Independent University **Bangladesh (IUB)**

IUB Academic Repository

Department of Law Faculty Publication

2024-03-04

Impacts of data localization policies and lessons for Bangladesh

Md. Toriqul Islam

Oxford University Press

http://ar.iub.edu.bd/handle/11348/950

Downloaded from IUB Academic Repository

Impacts of data localization policies and lessons for Bangladesh

Md. Toriqul Islam* and Borhan Uddin Khan**

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University, Bangladesh user on 09 July 2024

Key Points

- This study examines data localization policies and their impacts, considering the significance of data security and privacy in countries like Bangladesh.
- It succinctly discusses the meaning of data localization policies, and historical development while tracing its evolution over time.
- This study also analyses the motivations behind data localization policies and narrows its scope to Bangladesh, revealing insights into the nation's approach to data protection. Moreover, this article critically assesses data localization policies in Bangladesh, evaluating their effectiveness and potential drawbacks.
- Finally, the study investigates the broader implications of data localization policies, including their economic impacts in Bangladesh, while proposing suitable alternatives to them.

Introduction

The emergence of digital technologies, especially the Internet, has led to a significant increase in digital data covering all aspects of human life. The expansion of digital data entails enormous benefits but raises serious concerns about data privacy, data security, and data protection. In response to these challenges, some governments attempt to implement data localization policies, which restrict data transfer to particular countries, regions, or territorial jurisdictions. The rationales behind the implementation of these policies are often rooted in the belief that they would ensure the preservation of national sovereignty, security, public interest, and data protection.[1]

This stance reflects concerns surrounding US-led surveillance programmes implemented globally. Growing anxieties about potential US government access to user data through major tech companies like Alphabet, Amazon, Apple, Meta, Microsoft, and Yahoo have led to scepticism among some foreign governments. This concern has eroded trust in the services provided by these companies, prompting some foreign leaders to re-evaluate their reliance on them. In 2013, a Guardian report demonstrated that the National Security Agency (NSA) of the USA and the Government Communications Headquarters (GCHQ) of the UK, along with their foreign allies, continuously monitored people's data under the guise of law enforcement.[2] In 2015, Amnesty International and Privacy International compiled a list of 10 surveillance programmes led by the USA and its allies, which constantly monitored people around the world and processed data about them.[3] Even though governments worldwide increasingly block cyberspace over concerns about privacy, data security, effective surveillance operations, and domestic law enforcement grounds, this approach does not effectively safeguard data privacy and security.

However, data localization policies in the legal regime of Bangladesh could have adverse consequences, negatively impacting local trade, businesses, productivity, and

* Md. Toriqul Islam, Department of Law, Independent University, Bangladesh (IUB), Dhaka, Bangladesh.

** Borhan Uddin Khan, Department of Law, University of Dhaka, Dhaka, Bangladesh.

This work is an authentic and original contribution. Ethical approval is not required as there is no funding authority involved, and there are no potential conflicts of interest with any individual or institution for this study.

1 N Cory and L Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally and What They Cost' (Information Technology and Innovation Foundation (ITIF)), 19 July 2021) <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/> accessed 9 July 2023.

2 Ewen MacAskill and others, 'GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications' *The Guardian* (London, 21 June 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 9 July 2023.

3 Amnesty International, '10 Spy Programmes with Silly Codenames used by GCHQ and NSA' (18 March 2015) <https://www.amnesty.org/en/latest/campaigns/2015/03/10-spy-programmes-with-silly-codenames-used-by-gchq-and-nsa/> accessed 10 July 2023.

© The Author(s) 2024. Published by Oxford University Press. All rights reserved.
For permissions, please email: journals.permissions@oup.com

the prices of products and services that are heavily reliant on digital data. Specifically, adopting data localization measures might weaken Bangladesh's capacity to leverage digital data and technologies for national growth and development. The recent economic analysis conducted by the Information Technology and Innovation Foundation (ITIF) reveals that the implementation of restrictive data policies in countries like Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam would result in a significant increase in import costs and a reduction in trade volumes, thereby undermining the overall economy. These policies pose a lose–lose situation particularly for Bangladesh, negatively impacting its economic interests.[4]

Given the current circumstances, there exists an urgent necessity to conduct a comprehensive and econometric study on the implications of data localization policies in Bangladesh to determine the appropriate course of action. This article seeks to make a significant contribution to the ongoing policy discourse surrounding data localization requirements and their potential consequences. It also aims to provide a comprehensive overview of data localization policies and their broader economic impacts, both in Bangladesh and in other relevant economies. The findings of this study will be highly valuable to policymakers, businesses, and academics in Bangladesh and beyond. Bangladesh and other countries with similar data privacy concerns can use the lessons learned from this analysis to develop their data protection frameworks.

This article is structured as follows: The section 'Data localization: Meaning, history, and rationale' explains data localization policies, including their meaning, history, and rationales. The section 'Data localization policy in Bangladesh' details data localization policies in Bangladesh, while the section 'Overall impacts and lessons learned' examines the overall impacts of data localization policies in Bangladesh. The section 'Alternatives to data localization' proposes alternatives to data localization policies, and finally, the section 'Conclusion' offers a precise conclusion.

Data localization: meaning, history, and rationale

Meaning of data localization

The term 'data localization' (also known as 'data residency', 'data nationalism', or 'data sovereignty') refers to the practice of retaining data within the geographical boundaries of a country or region where it was originally generated. Data localization laws require specific types of data to remain within a country's borders before being allowed to cross national transfers.[5] According to Regulation (EU) 2018/1807 of the European Union (EU), data localization refers to any requirements imposed by a Member State that restrict the processing of data within its territory or prohibit its processing in another Member State.[6]

Data localization is a complex issue that encompasses a wide range of topics, including Internet governance, international trade law, national security, legal regulations, and transparency. Considering this context, the Organisation for Economic Co-operation and Development (OECD) Digital Economy Paper defines data localization as a rule or regulation mandating data storage or processing within a specific jurisdiction, either exclusively or non-exclusively, following legal or administrative requirements.[7] Based on the foregoing discussion, we can conclude that data localization requirements are legal, regulatory, or policy measures which mandate the storage, processing, and access of data originating from a particular country or region solely within that geographical boundary. In essence, these policies restrict cross-border data transfers.

Data localization provisions vary considerably in scope and implementation across countries. Some nations have relatively limited data localization laws, while others adopt more comprehensive data localization policies. For instance, the 'Personally Controlled Electronic Health Records Act 2012' of Australia imposes restrictions on transferring health data outside the country, subject to specific conditions.[8] The Vietnamese data protection framework requires Internet service providers to maintain a copy of

4 N Cory, L Dascoli and I Clay, 'The Cost of Data Localization Policies in Bangladesh, Hong Kong, Indonesia, Pakistan, and Vietnam' (Information Technology and Innovation Foundation (ITIF), 12 December 2022) <https://itif.org/publications/2022/12/12/the-cost-of-data-localization-policies-in-bangladesh-hong-kong-indonesia-pakistan-and-vietnam/> accessed 10 July 2023.

5 M Newton and J Summers, 'Russian Data Localisation Laws: Enriching Security & the Economy' (2018) The Henry M. Jackson School of International Studies, University of Washington, 28 <https://jsis.washington.edu/news/russian-data-localisation-enriching-security-economy/> accessed 10 July 2023.

6 EUR-Lex, 'Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-personal Data in the European Union' (2018), art 3(5) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807>.

7 D Svantesson, (2020), 'Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines' (OECD Digital Economy Papers, No. 301, OECD Publishing, Paris) <http://dx.doi.org/10.1787/7fbaed62-en> accessed 10 July 2023.

8 *Personally Controlled Electronic Health Records Act 2012* (2012) No 63 (Cth) ss 77–78.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University, Bangladesh user on 09 July 2024

their data within the country to facilitate potential government scrutiny.[9] However, governments worldwide often adopt data localization policies with the purported aim of achieving various objectives, such as strengthening data security, protecting national interests, or fostering economic growth, but achieve a few only through these policies.

