protection, directly, has relation with goods and service trade all over the world [76]. The states, to remove this obstacle, should be advised to review and amend their national data protection law and to work in a body to comply with the GDPR principles.

The authors, after paying attention to all these proofs and facts, foresee that the South Asian Region will come forward as a body to take collective steps to enact data protection laws with GDPR compliance. This will provide the region with a great benefit in privacy protection related economy, outsourcing industries, and will finally help the region's economic development.

Although Afghanistan and the Maldives have yet to implement privacy protection, the cyber-security and data protection legislation, enacted by Sri Lanka, Bangladesh and Nepal, will affect the future data protection measures in the region. Moreover, the laws, if enacted and enforced judiciously (and not arbitrarily), have the potential to influence the South Asian Regional digital economy [77]. That is why all the necessary measures ought to be adopted in such a way so that there will be no contradiction between right to trade and right to privacy since both are: inalienable and of equal significance.

References

[1] Data - Definition, Meaning & Synonyms, [Online]; Available at: https://www.vocabulary.com/dictionary/data.
[2] Cambridge Dictionary, DATA | Meaning in the Cambridge English Dictionary, October 2019 [Online]; Available at: https://dictionary.cambridge.org/dictionary/english/data.
[3] P. Crocetti, What is Data Protection and Why is it Important? Definition from WhatIs.com, February 2021 [Online]; Available: https://www.techtarget.com/searchdatabackup/definition/data-protection.
[4] E. L. Fuller, Hardwick v. Bowers: An Attempt to Pull the Meaning of Doe v. Commonwealth's Attorney out of the Closet, Univ. Miami Law Rev., 39(5) (1985) 974.
[5] G. Greenleaf, Privacy in South Asian (SAARC) States: Reasons for Optimism, UNSW Law Res. Ser., (2017) 18–30.
[6] Universal Declaration of Human Rights, 1948, Article 12.
[7] United Nations International Covenant on Civil and Political Rights, 1966, Article 17.
[8] UN Convention on the Rights of the Child, 1989, Article 16.
[9] The United Nations International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990, Article 14.
[10] Cairo Declaration on Human Rights in Islam, 1990, Article 18.
[11] G. Greenleaf, Asia- Pacific Data Privacy: 2011, Year of Revolution?, Kyung Hee Law Journal, (2011) 21-24.
[12] V. Bentotahewa, C. Hewage, and J. Williams, The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries, SN Comput Sci., 3(3) (2022) 1–18.
[13] Guide to the General Data Protection Regulation (GDPR), Information Commissioner's Office, 2019 [Online]; Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
[14] A. Burman, Will a GDPR-Style Data Protection Law Work for India?, Carnegie Endowment for International Peace, (2019) 1–7, [Online]; Available at: https://carnegieindia.org/2019/05/15/will-gdpr-style-data-protection-law-work-for-india-pub-79113.
[15] General Data Protection Regulation (GDPR), 2016, Article 5.
[16] D. Vaile, Data Privacy Law in the Asian Region Review of "Asian Data Privacy Laws -Trade and Human Rights Perspectives" by Graham Greenleaf, Australian Journal of Telecommunications and the Digital Economy, 3 (2015) 60–63.
[17] C. Ryngaert and M. Taylor, The GDPR as Global Data Protection Regulation?, AJIL Unbound, 114 (2020) 5–9.
[18] Balancing Data Protection and Free Flow, APEC (2018) [Online]; Available at: https://www.apec.org/press/features/2018/0319_ppd.
[19] M. T. Islam, M. Sahula, and M. E. Karim, Understanding GDPR: Its Legal Implications and Relevance to South Asian Privacy Regimes, UUM Journal of Legal Studies, 13 (2021) 45–76.
[20] N. Doulah, Bangladesh - Data Protection Overview, (14 May 2020) [Online]; Available at: https://www.dataguidance.com/notes/bangladesh-data-protection-overview.
[21] The Constitution of the People's Republic of Bangladesh, Art. 43(b).
[22] A. B. M. H. Mishbah, Bangladesh Steps into the Data Protection Regime, (8 April 2019) [Online]; Available at: https://www.thedailystar.net/opinion/human-rights/news/bangladesh-steps-the-data-protection-regime-1726351.
[23] The Information & Communication Technology Act, 2006 [Act. No. 39 of 2006].
[24] S. S. Dipon, Necessity of Data Protection Laws, (1 December 2015) [Online]; Available at: https://www.thedailystar.net/law-our-rights/necessity-data-protection-laws-180373.
[25] M. Chacko, A. Misra, and P. Kittane, India - Data Protection Overview (18 February 2020), Data Guidance, [Online]. Available at: https://www.dataguidance.com/notes/india-data-protection-overview.
[26] Writ Petition (Civil) No. 494 of 2012.
[27] India's Personal Data Privacy Law Triggers Surveillance Fears | DW | (11 November 2020) [Online]; Available at: https://www.dw.com/en/indias-personal-data-privacy-law-triggers-surveillance-fears/a-55564949.
[28] 2004 CLD 1680.
[29] S. Rehman and S. Ansari, Pakistan - Data Protection Overview, (3 June 2020) [Online]; Available at: https://www.dataguidance.com/notes/pakistan-data-protection-overview.
[30] S. Khan and S. H. Khan, Data Privacy Comparative Guide - Privacy – Pakistan, [Online]; Available at: https://www.mondaq.com/privacy/1005646/data-privacy-comparative-guide.
[31] M. Sirimane and N. Puvimanasinghe, Sri Lanka - Data Protection Overview, (8 December 2020) [Online], Available at: https://www.dataguidance.com/notes/sri-lanka-data-protection-overview.
[32] The Banking Act (Act No. 30 of 1988).
[33] The Telecommunications Act (Act No. 25 of 1991).
[34] The Intellectual Property Act (Act No. 36 of 2003).
[35] The Electronic Transactions Act (Act No. 19 of 2006).
[36] The Computer Crime Act (Act No. 24 of 2007).
[37] The Right to Information Act (Act No. 12 of 2016).
[38] The Data Protection Bill, 2019.
[39] The Constitution of Nepal, 2015, Article 28.
[40] Only available in Nepali at: https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/106060/129899/%20F1095481449/NPL106060%20Npl.pdf.
[41] D. Pradhan and A. Kansakar, Nepal - Data Protection Overview | DataGuidance (16 March 2020) [Online]; Available at: https://www.dataguidance.com/notes/nepal-data-protection-overview.
[42] NKP 2064 D.N. 7880 [1208].
[43] NKP 2074 D.N. 9740.
[44] The Information, Communications and Media Act (of Bhutan), 2018.
[45] G. Greenleaf, Advances in South Asian Data Privacy Laws: Sri Lanka, Pakistan and Nepal, Privacy Laws and Business International Report, (2019) 22-25.
[46] G. Greenleaf, Privacy in South Asian (SAARC) States: Reasons for Optimism, UNSW Law Res. Ser., (2017) 1.

