CRITICAL ANALYSIS OF RIGHT TO PRIVACY IN SAARC NATIONS

Nandu Sam Jose, Research Scholar, School of Legal Studies, Cochin University of Science and Technology)

ABSTRACT

This article presents a critical analysis of the right to privacy in SAARC nations, examining the legal frameworks, challenges, and the significance of regional cooperation in addressing privacy concerns in the digital age. The right to privacy is a fundamental aspect of human rights and is essential for a democratic society. However, SAARC nations face several challenges in ensuring effective privacy protection, including inadequate legal frameworks, weak enforcement mechanisms, limited resources and expertise, lack of public awareness, issues with cross-border data flows and harmonization, balancing privacy and national security, and addressing cybersecurity threats.

The article discusses the privacy protection landscape in each SAARC nation, highlighting the existing legislation and the challenges faced in safeguarding privacy rights. It further emphasizes the importance of regional cooperation among SAARC nations in strengthening digital privacy protection across the region. By sharing best practices, building capacity, collaborating on cybersecurity efforts, harmonizing data protection standards, and raising public awareness, SAARC countries can work together to address the complex privacy challenges of the digital age.

In conclusion, to effectively safeguard privacy rights, it is crucial for SAARC nations to prioritize privacy protection in their national agendas, invest in capacity building, and collaborate on developing comprehensive data protection legislation. Through regional cooperation, SAARC countries can ensure adequate privacy protection, fostering trust, promoting economic integration, and contributing to the overall development and progress of the region.

Introduction:

In the digital age, the right to privacy has emerged as a crucial concern for individuals and governments alike. The South Asian Association for Regional Cooperation (SAARC) comprises eight countries—Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, and Sri Lanka—that share cultural, historical, and economic ties. These countries have acknowledged the significance of privacy rights in protecting their citizens from potential abuses and preserving democratic values. This article critically analyzes the right to privacy in SAARC nations, focusing on each country's privacy legislation and its effectiveness in safeguarding individual privacy rights. Furthermore, the article delves into the importance of digital privacy, the role of regional cooperation in addressing privacy issues, and the challenges faced by SAARC nations in establishing robust privacy frameworks.

Right to Privacy in SAARC Nations

Afghanistan

Privacy rights in Afghanistan are recognized in the country's constitution. Articles 24, 37 & 38 of Afghan Constitution ensures the protection of privacy rights, including the sanctity of one's residence, correspondence, and personal information.[1] However, the absence of comprehensive data protection legislation and limited enforcement mechanisms significantly hampers privacy protection in Afghanistan. The country is grappling with ongoing conflicts and political instability, which further exacerbates privacy concerns.[2]

Afghanistan's legal framework for privacy protection remains underdeveloped, with no specific data protection law in place. The country primarily relies on the constitutional provisions and general legal principles to address privacy issues. This lack of comprehensive legislation makes it challenging to tackle contemporary privacy concerns such as data breaches, surveillance, and cross-border data transfers.

In addition to the legislative shortcomings, Afghanistan faces numerous challenges in implementing and enforcing privacy protection measures. The ongoing conflicts and political instability in the country have made it difficult to prioritize privacy rights and allocate resources

[1] Constitution of Afghanistan (1964) and Constitution of Afghanistan (2004)
[2] Afghanistan's Security Challenges under the Taliban, (2022), https://www.crisisgroup.org/asia/south-asia/afghanistan/afghanistans-security-challenges-under-taliban (last visited Mar 22, 2023).

for the development and enforcement of data protection laws.[3] Moreover, limited public awareness about privacy rights and the potential risks associated with digital platforms hinders the effective protection of privacy in Afghanistan.[4]

In conclusion, while Afghanistan's constitution acknowledges the importance of privacy rights, the country faces significant challenges in protecting individual privacy. The absence of comprehensive data protection legislation and limited enforcement mechanisms, coupled with ongoing conflicts and political instability, have left Afghan citizens vulnerable to privacy violations. To improve privacy protection in Afghanistan, there is a need to prioritize the development and implementation of robust data protection laws and foster regional cooperation to share resources and expertise in addressing privacy challenges.