Historical development

Despite the common perception that data localization is a new phenomenon, governments have been using such measures for over four decades, predating the Internet era. Even in the mid-19th century, restrictions over cross-border data transfer were evident.[10] For example, in the late 1970s, Kerstin Amer, a Swedish Under Secretary, raised concerns about the protection of the personal data of Swedish residents due to inadequate data protection measures in other jurisdictions.[11] Therefore, Sweden enacted its first national data protection law in 1973, requiring authorization for cross-border data transfer. Similarly, during the 1970s, Canada and Brazil had concerns about cross-border data flows.[12] However, data localization policies became widespread in the 1990s when governments worldwide faced logistic, privacy, and security challenges due to the rapid growth and diversification of digital data.[13]

While not imposing strict data localization requirements, Article 25 of the EU's 1995 Data Protection Directive (Directive 95/46/EC) pioneered personal data control for EU citizens by regulating the transfer of personal data to third countries based on their data protection levels.[14] Article 44 of the General Data Protection Regulation (GDPR) further emphasizes data protection by prioritizing safeguards for data transfers outside the EU, rather than solely relying on data localization.[15] Similarly, Article 10 of the Data Protection Law Enforcement Directive maintains flexibility regarding data storage locations for law enforcement purposes, acknowledging the complex interplay between privacy and crime prevention.[16] Article 25 of the Regulation on Europol aligns with this approach, allowing data transfers to third countries only when adequate safeguards are in place, even in the context of law enforcement cooperation.[17] Thus, EU law prioritizes data protection and the free flow of non-personal data within the EU, while recognizing the need for flexibility in specific circumstances like law enforcement, national security, and public health crises. This approach balances data protection, economic interests, and security concerns.

Although there were speculations in the past that only authoritarian regimes utilize data localization requirements to force companies to store data within their borders, these policies are now widespread in both democratic regions, such as Europe, and less democratic regions, including China, Russia, Vietnam, Turkey, and Iran.[18] Data localization measures are on the rise, and more than 75 per cent of countries with data privacy laws currently implement some form of data localization.[19] As of July 2021, approximately 162 countries worldwide have data privacy legislation. Of these, over half (62) have implemented 144 data localization

9 Internet Society, 'Internet Impact Assessment Toolkit: Use Case: Data Localization' (2020) <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/> accessed 2 January 2024.

10 WJ Drake, 'Background Paper for the Workshop on Data Localisation and Barriers to Transborder Data Flows' (14–15 September 2016) The World Economic Forum, Geneva <https://www3.weforum.org/docs/Background_Paper_Forum_workshop%2009.2016.pdf> accessed 15 February 2024.

11 Christopher Kuner and others, 'Internet Balkanization Gathers Pace: Is Privacy the Real Driver?' (2015) 5 (1) International Data Privacy Law 1–2.

12 Ibid.

13 J Hill, 'The Growth of Data Localisation Post-Snowden: Analysis and Recommendations for US Policymakers and Business Leaders' (Conference on the Future of Cyber Governance, The Hague Institute for Global Justice, 2014).

14 *EU Directive 95/46*: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

15 *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

16 *EU Directive (EU) 2016/680*: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

17 *EU Regulation (EU) 2016/794:* Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA, and 2009/968/JHA [2016] OJ L 135/53.

18 A comprehensive list of countries having explicit, de facto, and proposed data localization policies around the world has been shared in a recent study conducted by Nigel Cory, Luke Dascoli and Ian Clay. For details see Cory and Dascoli (n 1) 27–57.

19 It is worth noting also that as per UNCTAD's estimation, 137 of 194 countries in the world have some form of data privacy legislation, representing 71% of all nations. Around 9% of countries have initiated processing the draft legislation, 15% have no legislation, and 5% have no data about this matter. See UNCTAD, 'Data Protection and Privacy Legislation Worldwide' (2023) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide#:~:text=137%20out%20of%20194%20countries,in%20only%2048%20per%20cent> accessed 10 July 2023.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University Bangladesh user on 09 July 2024

restrictions. This represents more than a doubling since 2017 when only 35 countries had 67 such policies in place.[20]

The rationale behind data localization

There are numerous motivations behind the adoption of data localization policies. In the EU context, the Member States adopted data localization policies for several reasons, such as restrictions on trans-border data flow imposed by the GDPR,[21] invalidation of the EU–US Privacy Shield Agreement,[22] and renewed emphasis on European digital sovereignty.[23] However, countries worldwide adopt data localization policies for a variety of reasons.

These reasons include:

- National security and sovereignty
- Privacy and data protection
- Economic growth and innovation
- Legal compliance and political control
- Cultural preservation and environmental protectionism.

National security and sovereignty

Some countries like Russia, China, Indonesia, Mexico, South Africa, and India have adopted data localization policies primarily for national security and sovereignty reasons, fuelled by concerns about data breaches allegedly involving US tech companies and intelligence agencies.[24] However, their allegations are not beyond logic. The Snowden disclosures revealed that major US technology companies, including AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype, Yahoo, and YouTube, had granted the NSA access to user data through various programmes, including PRISM, officially known as US-984XN.[25] This collaboration between the NSA and the Federal Bureau of Investigation (FBI) obliged Internet companies to provide data in response to warrants issued by an intelligence court. Additionally, the programmes MUSCULAR and Temporal Reasoning Universal Elaboration (TEMPORA), allowed the NSA to access data transmitted through communication links of US-owned firms located and operated outside the USA.[26] Following the disclosure of the PRISM programme, government officials from Germany, France, and Brazil encouraged citizens against using US servers like Google and Facebook, advocating for establishing data centres within their respective territories to enhance data security.[27] Moreover, policymakers, academics, civil society, and business leaders in many developing countries support 'digital colonialism' through data localization policies, citing national security concerns. Tech giants, driven by 'surveillance capitalism', oppose these policies, arguing they hinder their global operations.[28] The debate has proponents and critics, emphasizing the importance of a neutral standpoint to balance conflicting interests.

Privacy and data protection

Governments globally try to grapple with data-related challenges, with a growing focus on cross-border data

20 Ibid.

21 See GDPR (n 15), chapter V (Transfer of personal data to third countries or international organizations (art 44), adequacy decisions (art 45), appropriate safeguards (art 46), binding corporate rules (art 47), derogations for specific situations (art 49), international cooperation for the protection of personal data).

22 CJEU, C-311/18 *Facebook Ireland Ltd v Maximillian Schrems*, [2020].

23 F Burwell and K Propp, 'The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?' (2020) Issue Brief <https://www.atlantic council.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/> accessed 8 July 2023; C Hobbs, (ed), 'Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry' (European Council on Foreign Relations, Essay Collection 2020) ECFR/336.

24 For details see generally A Chander and UP Lê, 'Data Nationalism' (2015) 64 Emory Law Journal 677–80; I Byhovsky and D Garrie, 'Privacy and Data Protection in Russia' (2017) 5(2) Journal of Law & Cyber Warfare 235; S Sacks, Q Chen and G Webster, 'Five Important Takeaways From China's Draft Data Security Law' (*New America*, 2020) <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-important-take-aways-chinas-draft-data-security-law/> accessed 15 February 2024; Treutler TJ and Tran GTH, 'Update on the Implementation of Vietnam's New Cybersecurity Law and Status of Implementing Decrees' (Lexology, 2023) <https://www.lexology.com/library/detail.aspx?g=8833627c-e189-4d60-a472-6ee742cc38fd>; Cory and Dascoli (n 1) 10.

25 For details about the PRISM surveillance programme, refer to Glenn Greenwald and Ewen MacAskill, 'NSA Prism Program Taps into User Data of Apple, Google, and others' *The Guardian* (London, 7 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 27 December 2023.

26 MacAskill and others (n 2).

27 AP (Associated Press), 'German Minister: Drop Google if you Fear US Spying' (*Yahoo!news*, 3 July 2013) <news.yahoo.com/german-minister-drop-google-fear-105418688.html?guccounter=1> accessed 15 February 2024; V Marchive, 'France Hopes to Turn PRISM Worries into Cloud Opportunities' (*ZDNET*, 21 June 2013) <https://www.zdnet.com/google-amp/article/france-hopes-to-turn-prism-worries-into-cloud-opportunities/> accessed 15 February 2024; United States Senate Committee on Finance, 'Wyden Remarks on Ending Mass Surveillance to Boost Digital Economy' (8 October 2014) <finance.senate.gov/chairmans-news/wyden-remarks-on-ending-mass-surveillance-to-boost-digital-economy> accessed 10 July 2023.

28 The term 'surveillance capitalism' was coined by Shoshana Zuboff, a renowned scholar and professor at Harvard Business School. In her book *'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power'*, published in 2018, Zuboff extensively explores and analyses the concept of surveillance capitalism and its implications for individuals, society, and the economy. Her work has been influential in shaping the discourse and understanding of the economic and social consequences of the data-driven surveillance practices employed by tech companies. For details see generally S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York, Public Affairs, 2019).