[47] V. Bentotahewa, C. Hewage, and J. Williams, The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries, SN Comput. Sci., 3 (2022) 1.
[48] The Constitution of the Islamic Republic of Afghanistan, 2004, Article 34.
[49] G. Greenleaf, Privacy in South Asian (SAARC) States: Reasons for Optimism, UNSW Law Res. Ser., (2017) 18–30
[50] V. Bentotahewa, C. Hewage, and J. Williams, The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries, SN Comput. Sci., 3 (2022) 1.
[51] V. Bentotahewa, C. Hewage, and J. Williams, The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries, SN Comput. Sci., 3(3) (2022) 1–18.
[52] The Access to the Information Law, 2018, S 16.
[53] The Penal Code, 1860, section 509.
[54] The Information and Communication Technology Act, 2006, section 63.
[55] The Digital Security Act, 2018, section 33.
[56] Y. Javed, K. M. Salehin, and M. Shehab, A Study of South Asian Websites on Privacy Compliance, IEEE Access, 8 (2020) 156067–156083.
[57] The Information, Communication and Media Act, 2017, section 464.
[58] G. Greenleaf, Promises and Illusions of Data Protection in Indian law, International Data Privacy Law, 1(1) (2011) 47.
[59] The Information Technology Rules, 2008, section 2.
[60] A. Burman, Will a GDPR-Style Data Protection Law Work for India?, Carnegie Endowment for International Peace, (2019) 1–7.
[61] The Right to Information Act, 2014, section 2(d).
[62] G. Greenleaf, Privacy in South Asian (SAARC) States: Reasons for Optimism, UNSW Law Res. Ser., (2017) 1.
[63] The Privacy Act, 2018, section 2(1).
[64] F. Daudpota, Fundamental Scope of the Right to Privacy in Pakistan - Need for a New Data Protection Law, SSRN Electronic Journal, (2016) 1-6.
[65] The Personal Data Protection Bill, 2018, section 2(g).
[66] R. L. W. Rajapakse, Personal Data Protection in the Context of Employment: A Discussion of Law in Sri Lanka in the Light of the GDPR, International Research Conference Article (KDU Library 2021) 109–115.
[67] Sri Lanka Becomes the First South Asian Country to Pass Comprehensive Privacy Legislation, (30 March 2022) [Online]; Available at: https://www.wilmerhale.com/en/insights/blogs/WilmerHale-Privacy-and-Cybersecurity-Law/20220330-sri-lanka-becomes-the-first-south-asian-country-to-pass-comprehensive-privacy-legislation.
[68] T. Abeysekara, Holistic Approach in Introducing Proper Legal Framework to Regulate Data Protection and Privacy in Sri Lanka, Vidyodaya Journal of Management, 8 (2022) 169.
[69] A. K. M. Bahalul Haque, Need For Critical Cyber Defence, Security Strategy and Privacy Policy in Bangladesh - Hype or Reality?, International Journal of Managing Information Technology, 11 (2019) 37.
[70] B. Kovačić, E. Tijan, and A. Skendžić, General Data Protection Regulation - Protection of Personal Data in an Organization, 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, May, 2018, 1370-1375.
[71] P. Raghunath, Human Security in a Ratifying South Asia: Approaching Data Protection, International Journal of Media Studies, 1(1) (2019), 56-68.
[72] M. O. Faruque and S. M. Habibullah, Privacy as a Human Right in the Digital Age: In Quest of a Safer Protection Regime in Bangladesh, ELCOP Yearbook of Human Rights 2018, 97-126.
[73] Association of Southeast Asian Nations (ASEAN) | DFAT [Online], Available at: https://www.dfat.gov.au/international-relations/regional-architecture/asean.
[74] M. T. Islam, M. Sahula, and M. E. Karim, Understanding GDPR: Its Legal Implications and Relevance to South Asian Privacy Regimes, UUM Journal of Legal Studies, 13(1) (2021) 45–76.
[75] A. Adib, Bridging the Gap between Right to Trade and Right to Privacy: An Application of the 'Principle of Inter-Operational Equity', Jahangirnagar University Journal of Law, 10 (2022) 71–73.
[76] Data Protection Regulations and International Data Flows: Implications for Trade and Development | UNCTAD [Online], Available at: https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.
[77] N. S. Dutta, New Era of Data Protection Regulation in South Asia | Ikigai Law (17 July 2019) [Online]; Available at: https://www.ikigailaw.com/new-era-of-data-protection-regulation-in-south-asia/