Bangladesh

Bangladesh's right to privacy is enshrined in Article 43 of its constitution, which guarantees the protection of citizens' privacy in their homes, correspondence, and personal communications.[5] Although this constitutional provision recognizes the importance of privacy rights, Bangladesh's legal framework for privacy protection remains inadequate in addressing contemporary privacy challenges.

The Information and Communication Technology (ICT) Act of 2006[6] and the Digital Security Act of 2018[7] govern digital privacy issues in Bangladesh. However, these laws have faced criticism for their vague provisions and potential misuse. The ICT Act, in particular, has been criticized for its broad and ambiguous language, which has led to concerns about violations of freedom of expression and privacy rights.[8] The Digital Security Act, while intended to strengthen cybersecurity and protect digital privacy, has also been criticized for its potential to curb free speech and undermine citizens' privacy rights.[9]

---

[3] *Id.*
[4] Javid Hamdard, Abdurauf Khamosh & Jonathan H. Chan, *A Survey for User's Awareness and Practices Regarding Smartphone Security and Privacy in Afghanistan*, *in* 2020 - 5TH INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY (INCIT) 66 (2020), https://ieeexplore.ieee.org/document/9310935/ (last visited Mar 26, 2023).
[5] The Constitution of the People's Republic of Bangladesh (1972)
[6] The Information and Communication Technology Act, BANGLADESH (2006)
[7] Digital Security Act, BANGLADESH (2018)
[8] Bangladesh: Freedom on the Net 2020 Country Report, FREEDOM HOUSE, https://freedomhouse.org/country/bangladesh/freedom-net/2020 (last visited Mar 26, 2023).
[9] *Id.*

Despite these existing laws, Bangladesh lacks a comprehensive data protection legislation that specifically addresses data privacy concerns. This legislative gap has left the country vulnerable to privacy violations and data breaches.

In addition to the legislative challenges, Bangladesh faces issues in the implementation and enforcement of privacy protection measures. Limited public awareness about privacy rights and the potential risks associated with digital platforms hinders the effective protection of privacy in Bangladesh. Moreover, the lack of an independent data protection authority and limited resources for privacy enforcement further exacerbate the problem.[10]

In conclusion, while Bangladesh's constitution guarantees the right to privacy, the country's legal framework for privacy protection remains inadequate. The existing ICT Act and Digital Security Act have faced criticism for their vague provisions and potential misuse, and there is a pressing need for comprehensive data protection legislation that ensures robust privacy protection while safeguarding against potential abuse. Additionally, Bangladesh must improve public awareness about privacy rights, establish an independent data protection authority, and allocate resources to strengthen privacy enforcement mechanisms.

Bhutan

Bhutan's constitution guarantees the right to privacy under Article 7(19), which states that every person shall have the right to privacy in their homes, correspondence, and other personal communications.[11] While this constitutional provision recognizes the importance of privacy rights, Bhutan's legal framework for privacy protection is still in its infancy.

The Information, Communications, and Media Act of 2018 (ICMA) is the primary legislation that governs digital privacy in Bhutan.[12] The ICMA seeks to protect digital privacy by regulating data collection, processing, and disclosure practices. The Act mandates that data controllers and processors must obtain consent from individuals before collecting, processing, or sharing their personal information.[13] Additionally, the ICMA establishes a regulatory

---

[10] Mansi Babbar et al., *Adoption of digital technologies amidst COVID-19 and privacy breach in India and Bangladesh*, POLICY DES. PRACT. 1 (2023), https://www.tandfonline.com/doi/full/10.1080/25741292.2022.2162255 (last visited Mar 26, 2023).
[11] Constitution of Bhutan (2008)
[12] The Information, Communications, and Media Act of Bhutan, BHUTAN (2018)
[13] *Id* at 286

authority—the Bhutan InfoComm and Media Authority (BICMA)—to oversee and enforce privacy protection measures.[14]

Despite these legislative efforts, privacy protection in Bhutan remains underdeveloped. One of the main challenges in implementing robust privacy protection is the lack of resources and expertise in the country. This limitation hampers the development of a comprehensive data protection framework, leaving the country vulnerable to privacy violations and data breaches.