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University, Bangladesh user on 09 July 2024

flows. To address these issues, some governments advocate for data localization policies. These policies are often presented as safeguards for privacy and sovereignty, aiming to protect sensitive data within national borders. However, this argument has inherent flaws, as data security depends on the strength of technical, physical, and administrative controls rather than the data's physical location.[29] Storing all data in one geographic location may jeopardize data security by exposing it to physical threats and targeted cyberattacks.[30] Moreover, implementing data localization measures could undermine collaborative solutions provided by public cloud service providers and cybersecurity firms required for addressing cybersecurity challenges. Although some governments may justify data localization policies by claiming that they would protect privacy, they may be motivated by other goals, such as increasing surveillance or gaining economic advantages. A recent Centre for Strategic and International Studies (CSIS) report argues that these measures have numerous adverse effects on many interests, including human rights, privacy, and economic well-being.[31]

Economic growth and innovation

While some governments like China, India, and Indonesia believe that data localization policies can stimulate economic growth by promoting local data centres and services, the real impact is negative.[32] For instance, data localization policies reduce Internet accessibility and security and increase both cost and complexity. Moreover, these policies harm data-intensive services, economic productivity, and innovation.[33] They benefit a few local businesses while harming the overall economy, potentially reducing gross domestic product (GDP).[34] These policies raise costs, limit access to services, hinder startup growth, and obstruct new technology adoption. In contrast, research shows that unrestricted data flows promote trade openness, enabling businesses to expand into multiple markets, with a 10 per cent increase in bilateral digital connectivity linked to over 5 per cent growth in service trade.[35]

Legal compliance and political control

To ensure legal compliance and uphold local laws, some governments may advocate for data localization policies. This position finds support in a European Union report, which reveals that electronic evidence plays a crucial role in criminal investigations. Nearly 85 per cent of such investigations rely on electronic evidence, with over half requiring cross-border access to such data.[36] However, law enforcement-driven data localization policies can serve as tools of political oppression, enabling governments to control information flow, identify and intimidate individuals, and suppress democratic values like privacy, data protection, and freedom of expression. For example, countries like China and Russia prioritize physical access to critical data centres for surveillance and political control ends.[37]

Cultural preservation and environmental protectionism

Some governments may implement data localization policies to protect cultural values and practices by regulating how cultural information is accessed and used. For example, under 'Decree—Protection of Personal Data 2023', the Vietnamese authority aims to protect the data relating to the environment, culture, sports, tourism, and other areas.[38] While proponents of data localization policies argued that localization can preserve culture, environment, or energy efficiency, our analysis reveals these policies primarily serve national security interests by granting governments greater control over digital data, at the expense of trade, productivity, and industry competitiveness.

29 Cory, Dascoli and Clay (n 4) 12.

30 Cory and Dascoli (n 1) 5.

31 CSIS, 'The Real National Security Concerns over Data Localisation' (Centre for Strategic and International Studies, 2021) <https://www.csis.org/analysis/real-national-security-concerns-over-data-localisation> accessed 26 December 2023.

32 James Kaplan, 'Data Localisation and New Competitive Opportunities' (McKinsey & Company, 30 June 2022) <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localisation-of-data-privacy-regulations-creates-competitive-opportunities> accessed 29 December 2023.

33 A Goldfarb and D Trefler, 'AI and International Trade' (National Bureau of Economic Research, Working Paper No 24254 2018) <https://www.nber.org/papers/w24254> accessed 27 December 2023; J Triplett and B Bosworth, 'Productivity Measurement Issues in Services Industries: Baumol's Disease Has Been Cured' (2003) 9(3) Economic Policy Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=789545> accessed 27 December 2023.

34 Matthias Bauer and others, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery', (2014) ECIPE Occasional Paper No 3, European Centre for International Political Economy <https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf> accessed 25 February 2024.

35 J López González and J Ferencz, 'Digital Trade and Market Openness' (2018) *OECD Trade Policy Papers*, No 217 (OECD Publishing, Paris) <https://doi.org/10.1787/1bd89c9a-en> accessed 15 February 2024.

36 EU Commission, 'Commission Staff Working Document: Executive summary of the impact assessment accompanying the document Proposal for A Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online' (2018) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0118:FIN:EN:PDF> accessed 15 February 2024.

37 Cory and Dascoli (n 1) 7.

38 Vietnam Government, 'Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân' [Decree No 13/2023/NĐ-CP on personal data protection] <https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx> accessed 17 July 2023.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University, Bangladesh user on 09 July 2024

Data localization policy in Bangladesh

Countries can be categorized based on their data localization policies: those without any restrictions, those with limited requirements for specific sectors, and those with comprehensive regulations governing data types and transfers. Iceland, Ireland, Hong Kong, and the Netherlands fall into the first category; Thailand and Australia have adopted less restrictive data localization policies, while China, Russia, and Turkey have implemented highly restrictive data localization policies. The implementation of strict data localization policies can have several implications. These policies have the potential to impede international data flows, hinder collaboration, and stifle innovation. Additionally, they may increase operational costs for multinational businesses. This impact on costs could potentially affect the competitiveness of businesses operating in countries with strict data localization policies. Instances of such effects can be observed in countries like China, Indonesia, Russia, and South Africa.[39]

Earlier, Bangladesh was identified as a country with the most stringent data localization measures, followed by Vietnam, Indonesia, Hong Kong, and Pakistan.[40] Bangladesh is now a country with the second category of data localization policies due to subsequent changes in the latest draft of the Personal Data Protection Act, 2023 (PDPA), the primary legal instrument aiming to enforce data localization policies in Bangladesh. The previous draft of the Data Protection Act, 2022 (DPA) required that sensitive, user-generated, or classified data be stored in Bangladesh (section 42). Additionally, the government could periodically publish the list of open data, which could then be transferred outside of Bangladesh for any use without approval from the government (section 43). Finally, sensitive, and user-generated data could be transferred to any other country, business outside Bangladesh, or international organization with the consent of the data subject (section 43).[41]

However, the latest draft of the Personal Data Protection Act, 2023 (PDPA) requires that only the classified data, as defined by the government by rule subsequently, be stored in Bangladesh (section 50, PDPA 2023 (draft)).[42] While the PDPA mandates the localization of classified data, it fails to define this critical term itself but rather empowers the government to prescribe a definition through rules. This delegation of definitional authority to non-legislative actors is inherently problematic due to the lack of transparency and potential for abuse.[43] An overly broad definition of 'classified data', for example, could lead to excessive data localization, restrictions on cross-border transfer, and even infringements on individual privacy rights through hidden surveillance. Moreover, implementing data localization policies necessitates establishing and maintaining national critical data server infrastructures, but this may pose significant challenges for Bangladesh due to its limited resources and technical expertise.

Additionally, strict data localization policies can exacerbate citizens' vulnerability to privacy violations by increasing data concentration within the country and impede their freedom of expression by restricting access to certain services and technologies.[44] Furthermore, data localization policies can lead to increased business costs, innovation barriers, and fragmentation of the data ecosystem, potentially harming the overall economy and hindering the development of local technology companies, a key aspect of Bangladesh's 'Smart Bangladesh' vision.[45] Notably, mandatory data localization requirements could significantly impede the

39 McKinsey and Company, 'Data Localisation and New Competitive Opportunities' (*McKinsey*, 30 June 2022) <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localisation-of-data-privacy-regulations-creates-competitive-opportunities> accessed 27 December 2023; InCountry, 'Data Residency Laws by Country: Overview' (2020) <https://incountry.com/blog/data-residency-laws-by-country-overview/> accessed 27 December 2023.

40 Cory, Dascoli and Clay (n 4) 5.

41 ICT Division, Government People's Republic of Bangladesh, Data Protection Act, 2022 (Draft) <https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/Data%20Protection%20Bill%20en%20V13%20Unofficial%20Working%20Draft%2016.07.22.pdf> accessed 27 December 2023.

42 ICT Division, Government People's Republic of Bangladesh, Personal Data Protection Act, 2023 (Draft) (Bengali version) <https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/%E0%A6%89%E0%A6%AA%E0%A6%BE%E0%A6%A4%E0%A7%8D%E0%A6%A4%20%E0%A6%B8%E0%A7%81%E0%A6%B0%E0%A6%95%E0%A7%8D%E0%A6%B7%E0%A6%BE%20%E0%A6%86%E0%A6%87%E0%A6%A8%2C%20%E0%A7%A8%E0%A7%A6%E0%A7%A8%E0%A7%A9%20%E0%A7%A7%E0%A7%A7.%E0%A7%A7%E0%A7%A6.%E0%A7%A8%E0%A7%A9.pdf> accessed 26 December 2023.