Furthermore, public awareness about privacy rights and the potential risks associated with digital platforms is limited in Bhutan. This lack of awareness makes it difficult to ensure effective protection of individual privacy rights.[15]

In conclusion, while Bhutan's constitution guarantees the right to privacy, the country's privacy protection framework is still in its infancy. The Information, Communications, and Media Act of 2018 marks a significant step toward improving privacy protection, but a lack of resources and expertise has hampered the development of a comprehensive data protection framework. To strengthen privacy protection in Bhutan, the country must invest in capacity-building, raise public awareness about privacy rights, and foster regional cooperation to share resources and expertise in addressing privacy challenges.

India

The right to privacy in India is recognized as a fundamental right under Article 21 of the country's constitution, following the landmark Supreme Court judgment in the *Justice K.S. Puttaswamy vs Union of India* case.[16] This judgment acknowledged the importance of privacy rights and laid the foundation for privacy protection in India. However, the legal framework for privacy protection in the country remains a work in progress.

The Information Technology (IT) Act of 2000 and its subsequent amendments serve as the primary legislation governing digital privacy in India.[17] The IT Act contains provisions related to data privacy, such as penalizing unauthorized access to, and disclosure of, personal

[14] *Id* at Chapter 3
[15] GRAHAM GREENLEAF, *Privacy in South Asian (SAARC) States: Reasons for Optimism*, (2017), http://138.25.65.17/au/journals/UNSWLRS/2018/11.pdf (last visited Feb 3, 2023).
[16] K. S. Puttaswamy v Union of India, AIR 2017 SC 4161, 547 (2017).
[17] Information Technology Act, (2000).

data. However, the act is not a comprehensive data protection law, and its provisions are insufficient to address the complex privacy challenges of the digital age.

Despite the constitutional guarantee of privacy rights, privacy protection in India is hindered by inadequate legislation and a lack of enforcement. The absence of a comprehensive data protection law leaves citizens vulnerable to privacy violations, data breaches, and unauthorized surveillance. Furthermore, although various authorities are responsible for overseeing privacy laws, there is no independent data protection authority in India to provide unified oversight and enforcement of privacy laws.

Another challenge faced by India in ensuring effective privacy protection is the lack of public awareness about privacy rights and the potential risks associated with digital platforms.[18] This limited awareness hinders the effective protection of individual privacy rights in the country.

In conclusion, while India's constitution recognizes privacy rights as a fundamental right, the country's legal framework for privacy protection remains a work in progress. The Information Technology Act of 2000 and its subsequent amendments are insufficient to address the complex privacy challenges of the digital age. To strengthen privacy protection in India, the country must focus on enacting the proposed Personal Data Protection Bill, establishing an independent data protection authority, and raising public awareness about privacy rights and potential risks associated with digital platforms.

Maldives

Privacy rights in the Maldives are enshrined in Article 24 of the country's constitution, which guarantees the right to privacy for every individual, including the privacy of their homes, property, and personal communications.[19] Despite this constitutional guarantee, the Maldives lacks specific data protection legislation, and the current legal framework for privacy protection remains inadequate.

The Maldives does not have a comprehensive data protection law, but the 2019 Data Protection and Privacy Regulation provides a basic framework for data privacy.[20] This regulation, which is overseen by the Communication Authority of Maldives, establishes rules

[18] Babbar et al., *supra* note 10.
[19] Constitution of the Republic of the Maldives (2008)
[20] Data Protection and Privacy Regulation, MALDIVES (2019)

for the collection, processing, storage, and disclosure of personal information. It also mandates that data controllers and processors must obtain consent from individuals before collecting or processing their personal data.

Despite these efforts, the country's data protection infrastructure remains insufficient. The Data Protection and Privacy Regulation is limited in scope and lacks the robustness of comprehensive data protection legislation. Furthermore, the enforcement mechanisms for privacy protection in the Maldives are weak, with no independent data protection authority to oversee and enforce privacy laws.

Another challenge faced by the Maldives in ensuring effective privacy protection is the lack of public awareness about privacy rights and the potential risks associated with digital platforms. This limited awareness hinders the effective protection of individual privacy rights in the country.[21]

In conclusion, while privacy rights are enshrined in the Maldives' constitution, the country's current legal framework for privacy protection is inadequate. The 2019 Data Protection and Privacy Regulation provides a basic framework for data privacy, but comprehensive legislation and enforcement mechanisms are needed to effectively protect privacy rights. The Maldives must focus on developing comprehensive data protection legislation, establishing an independent data protection authority, and raising public awareness about privacy rights and potential risks associated with digital platforms to strengthen its privacy protection framework.