43 'Submission-on-the-Bangladesh-Data-Protection-Act-2023' (*Access Now*, 26 October 2023) <https://www.accessnow.org/wp-content/uploads/2023/10/Submission-on-the-Bangladesh-Data-Protection-Act-2023-Access-Now-and-Tech-Global-Institute.pdf> accessed 26 December 2023.

44 Transparency International Bangladesh (TIB), 'Draft Data Protection Act (PDPA) 2023 - Review and Recommendations' <https://www.ti-bangladesh.org/upload/files/position-paper/2023/Position-Paper-on-Revised-Draft-Data-Protection-Act-Review-Recommendations.pdf> accessed 15 February 2024.

45 Driven by the ambition to transform Bangladesh into a technologically empowered and sustainable nation by 2041, the Smart Bangladesh initiative builds upon the Digital Bangladesh foundation. It envisions a future woven with smart cities, agriculture, healthcare, education, energy, governance, and institutions, all aimed at creating a prosperous, equitable, and sustainable future for Bangladeshis. Four interconnected pillars—connectivity, e-governance, innovation, and human resource development—underpin this smart ecosystem, echoing the aspirations of Bangabandhu Sheikh Mujibur Rahman, the Father of the Nation of Bangladesh. For details, see a2i, 'Smart Bangladesh Vision 2041' (2020) <https://a2i.gov.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University, Bangladesh user on 09 July 2024

growth of local tech companies, directly contradicting the vision's goals.

Therefore, the PDPA 2023 takes a nuanced approach to data localization. While classified data remains subject to localization, data flows are generally relaxed for trade, international relations, and other government-approved purposes. Nevertheless, concerns remain due to ambiguities like undefined safeguard procedures and the potential for conflicting regulations by sectoral authorities. This flexibility, coupled with an expanded definition of sensitive data, opens the door for potential government interference in economic matters like capital control and taxation.[46] Overall, the approach of data localization policies in PDPA appears balanced but lacks crucial details, leaving its true impact uncertain.

The proposed data localization requirements within the PDPA may also have adverse effects on Bangladesh's software and tech startup ecosystem, potentially limiting its ability to attract investments and compete on a global scale. Furthermore, these restrictions on data transfers could hinder cross-border transactions, restricting access to knowledge, digital tools, and commercial opportunities for Bangladeshi businesses. These requirements might impede digital innovation and inclusive development through international cooperation. Above all, these policies may also hinder Bangladesh's participation in regional trade initiatives, such as the Indo-Pacific Economic Framework, due to conflicts with international agreements.[47]

Apart from the PDPA 2023, Bangladesh has several laws and regulations requiring data to be stored within the country. For example, the 'Guidelines on Cloud Computing, 2023 (Version 1.0)' incorporates data localization provisions, requiring the storage of sensitive data within Bangladesh. The same regulations also apply to cross-border hybrid clouds with the same conditions (Cloud Computing Guidelines, 2023, secs 2.3.1.2 and 2.3.4.5, respectively).[48] The Bangladesh Bank also requires banks to obtain prior approval before transferring business-related documents outside the country (section 12 of the Bank Company Act, 1991). Additionally, mobile operators must establish local data centres to store data in Bangladesh for national security purposes (Bangladesh Telecommunication Act, 2001 (amended in 2006), sections 35 and 97 (Ka)).[49]

In essence, data localization mandates confine citizen data within national borders, granting governments control over both the data and the companies processing it. Forcing platforms like Google and social media giants to store data locally allows governments unprecedented access, thereby facilitating the curtailment of free speech, privacy, and other fundamental liberties. This insidious trend breeds digital censorship states, chilling public discourse and empowering regimes like those in China, Russia, Bangladesh, and beyond.[50] At its core, the issue of data localization revolves around a dichotomy between two contrasting visions: one that embraces the extensive opportunities of the global digital economy through cooperation and interoperable laws and the other that assumes a costly, misguided, and nationalistic approach to control and protectionism.[51] Instead of pursuing the latter stance, policymakers of Bangladesh should aim for a data governance framework that effectively addresses legitimate public policy concerns, such as privacy, cybersecurity, and government access to data, in a prudent and balanced manner. It is also crucial to avoid the misleading appeal of data nationalism.

Overall impacts and lessons learned

While data localization policies, aiming to retain data within national borders, have garnered significant appeal among policymakers globally, their effects on emerging economies like Bangladesh present a nuanced narrative. Despite impressive economic growth in the past two decades, Bangladesh still faces substantial economic challenges. According to the World Bank, the economy faces considerable challenges with rising inflationary pressure, energy shortages, a balance-of-

bd/a2i-missions/smart-bangladesh-vision-2041/> accessed 26 December 2023.

46 Christabel Randolph, 'Bangladesh Draft Data Protection Act 2023: Potential and Pitfalls' (*Atlantic Council—South Asia Center*, May 2023) <https://www.atlanticcouncil.org/wp-content/uploads/2023/05/Bangladesh-Draft-Data-Protection-Act-2023-Potential-and-Pitfalls.pdf> accessed 26 December 2023.

47 Global Data Alliance, 'Global Data Alliance Best Practices on Global Data Protection Assessments (GDPA)' (7 September 2022) <https://globaldataalliance.org/wp-content/uploads/2022/09/09072022gdabgdpa.pdf> accessed 15 February 2024.

48 BB (Bangladesh Bank), 'BRPD Circular No. 05: Guideline on Outsourcing of IT Operations of Banks' (Vol 2) (2023) <https://www.bb.org.bd/mediaroom/circulars/brpd/mar162023brpd05.pdf> accessed 15 February 2024.

49 ITU (International Telecommunication Union), 'Bangladesh Telecommunication Act 2001' (n.d.) <https://www.itu.int/ITU-D/treg/Documentation/Bangladesh/BTRC-TelecomLaw2001.pdf> accessed 15 February 2024; Telenor, Authority Request Legal Overview: Bangladesh (2017) <https://www.telenor.com/binaries/sustainability/responsible-business/handling-access-requests-from-authorities/Authority-Request-Legal-Overview_March-2017-bangladesh.pdf> accessed 15 February 2024.

50 CSIS (n 31).

51 Cory, Dascoli and Clay (n 4) 4.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University Bangladesh user on 09 July 2024

payments deficit, and a revenue shortfall.[52] Experts further highlight the persistent high inflation, rising foreign exchange rate, and deepening liquidity crunch in the banking sector as major concerns for Bangladesh's economic stability.[53] In this context, this section delves specifically into the economic implications of data localization policies for Bangladesh, exploring both potential benefits and unforeseen consequences. Our analysis aims to inform policymakers as they navigate the intricate landscape of data governance, balancing national interests with the need for continued economic growth and prosperity.

While proponents of data localization may highlight potential benefits like job creation in data centres or tighter data control, scholars and liberal economists argue that these policies pose significant negative economic consequences, including decreased trade, reduced innovation, and increased compliance costs for businesses. ITIF's econometric modelling, for example, estimates a 7 per cent decrease in traded output, a 1.5 per cent rise in industry prices, and a 2.9 per cent drop in productivity due to increased data restrictions.[54] A 2016 study on the long-term financial impacts of data localization in seven selected countries, conducted by the European Centre for International Political Economy (ECIPE), also revealed that the data localization requirements had significant implications for the GDP of all the countries examined.[55] Another study of the same year further concluded that consumers worldwide would ultimately pay for data localization as companies, facing increased compliance costs and operational burdens, pass these expenses on through higher prices, reduced services, or limited choices.[56]

A 2014 study further estimated welfare losses of $63 billion in China and a staggering $193 billion in the European Union, highlighting the significant economic burden imposed by data localization policies.[57] Further, a GSMA-run study in 2021 focusing on three developing regions, including South America, South-East Asia, and Africa, showed a substantial decline in productivity and revenue gains, estimated to be between 59 per cent and 68 per cent because of data localization. The study also demonstrated that data localization policy could lead to investment losses ranging from $4 to $5 billion and job losses ranging from 182,000 to 372,000 jobs annually.[58]

The World Bank's World Development Report 2020 reveals that countries could enhance their productivity by an average of 4.5 per cent by removing restrictive data policies and reducing limitations on data trade services, leading to overall 5 per cent benefits.[59] A 2018 OECD report further revealed that digitalization has a link to greater trade openness and a 10 per cent increase in bilateral digital connectivity results in over a 3.1 per cent increase in trade in services.[60] Furthermore, stringent data localization requirements can severely impact the productivity of local companies engaged in digital technologies and services.

Some countries may justify centralized data storage policies with the promises of enhanced data security, privacy, and government control. However, this approach can backfire, as these central repositories become attractive targets for malicious actors like state-sponsored hackers. While proponents argue that such policies promote local digitization and technological independence, critics point out that strict requirements can stifle innovation and hamper digital growth by hindering international data flow, particularly for emerging technologies like cloud services, e-commerce, and the Internet of Things (IoT).[61] In essence, the data localization policies obstruct cross-border data flow, limit innovation, and inflate business costs, sparking a global debate about their effectiveness and potential drawbacks, especially in the context of Bangladesh. The potential adverse consequences of data localization policies, particularly for Bangladesh, can therefore be summarized as follows.

Business costs, efficiency, and performance

Data localization policies could increase business costs, reduce business efficiency, and affect overall business

52 World Bank, 'Bangladesh: Overview' (last updated 9 December 2023) <https://www.worldbank.org/en/country/bangladesh/overview> accessed 29 December 2023.

53 The Daily Star Editorial, 'Major Economic Challenges Lie Ahead for Bangladesh' <https://www.thedailystar.net/views/editorial/news/major-economic-challenges-lie-ahead-bangladesh-2917736> accessed 29 December 2023.

54 Cory and Dascoli (n 1)

55 European Centre for International Political Economy (ECIPE), 'Trade in Data: The Next Frontier in International Trade and Internet Governance' (2014) <https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf?_gl=1*wkpql0*_up*MQ.*_ga*MjAxOTc4Nzg0MC4xNjg5Njk3MDAz*_ga_T9CCK5HNCL*MTY4OTY5NzAwMi4xLjAuMTY4OTY5NzAwMi4wLjAuMA.> accessed 15 February 2024.

56 University of Kentucky, P Rothstein and E King, 'How Will the Use of Big Data Affect Privacy Law?' (2015) 57(1) Boston College Law Review, 282–318 <https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1593&context=law_facpub> accessed 15 February 2024.

57 Bauer and others (n 34).

58 Hosuk Lee-Makiyama and Simon Lacey, 'Cross-Border Data Flows: The Impact of Data Localisation on IoT' (2021), GSMA <https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf> accessed 15 February 2024.

59 López González. and Ferencz (n 35).

60 Ibid.

61 RD Taylor, '"Data localisation": The Internet in the Balance' (2020) 44(8) Telecommunications Policy 1–15.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University, Bangladesh user on 09 July 2024

performance in Bangladesh. Apart from increased business costs, data localization policies render the transfer of data across borders unattractive or impractical.[62] If companies like Google, Facebook, WhatsApp, Amazon, and YouTube, are required to store their data locally, they may need to invest in additional infrastructure and resources to comply with the regulations. This could increase the cost of doing business in the country, which may discourage foreign companies from investing in Bangladesh. Peter Haas, the US Ambassador to Bangladesh, for example, warned that 'if the DPA is passed with strict data localization requirements, it may compel certain US companies currently operating in Bangladesh to exit the market'.[63] In reality, if US-based companies like Facebook become unavailable, it would result in the closure of over 2000 start-ups in Bangladesh that rely on the platform for their business operations.[64]

Additionally, data localization requirements impose substantial financial burdens on businesses. A recent ITIF study on the economic effects of such policies in Bangladesh, Hong Kong, Indonesia, and Pakistan indicates that all five economies could witness increased import prices, leading to higher business costs and reduced trade.[65] Establishing local data centres or securing local partners for data storage poses substantial financial challenges, with compliance costs ranging from thousands to millions of dollars, placing particularly burdensome strains on SMEs compared to larger corporations.

Moreover, data localization requirements can reduce business efficiency by slowing down data transfer speeds and increasing delays. These policies often require businesses to store and process data within a specific geographic location, which can result in slower data transfer speeds and increased latency. Hence, data localization requirements can negatively impact business operations and decrease efficiency. Slower data transfer speeds could cause delays in decision-making, reduce productivity, and result in increased costs due to missed opportunities.[66]

Data localization rules not only require foreign organizations and businesses to store data in Bangladesh but also seek permission from the government of Bangladesh for cross-border data transfers. This could cause problems for these organizations and businesses, and eventually, affect the overall performance of diverse businesses in Bangladesh. Indeed, data localization is not a complete solution for protecting personal data or data security, even though some policymakers think so. In most cases, data localization mandates neither enhance commercial privacy nor data security.[67]

Challenges in Bangladesh's digital services

Implementing data localization policies can prevent foreign companies from offering services in Bangladesh, harming the country's digital economy. These policies can restrict access to digital services and technologies, potentially deterring foreign companies from operating in Bangladesh due to the costly infrastructure required for local data storage. Specifically, data localization requirements in the proposed PDPA could force American companies to leave Bangladesh.[68] Data localization requirements can also limit the use of cloud computing, which relies on data being stored and processed in multiple locations. This can lead to a fragmented data ecosystem, reduced data quality, and increased costs for cloud service providers.[69] Recent research by Research and Policy Integration for Development (RAPID) and Consumer Unity & Trust Society (CUTS) International shows strong growth in Bangladesh's Information and Communications Technology (ICT) industry, with a target to increase ICT export revenue to $5 billion by 2025. However, stringent data localization could lead to a decline in digital service exports by 29 per cent to 44 per cent, potentially reducing Bangladesh's GDP by 0.6 per cent to 0.9 per cent.[70]

62 Drake (n 10) 11.

63 TBS News, 'Over 2,000 Startups could go out of Business for Data Protection Act: US Ambassador' (n.d.) <https://www.tbsnews.net/bangladesh/over-2000-startups-could-go-out-business-data-protection-act-us-ambassador-580770> accessed 15 February 2024.

64 Ibid.

65 World Bank, 'World Development Report 2020: Trading for Development in the Age of Global Value Chains' (World Bank 2020) <https://www.worldbank.org/en/publication/wdr2020> accessed 30 December 2023.

66 N Kshetri, 'Blockchain's Roles in Meeting Key Supply Chain Management Objectives' (2018) 39 International Journal of Information Management 80–89.

67 ITIF (Information Technology and Innovation Foundation), 'The False Promise of Data Nationalism' (2013) <https://www2.itif.org/2013-false-promise-data-nationalism.pdf> accessed 15 February 2024.

68 UNB, Dhaka, 'US has Concerns over Data Protection Act, other Media Regulations: Haas' *The Daily Star* (Dhaka, 5 February 2023) <https://www.thedailystar.net/news/bangladesh/diplomacy/news/us-has-concerns-over-data-protection-act-other-media-regulations-haas-3239856> accessed 18 July 2023.

69 IPCE (Information Policy Centre for the Environment), 'The Real-Life Harms of Data Localisation Policies (CIPL-TLS Discussion Paper, Paper I)' (n.d.) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localisation_policies.pdf> accessed 15 February 2024.

70 RAPID (Research and Policy Integration for Development), and CUTS International, 'Impact of Cross-Border Data Flow Restrictions on Bangladesh Economy: Report Two' (2022) <https://www.rapidbd.org/wp-content/uploads/2022/12/Impact-of-Cross-Border-Data-Flow-Restrictions-on-Bangladesh-Economy-Report-Two.pdf> accessed 15 February 2024.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University, Bangladesh user on 09 July 2024

Hamper the digital economy of Bangladesh

Despite witnessing numerous development challenges, Bangladesh has excelled in utilizing digital commerce providing opportunities to diversify from traditional industries. According to the United Nations Conference on Trade and Development (UNCTAD) report, Bangladesh's ICT sector has been growing at an average rate of 40 per cent annually since 2010.[71] However, the country's services export-GDP ratio is only 1.5 per cent, in contrast to other nations, such as India, the Philippines, and Sri Lanka, where the ratio is around 40 per cent.[72] Bangladesh's remarkable domestic and export growth has attracted considerable foreign direct investment from various countries, including Malaysia, the USA, India, and Norway. Particularly, the ICT- and IT-enabled services sector alone attracted $758 million in foreign direct investments during the 2019–2020 fiscal year.[73] Nonetheless, the progress in the digital economy of Bangladesh could witness significant challenges and catch up with other nations due to data localization requirements.