Nepal

Nepal's constitution guarantees privacy rights under Article 28, which states that every person shall have the right to privacy in their residence, property, personal communications, and personal information. While this constitutional guarantee acknowledges the importance of privacy rights, Nepal's legal framework for privacy protection remains inadequate in addressing contemporary privacy challenges.

The Electronic Transactions Act of 2008 (ETA) serves as the primary legislation governing digital privacy in Nepal.[22] It contains provisions related to data privacy, such as requiring consent for the collection and processing of personal information, and penalizing

---

[21] GREENLEAF, *supra* note 15.
[22] Electronic Transactions Act, NEPAL (2008)

unauthorized access to, and disclosure of, personal data. However, the ETA is not a comprehensive data protection law, and its provisions are insufficient to address the complex privacy challenges of the digital age.

In addition to the ETA, the Information Technology Bill has been proposed to address some of the gaps in Nepal's digital privacy framework.[23] The bill includes provisions on data protection, cybercrimes, and the establishment of a regulatory authority. However, it has faced criticism for its potential to infringe on freedom of expression and privacy rights due to vague and broadly defined provisions.

Despite the constitutional guarantee of privacy rights, privacy protection in Nepal is hindered by inadequate legislation and a lack of enforcement. The absence of a comprehensive data protection law leaves citizens vulnerable to privacy violations, data breaches, and unauthorized surveillance. Furthermore, there is no independent data protection authority in Nepal to oversee and enforce privacy laws, which exacerbates the problem.

Another challenge faced by Nepal in ensuring effective privacy protection is the lack of public awareness about privacy rights and the potential risks associated with digital platforms. This limited awareness hinders the effective protection of individual privacy rights in the country.[24]

In conclusion, while Nepal's constitution guarantees privacy rights, the country's legal framework for privacy protection remains inadequate. The Electronic Transactions Act of 2008 and the proposed Information Technology Bill are insufficient to address the complex privacy challenges of the digital age. To strengthen privacy protection in Nepal, the country must focus on developing comprehensive data protection legislation, establishing an independent data protection authority, and raising public awareness about privacy rights and potential risks associated with digital platforms.

Pakistan

Privacy rights in Pakistan are enshrined in Article 14 of the country's constitution, which guarantees the inviolability of the dignity of every citizen and the privacy of their homes.[25] While this constitutional guarantee acknowledges the importance of privacy rights,

---

[23] Information Technology Bill, NEPAL (2019)
[24] GREENLEAF, *supra* note 15.
[25] Constitution of Pakistan (1973)

Pakistan's legal framework for privacy protection remains inadequate in addressing contemporary privacy challenges.

The Prevention of Electronic Crimes Act (PECA) of 2016 is the primary legislation governing digital privacy in Pakistan.[26] PECA contains provisions related to data privacy, such as penalizing unauthorized access to, and disclosure of, personal data. However, the act is not a comprehensive data protection law, and its provisions are insufficient to address the complex privacy challenges of the digital age. Furthermore, PECA has faced criticism for its potential to infringe on freedom of expression and privacy rights due to its vague and broadly defined provisions.

In addition to PECA, the Personal Data Protection Bill (PDPB) has been proposed to address some of the gaps in Pakistan's digital privacy framework.[27] The bill aims to establish a comprehensive data protection regime, including provisions on data protection principles, data subject rights, data breach notifications, and the establishment of a data protection authority. However, the bill is still under review and has not yet been enacted into law.

Despite the constitutional guarantee of privacy rights, privacy protection in Pakistan is hindered by inadequate legislation and a lack of enforcement. The absence of a comprehensive data protection law leaves citizens vulnerable to privacy violations, data breaches, and unauthorized surveillance. Furthermore, there is no independent data protection authority in Pakistan to oversee and enforce privacy laws, which exacerbates the problem.[28]

Another challenge faced by Pakistan in ensuring effective privacy protection is the lack of public awareness about privacy rights and the potential risks associated with digital platforms. This limited awareness hinders the effective protection of individual privacy rights in the country.[29]

In conclusion, while Pakistan's constitution guarantees privacy rights, the country's legal framework for privacy protection remains inadequate. The Prevention of Electronic Crimes Act of 2016 and the proposed Personal Data Protection Bill are insufficient to address

---

[26] Prevention of Electronic Crimes Act, PAKISTAN (2016)
[27] Personal Data Protection Bill, PAKISTAN (2021)
[28] Vibhushinie Bentotahewa, Chaminda Hewage & Jason Williams, *The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries*, 3 SN COMPUT. SCI. 183 (2022), https://link.springer.com/10.1007/s42979-022-01079-z (last visited Mar 26, 2023).
[29] Khuram Mushtaque et al., *Critical Analysis for Data Privacy Protection in Context of Cyber Laws in Pakistan*, 4 J. BASIC APPL. SCI. RES. 1 (2014).

the complex privacy challenges of the digital age. To strengthen privacy protection in Pakistan, the country must focus on developing comprehensive data protection legislation, establishing an independent data protection authority, and raising public awareness about privacy rights and potential risks associated with digital platforms.

Sri Lanka

Privacy rights in Sri Lanka are recognized under Article 14 of the country's constitution, which guarantees the fundamental right to freedom from interference with one's correspondence and other means of communication.[30] Although this constitutional provision acknowledges the importance of privacy rights, Sri Lanka's legal framework for privacy protection remains inadequate in addressing contemporary privacy challenges.

The Computer Crimes Act of 2007[31] and the Right to Information Act of 2016[32] were the primary legislations governing digital privacy in Sri Lanka. The Computer Crimes Act contains provisions related to unauthorized access, use, and disclosure of data, while the Right to Information Act focuses on providing citizens with access to information held by public authorities. However, in 2022 Sri Lanka became the first SAARC nation to pass a comprehensive privacy legislation with the enactment of Personal Data Protection Act (PDPA) 2022.[33] PDPA establish a comprehensive data protection regime, including provisions on data protection principles, data subject rights, data breach notifications, and the establishment of a data protection authority.

However, the challenge faced by Sri Lanka in ensuring effective privacy protection is the lack of public awareness about privacy rights and the potential risks associated with digital platforms. This limited awareness hinders the effective protection of individual privacy rights in the country.[34] Thus, to strengthen privacy protection in Sri Lanka, the country must focus raising public awareness about privacy rights and potential risks associated with digital platforms.

---

[30] Constitution of Sri Lanka (1978)
[31] Computer Crimes Act, SRI LANKA (2007)
[32] Right to Information Act, SRI LANKA (2016)
[33] Sri Lanka Becomes the First South Asian Country To Pass Comprehensive Privacy Legislation, (2022), 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 (last visited Mar 26, 2023).
[34] S Chamara, *Do We Have the Right to Privacy?* CEYLON TODAY (Colombo) 26 January 2020 https://archive.ceylontoday.lk/print-more/50553 (last visited Dec 22, 2022)

Digital Privacy and the Significance of Regional Cooperation

The rapid advancement of technology and increased digital connectivity have made digital privacy a significant concern in the SAARC region. The cross-border flow of data and cyber threats necessitate regional cooperation among SAARC nations to establish harmonized privacy legislation and enforcement mechanisms. By sharing best practices, resources, and expertise, SAARC countries can collectively address digital privacy challenges and strengthen their data protection frameworks.

Sharing Best Practices: Regional cooperation enables SAARC countries to share best practices in privacy protection, such as legislative models, regulatory frameworks, and enforcement mechanisms. By learning from each other's experiences, countries can design and implement more effective and robust privacy protection measures.

Capacity Building: Many SAARC nations lack the resources and expertise to develop and implement comprehensive data protection frameworks. Regional cooperation can facilitate capacity building through training, technical assistance, and knowledge-sharing, helping countries strengthen their privacy protection infrastructure.

Collaborative Cybersecurity Efforts: As the digital landscape becomes increasingly complex, the potential for cyber threats and cross-border data breaches rises. Regional cooperation allows SAARC nations to collaborate on cybersecurity initiatives, share threat intelligence, and develop joint strategies to prevent and respond to cyber incidents that could compromise digital privacy.

Harmonization of Data Protection Standards: Regional cooperation can promote the harmonization of data protection standards across SAARC nations. Harmonized standards facilitate data transfers and promote economic integration while ensuring consistent privacy protection for individuals. A regional data protection framework can also help establish trust and credibility among member nations, fostering increased collaboration in other areas.