Restriction on freedom of expression

Freedom of expression is a crucial pillar of democratic societies, enabling individuals to openly express their thoughts, opinions, and creativity without fear of censorship or sentence. The Universal Declaration of Human Rights, 1948 guarantees the freedom of expression and the right to access and share information and ideas through any means, regardless of geographical boundaries (UDHR, Article 19).[74] Nonetheless, data localization policies can significantly restrict freedom of expression as they impede unrestrained data flow due to excessive government control, heightened surveillance, and stringent censorship over data. Thus, some scholars argue that data localization facilitates political oppression by granting the government control over information, enabling the identification and intimidation of individuals, which, in turn, has implications for privacy, data protection, and freedom of expression.[75]

Challenges in Bangladesh's legal regulation and MLA

Data localization introduces legal uncertainties, conflicts with existing laws, and requires additional time and resources for legal compliance. These challenges may be more significant than survey results suggest. For example, 47 per cent of respondents in an interview said that data localization is part of the problem, 31 per cent said it is both a problem and a solution, and only 12.5 per cent said it is part of the solution.[76] Moreover, data localization requirements make it difficult for businesses to comply with data storage, transfer, and privacy regulations. This is especially challenging for small and medium-sized enterprises (SMEs) with limited resources. The resulting higher administrative costs can impact the entire economy.[77]

Furthermore, data localization policies undermine international cooperation and prevent a country from participating in international treaties or agreements concerning mutual legal assistance (MLA) and access to evidence in civil, commercial, and other legal matters. For example, the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, 1970, is crucial for modern law enforcement, regulatory investigations, and enforcement in digital contexts.[78] Despite significant cybersecurity challenges, including rising phishing attacks and data breaches, Bangladesh has not yet signed any Mutual Legal Assistance Treaties (MLATs) on data-related matters, notably with the USA.[79] This lack of participation extends to the Cybercrime Convention;[80] which Bangladesh has neither signed nor joined as an observer.[81] This absence of international engagement could hinder international cooperation in investigating and prosecuting cybercrimes, potentially leaving Bangladeshi businesses and citizens vulnerable.

Disadvantageous for SMEs

According to a 2019 report by Bangladesh's Ministry of Planning, approximately two million young individuals

71 UNCTAD (United Nations Conference on Trade and Development), 'Bangladesh creates fertile ground for e-commerce growth' (n.d.) <https://unctad.org/news/bangladesh-creates-fertile-ground-e-commerce-growth> accessed 15 February 2024.

72 RAPID and CUTS International (n 70) 21.

73 Ibid.

74 United Nations, 'Universal Declaration of Human Rights' (1948) <https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed 15 February 2024.

75 E Fraser, 'Data Localisation and the Balkanisation of the Internet' (2016) *SCRIPTed*, 13, 366.

76 DJB Svantesson, 'Internet & Jurisdiction Global Status Report 2019' (2019) Internet & Jurisdiction Policy Network—Paris, France <https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Global-Status-Report-2019-Key-Findings_web.pdf> accessed 15 February 2024.

77 Drake (n 10) 12.

78 Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, 18 March 1970 [Hague Evidence Convention] ≤https://www.hcch.net/en/instruments/conventions/full-text/?cid=82≥ accessed 25 December 2023.

79 US Department of State, 'Money Laundering and Financial Crimes (Section 244(d) Report) Volume 2' (2012) <https://2009-2017.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm> accessed 15 February 2024.

80 Council of Europe, Convention on Cybercrime, opened for signature 23 November 2001, ETS No. 185 [Budapest Convention] ≤https://www.coe.int/en/web/cybercrime/the-budapest-convention: https://www.coe.int/en/web/cybercrime/the-budapest-convention≥ accessed 25 December 2023.

81 Council of Europe, 'Parties and Observers to the Budapest Convention' (n.d.) <https://www.coe.int/en/web/cybercrime/parties-observers> accessed 15 February 2024.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University, Bangladesh user on 09 July 2024

join Bangladesh's workforce annually, with only half of them securing jobs within the country or abroad, and SMEs can offer a solution to this challenge.[82] SMEs play a crucial role in Bangladesh's economic growth and job creation, representing 45 per cent of manufacturing value addition, 80 per cent of industrial employment, and 25 per cent of the labour force, contributing an estimated 75–80 per cent of export earnings and constituting 31 per cent of the country's GDP. It is noteworthy that out of the 79,754 SME establishments in Bangladesh, 93.6 per cent are small enterprises, while 6.4 per cent are medium-sized.[83]

However, SMEs in Bangladesh face significant challenges, including forced data localization laws. Research indicates that during the pandemic, over 70 per cent of businesses led by women in Bangladesh were established on Facebook, and there has been a 65 per cent increase in Instagram businesses owned by women.[84] If social media platforms like Facebook are compelled to cease operations in Bangladesh, SME entrepreneurs in the country would face job losses, resulting in a significant economic shock. Another research has shown that local companies would have to pay 30–60 per cent more for their computing needs due to forced data localization laws compared to countries without such requirements.[85]

Challenges for data-driven entrepreneurship and innovation

Data localization mandates harm innovation by inhibiting the growth of data-driven businesses.[86] The implementation of these policies not only stifles innovation but also discourages competition.[87] Furthermore, data localization requirements may put businesses at a competitive disadvantage, especially those with global operations, by increasing costs, burdens, and limitations on data collection and retention.[88] These policies can significantly impede international trade by making it more difficult for companies to operate in foreign markets.[89] For example, requiring businesses to store their data within specific geographical locations can restrict their access to the most recent technological advancements and impede collaboration with other businesses. Above all, data localization mandates hinder data flow and undermine data-driven services, economic productivity, and innovation by requiring companies to duplicate IT infrastructure and restricting their ability to collect, transmit, analyse, and utilize data effectively. This can hinder businesses from competing with others and developing new products and services, ultimately leading to a decline in investment in data-driven entrepreneurship and innovation.

Prevent growth of the IT-ITeS Market

With a current value of USD 1045.15 billion, the IT services market is set to witness a remarkable 8.38 per cent compound annual growth rate (CAGR) over the next five years. This translates to a market size of USD 1665.76 billion by 2028, marking a significant increase in just half a decade.[90] While India and the Philippines are the leading delivery destinations, other emerging locations have become more prominent because of their specific strengths, talent markets, and cost structures. Bangladesh is one of these emerging locations that has attracted the attention of many Information Technology enabled Services (IT–ITeS) players. Currently valued at US$ 0.9–1.1 billion, the domestic IT–ITeS industry in Bangladesh is projected to grow fivefold by 2025, reaching US$ 4.6–4.8 billion.[91] Notably, Bangladesh has emerged as the second-largest source of online labour globally after India.[92] Online workers from Bangladesh earn around $500 million

82 Ministry of Planning, Government of the People's Republic of Bangladesh 'Study on Future Direction of SMEs in Bangladesh' (2019) <https://plandiv.portal.gov.bd/sites/default/files/files/plandiv.portal.gov.bd/notices/afbffe34_be4c_417d_b36c_ecf8db4614fc/ToR%20final%20SME.pdf> accessed 28 December 2023.

83 MF Rahman, 'Potential of Small and Medium Enterprises' *The Daily Star* (Dhaka, 11 March 2015) <https://www.thedailystar.net/supplements/24th-anniversary-the-daily-star-part-2/potential-small-and-medium-enterprises-70927> accessed 15 February 2024.

84 Tech an Startup Desk, '4 Websites to Track Cyclone Mocha in rReal-time' *The Daily Star* (Dhaka 10 May 2023) <https://www.thedailystar.net/tech-startup/news/4-websites-track-cyclone-mocha-real-time-3316201> accessed 15 February 2024.

85 Leviathan Security Group, 'Quantifying the Cost of Forced Localisation' (n.d.) <https://www.leviathansecurity.com/media/quantifying-the-cost-of-forced-localisation> accessed 19 July 2023.

86 World Bank Group, *Data for Better Lives* (The World Bank, Washington, 2021).

87 Svantesson (n 7) 21.

88 Zuboff (n 28).

89 Joshua P Meltzer, 'Data and the Transformation of International Trade' (2019) <https://www.brookings.edu/articles/data-and-the-transformation-of-international-trade/> accessed 2 January 2024; Centre for Strategic and International Studies, 'Data Localization: A Free-for-All?' (2016) <https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all> accessed 2 January 2024.

90 Mordor Intelligence, 'IT Services Market—Growth, Trends, COVID-19 Impact, and Forecasts (2021—2026)' <https://www.mordorintelligence.com/industry-reports/it-services-market> accessed 29 December 2023.

91 BASIS (Bangladesh Association of Software and Information Services), 'IT and ITeS Industry Overview' (2018) <https://basis.org.bd/public/files/publication/5e127d7cb6967ba96136a3b168568073f9800e5b0f5b9.pdf> accessed 28 December 2023; LightCastle Partners, 'ICT Outsourcing Sector in Bangladesh' (2020) <https://www.lightcastlebd.com/insights/2020/01/ict-outsourcing-sector-bangladesh/> accessed 28 December 2023; BIDA (Bangladesh Investment Development Authority), *Information Technology* <https://bida.gov.bd/information-technology> accessed 28 December 2023.