Public Awareness Campaigns: Public awareness about privacy rights and potential risks associated with digital platforms is crucial for effective privacy protection. Regional cooperation allows SAARC countries to pool resources and expertise to develop and implement public awareness campaigns, ensuring citizens are informed about their privacy rights and the steps they can take to protect their personal information.

Regional cooperation among SAARC nations plays a significant role in strengthening digital privacy protection across the region. By sharing best practices, building capacity, collaborating on cybersecurity efforts, harmonizing data protection standards, and raising public awareness, SAARC countries can work together to address the complex privacy challenges of the digital age and safeguard the privacy rights of their citizens.

Challenges to Privacy Protection in SAARC Nations

SAARC nations face numerous challenges in protecting privacy rights in the digital age. These challenges can hinder the effective implementation and enforcement of privacy protection measures, leaving citizens vulnerable to privacy violations and data breaches. Some of the key challenges faced by SAARC countries in privacy protection include:

Inadequate Legal Frameworks: Many SAARC nations lack comprehensive data protection laws that address the complex privacy challenges of the digital age. Existing laws, such as the Information Technology Act in India and the Electronic Transactions Act in Nepal, are often outdated or insufficient to effectively protect individual privacy rights.

Weak Enforcement Mechanisms: Even when privacy protection laws exist, enforcement mechanisms in many SAARC countries are weak or nonexistent. The absence of independent data protection authorities to oversee and enforce privacy laws exacerbates the problem, leaving privacy rights inadequately protected.

Limited Resources and Expertise: Developing and implementing robust privacy protection frameworks require significant resources and expertise. Many SAARC countries face resource constraints and lack the necessary expertise to establish comprehensive data protection regimes, hindering effective privacy protection.

Lack of Public Awareness: Public awareness about privacy rights and the potential risks associated with digital platforms is crucial for effective privacy protection. However, many SAARC nations struggle with limited public awareness about privacy rights, making it difficult to ensure that individuals are informed and empowered to protect their personal information.

Cross-border Data Flows and Harmonization: With increasing cross-border data flows in the region, the lack of harmonized data protection standards among SAARC countries poses a significant challenge. Divergent standards can impede economic integration, hinder data transfers, and lead to inconsistent privacy protection for individuals.

Balancing Privacy and National Security: SAARC nations face the challenge of balancing privacy protection with national security concerns. Some countries have implemented surveillance measures to address security threats, which can lead to privacy violations and undermine trust in government institutions.

Cybersecurity Threats: As the digital landscape becomes increasingly complex, cybersecurity threats pose a significant challenge to privacy protection in SAARC nations. Cyberattacks, data breaches, and other cyber threats can compromise individual privacy rights and personal information.

To address these challenges, SAARC nations must work together to develop comprehensive data protection legislation, establish independent data protection authorities, invest in capacity building, raise public awareness about privacy rights, harmonize data protection standards, and collaborate on cybersecurity initiatives. By addressing these challenges through regional cooperation, SAARC countries can strengthen privacy protection across the region and safeguard the privacy rights of their citizens.

Conclusion

In conclusion, the right to privacy is a fundamental aspect of human rights and an essential component of a democratic society. SAARC nations, while acknowledging the importance of privacy rights, face significant challenges in protecting individual privacy in the digital age. These challenges include inadequate legal frameworks, weak enforcement mechanisms, limited resources and expertise, lack of public awareness, issues with cross-border data flows and harmonization, balancing privacy and national security, and addressing cybersecurity threats.

Regional cooperation among SAARC nations plays a critical role in addressing these challenges and strengthening digital privacy protection across the region. By sharing best practices, building capacity, collaborating on cybersecurity efforts, harmonizing data protection standards, and raising public awareness, SAARC countries can work together to overcome these challenges and safeguard the privacy rights of their citizens.

To achieve this, it is crucial for SAARC nations to prioritize privacy protection in their national agendas, invest in capacity building, and collaborate on developing comprehensive data protection legislation. By working together, SAARC countries can ensure that privacy rights are adequately protected, fostering trust, promoting economic integration, and ultimately contributing to the overall development and progress of the region.