92 World Economic Forum, 'How the Digital Economy is Shaping a New Bangladesh' (World Economic Forum, 19 June 2019) <https://www.wefo

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University, Bangladesh user on 09 July 2024

each year, making up about 16 per cent of the global online workforce.[93] This growth rate surpasses the average forecasted growth for established and emerging locations, such as India and Vietnam. However, the potential IT market in Bangladesh may face fierce competition from other players because of data localization requirements.

Hostile for the environmental ecosystem

Data localization policies mandate the establishment of local data centres within the country's borders to ensure the physical storage and processing of data, thereby enhancing control over data governance and security. However, implementing such policies can be a costly endeavour for Bangladesh due to the need for a consistent power supply to these data centres. Recent statistics indicate that data centres account for approximately 3 per cent of global electricity consumption, a figure projected to reach 4 per cent by 2030.[94] On average, large-scale data centres consume between 20 and 50 megawatts of electricity annually, an amount that could potentially power around 37,000 homes.[95] Even data centres consume more electricity than many entire countries, such as Nigeria, Colombia, Argentina, Egypt, and South Africa. These countries' electricity consumption ranges from 29– 208 terawatts per hour, whereas data centres worldwide consume around 200–250 terawatts per hour.[96] According to the US Department of Energy and Data Centre, data centres employing evaporative cooling systems typically have a water usage effectiveness (WUE) of 1.8 litres per kilowatt-hour, resulting in a daily water consumption of 3–5 million gallons. This amount is comparable to the water usage of a city with a population of 30,000–50,000 people.[97] While data localization may offer some perceived benefits, policymakers in Bangladesh should carefully consider the significant costs and potential environmental impacts associated with implementing such policies within their legal frameworks.

Costly but creates fewer job opportunities

Typically, data centres, in the USA, have an average size of around 100,000 square feet, with some larger ones occupying up to a million square feet.[98] Despite requiring significant land and allocation of resources, which results in high costs, data warehouses offer limited employment opportunities. In recent years, major corporations such as Google, Microsoft, Amazon, and Adani Enterprises hugely invested in data centre construction, despite requiring vast amounts of land and finances and offering limited job creation prospects. For instance, Google's data warehouses in Alabama, built in 2018, employed only 100 individuals.[99] Similarly, Microsoft's billion-dollar cloud computing-based data centres in Virginia, established in 2015, had only a few dozen employees, mostly elite computer scientists recruited from outside Boydton.[100] There is an expectation that Amazon's $12 billion investment in five data centres in Oregon will create only 120 high-tech jobs per centre.[101] Likewise, Adani Enterprises plans to establish one of the largest data centres, in India, but is likely to generate job opportunities for only 1350 people in Noida.[102] The limited employment opportunities offered by data centres, especially for highly specialized staff from outside the region, raise concerns about the rationale behind allocating substantial amounts of land and resources to establish these data centres in Bangladesh.

rum.org/agenda/2019/06/how-the-digital-economy-is-shaping-a-new-bangladesh/> accessed 28 December 2023.

93 CPD, 'Presentation on the Digital Platform Economy' (CPD, July 2021) <https://cpd.org.bd/resources/2021/07/Presentation-on-the-Digital-Platform-Economy.pdf> accessed 28 December 2023; IDLC Monthly Business Review, 'The Crucial Role of Freelancers in the Post-pandemic Economy' (2022) <https://idlc.com/mbr/article.php?id=546#:~:text=The%20crucial%20role%20of%20freelancers,the%20Financial%20Express%20in%202022.> accessed 28 December 2023.

94 E Masanet and others, 'Recalibrating Global Data Center Energy-use Estimates' (2020) Science 367(6481) 984–86 <https://www.science.org/doi/abs/10.1126/science.aay8462> accessed 15 February 2024.

95 Marcus Law, 'Energy Efficiency Predictions for Data Centres in 2023' (2023) Data Centre <https://www.datacentremagazine.com/articles/efficiency-to-loom-large-for-data-centre-industry-in-2023> accessed 15 February 2024.

96 Timothy Rooks, 'Data Centers keep Energy use Steady Despite Big Growth' (2022) DW <https://www.dw.com/en/data-centers-energy-consumption-steady-despite-big-growth-because-of-increasing-efficiency/a-60444548> accessed 15 February 2024.

97 Marcus Law (n 95).

98 Datacenters.com Technology, 'And The Title of The Largest Data Center in the World and Largest Data Center in US Goes To …' (2018) <https://www.datacenters.com/news/and-the-title-of-the-largest-data-center-in-the-world-and-largest-data-center-in> accessed 15 February 2024.

99 Katie Fehrenbacher, 'Google to Build a Big Data Center at an Old Coal Plant in Alabama' (2015) Fortune <https://fortune.com/2015/06/24/google-data-center-alabama/> accessed 15 February 2024.

100 Quentin Hard, 'Cloud Computing Brings Sprawling Centers, but Few Jobs, to Small Towns' *The New York Times* (New York, 26 August 2016) <https://www.nytimes.com/2016/08/27/technology/cloud-computing-brings-sprawling-centers-but-few-jobs-to-small-towns.html> accessed 15 February 2024.

101 Tobias Mann, 'Amazon to Spend $12b on Five more Datacenters in Oregon' (*The Register*, 6 May 2022) <https://www.theregister.com/2022/05/06/aws_oregon_datacenter/> accessed 15 February 2024.

102 'Adani Enterprises' Data Centre to Create 1,350 Jobs in Noida' *ETHRWorld (Economic Times HR World)* <https://hr.economictimes.indiatimes.com/news/industry/adani-enterprisesdata-centre-to-create-1350-jobs-in-noida/84859143> accessed 15 February 2024.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University Bangladesh user on 09 July 2024

Compromise data protection and cybersecurity

Data localization requirements increase the risk of data breaches and cyberattacks.[103] When data is stored in a specific geographic location, it can be more vulnerable to cyberattacks and data breaches. Hackers may target data centres located in countries with weaker data protection laws and exploit weak cybersecurity infrastructure. The concentration of data in a single location also makes it easier for cybercriminals to launch targeted attacks. Additionally, data stored locally may be subject to less rigorous data protection laws than data stored in more developed countries, resulting in an increased risk of data breaches. Moreover, the limited availability of local data centres may lead to lower-quality and more expensive services.

While some governments may justify data localization policies on privacy and data protection grounds, this raises several questions. Do they genuinely aim to protect privacy, or are they motivated by vague notions of national sovereignty and economic advantages? By mandating data storage within their borders, governments gain greater access to individuals' personal data, leading to heightened surveillance and potential infringements on privacy rights. Critics argue that data localization could compromise data privacy by granting government agencies increased access to user data, weakening corporate privacy and security measures, and increasing the risk of corporate data breaches, leading to more data breaches.[104] Arguably, data localization requirements may exacerbate privacy risks by mandating data storage in centralized locations, which are more susceptible to unauthorized access.[105] Above all, data localization policies may have some advantages, but the disadvantages outweigh their benefits. These policies can increase costs, reduce efficiency, limit data accessibility, and hinder innovation. Therefore, it would be advantageous for Bangladesh to adopt a flexible data protection approach that allows cross-border data flows while ensuring sufficient data protection measures. This approach would enable Bangladesh to leverage the advantages of global data connectivity, promote innovation, and enhance competitiveness in the digital economy.

Alternatives to data localization

Countries like Bangladesh can utilize various secure cross-border data transfer mechanisms instead of enforcing data localization policies. These alternative mechanisms ensure the safe transfer of data while complying with relevant data privacy laws. The alternative measures to data localization policies may include the following: (i) MLATs, (ii) adequacy decisions, (iii) certification mechanisms, (iv) data protection principles, (v) anonymization and pseudonymization techniques, (vi) enhanced cybersecurity measures, (vii) breach reporting and response, (viii) secure cloud computing, (ix) utilizing blockchain technology, (x) impact assessments techniques, and (11) industry self-regulation.

Mutual legal assistance treaties

MLA, or MLATs, involve collaborative efforts among countries to collect, share and exchange information, evidence, and documents to support criminal investigations or other legal proceedings.[106] It enables the requesting country to obtain evidence, data, documents, and files from other countries, fostering international cooperation to ensure justice. Thus, MLA, or MLATs appear as a viable alternative to data localization policies for countries like Bangladesh that facilitate cross-border data sharing and cooperation between nations. MLATs are usually official agreements requiring formal registration and public disclosure with the United Nations.[107]

Promoting international cooperation and the development of global data protection standards can facilitate Bangladesh to exchange data while ensuring consistent privacy and security practices. Collaborative efforts can establish common frameworks that alleviate the need for data localization in countries like Bangladesh. Collaborating with other countries to develop international data governance frameworks can also facilitate the harmonization of data protection regulations and promote global interoperability without mandating data localization. Furthermore, engaging in multistakeholder dialogues involving government, industry, academia, civil society, and privacy advocates can help shape effective data governance frameworks that balance data flows, privacy rights, and security concerns.

103 H Cavusoglu, B Mishra and S Raghunathan, 'Economic and Security Implications of Data Localisation' (2018) Communications of the ACM 61(9), 26–29.

104 H Jacqueline Brehmer, 'Data Localization: The Unintended Consequences of Privacy Litigation' (2017) 67 American University Law Review 927.

105 ECA (Export Council of Australia), 'From Resource Boom to Digital Boom: Capturing Australia's Digital Trade Opportunity at Home and Abroad' (n.d.) <https://export.org.au/eca-institute/from-resource-boom-to-digital-boom-capturing-australias-digital-trade-opportunity-at-home-and-abroad/> accessed 15 February 2024.

106 European Commission, 'Mutual Legal Assistance and Extradition' (n.d.) <https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en> accessed 15 February 2024.

107 UN General Assembly, 'Charter of the United Nations' (1945), art 1.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University Bangladesh user on 09 July 2024

Adequacy decisions

The government of Bangladesh can also utilize adequacy decisions to avoid data localization requirements, permitting unrestricted data transfer across borders. Under Article 45 of the GDPR, the EU allows cross-border data transfer outside the EU through adequacy decisions.[108] An adequacy decision represents an official declaration by the European Commission (EC) acknowledging that a specific country, territory, sector, or international organization provides an equivalent level of personal data protection as the EU does.[109] Consequently, countries receiving adequacy certificates from the European Commission can freely process the personal data of EU residents for lawful purposes.

The adequacy decision of the European Commission holds significant influence across the globe.[110] Thus, there has been a global wave of receiving adequacy certificates from the European Commission. Although Bangladesh currently lacks an adequacy decision from the European Commission (EC), the country should obtain it due to the close economic relationship between Bangladesh and the EU. Notably, countries such as Andorra, Argentina, Canada (for commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the UK, and Uruguay have obtained adequacy certificates from the European Commission.[111] Due to the lack of a comprehensive data protection law, Bangladesh is not eligible for an adequacy decision from the European Commission, and consequently, has never sought one.

Certification mechanism

Countries like Bangladesh can also attempt to ensure data privacy and security by employing certification mechanisms. The certification framework for international data transfers enables verifying organizations' adherence to specific privacy and security standards, thereby facilitating data transfers without the need for data localization requirements. Asia-Pacific Economic Cooperation (APEC)'s Cross-Border Privacy Rules (CBPR) is a robust certification mechanism, which serves as a means for cross-border data transfers, comparable to the EU's Binding Corporate Rules (BCR) but with a broader scope.[112] The CBPR acts as a mechanism for cross-border transfers while serving as a comprehensive programme for domestic privacy compliance and accountability.

All 21 APEC economies have endorsed the CBPR, with Australia, Canada, Chinese Taipei, Mexico, and the Philippines taking diligent steps to join. Meanwhile, the USA, Japan, South Korea, and Singapore have implemented the CBPR.[113] This may raise the question: of whether non-APEC economies like Bangladesh participate in the CBPR and Privacy Recognition for Processors (PRP) systems. The Global CBPR Forum is now open to all, and accordingly, it welcomes new members and associate members from within and outside the APEC region. Upon full implementation, businesses across all participating countries will be eligible to seek CBPR certification.[114] To the best of our knowledge, Bangladesh has never sought to participate in APEC's certification mechanism.

Data protection principles

Data protection principles form the foundation of how individuals, businesses, and organizations handle the personal data of individuals.[115] They often set forth the rights of the data subjects and inform the essence of data protection rules, laws, and policies of a particular legal regime. The principles embody the central spirit of the data protection frameworks and hence admit minimal exceptions. Compliance with these principles seems to be a building block to fair data protection culture and practices. Non-compliance thereof leads to severe legal consequences.

The primary objectives of data protection principles are to ensure that the personal data of individuals is collected, processed, and stored securely, transparently, and lawfully.[116] Data protection principles play a crucial role as an alternative to data localization policies by providing a comprehensive framework for safeguarding

108 GDPR (n 15).

109 ICO (Information Commissioner's Office), 'What is Adequacy?' (n.d.) <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/adequacy/> accessed 15 February 2024.

110 Islam MT, 'Legal Development for Privacy and Data Protection in Bangladesh' (2022) 3 Global Privacy Law Review 4.

111 European Commission, 'Adequacy decisions' (n.d.) <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 15 February 2024.

112 CIPL (Centre for Information Policy Leadership), 'APEC CBPR & PRP Questions and Answers' (2020) <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl_cbpr_and_prp_q_a_final__19_march_2020_.pdf> accessed 15 February 2024.

113 Ibid 1.

114 CIPL (Centre for Information Policy Leadership), 'Cross Border Privacy Rules, Privacy Recognition for Processors, and Global CBPR and PRP' <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_cpbr_and_prp_faq_jun23.pdf > accessed 15 February 2024.

115 Privacy International (PI), 'A Guide for Policy Engagement on Data Protection' (n.d.) <https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf> accessed 15 February 2024.

116 ICO (Information Commissioner's Office), 'A Guide to the Data Protection Principles' (n.d.) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/> accessed 15 February 2024.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University Bangladesh user on 09 July 2024

personal data and promoting responsible data governance. Rather than mandating the physical storage of data within national borders, Bangladesh can incorporate data protection principles in the PDPA 2023 in light of global best practices and implement them properly to ensure the right to privacy, data security, and geographical integrity.

This approach allows for the free flow of data across borders, fostering international cooperation, enabling innovation, and supporting economic growth while addressing data privacy and security concerns. By emphasizing certain principles, such as informed consent, purpose limitation, data minimization, transparency, and accountability, Bangladesh can establish a strong foundation for protecting individuals' right to privacy and safeguarding personal data without resorting to restrictive data localization requirements.

Data privacy laws are generally based on key data protection principles established by the OECD in 1980 and adopted subsequently by most major data privacy regulations across the globe, but the draft Bangladeshi PDPA does not clearly articulate these principles.[117] While Bangladesh's draft Personal Data Protection Act 2023 (PDPA) comprises 10 data protection principles, including (i) consent and accountability, (ii) fair and reasonable, (iii) integrity, (iv) retention, (v) access to data and data quality, (vi) disclosure, (vii) security, (viii) risk-based protection and consistent protection, and (ix) enforceable standards,[118] it falls short of adequately reflecting the eight core principles enshrined in the 1980 OECD Privacy Guidelines,[119] the bedrock of data protection laws globally. This discrepancy warrants further examination.

Notably, the PDPA lacks the emphasis on data minimization and purpose limitation that the OECD Privacy Guidelines prioritize. Similarly, the PDPA primarily focuses on the accountability and transparency principles of the APEC Privacy Framework (2005, amended 2015)[120] but could benefit from incorporating its 'data portability' and 'cross-border cooperation' aspects for a more comprehensive approach. Compared to the EU GDPR, the PDPA aligns well with core principles and individual rights. However, it significantly lacks the GDPR's stringent data breach notification requirements and detailed provisions for automated decision-making and profiling. This disparity raises concerns about the PDPA's ability to adequately safeguard individuals in the face of increasingly sophisticated data processing practices. Likewise, while the PDPA shares the California Consumer Privacy Act of 2018 (CCPA)'s[121] focus on individual control and opt-out rights, it could benefit from adopting the CCPA's broader scope of data protection rights and a more precise definition of 'personal information'.

Anonymization and pseudonymization techniques

Promoting anonymization and pseudonymization techniques can safeguard data privacy in Bangladesh while allowing data transfers freely across borders. By leveraging anonymization and pseudonymization techniques, Bangladesh can share data across borders without violating data protection regulations. Arguably, anonymized and pseudonymized data serve as a viable alternative to data localization policies by enabling the global exchange of information while respecting individuals' privacy rights.

Anonymized data refers to information that does not pertain to an identified or identifiable person.[122] Through this technique, data processing happens in a manner which prevents it from being linked to any specific individual. Thus, anonymized data is no longer considered personal data and is not subject to data protection laws. Pseudonymized data, on the other hand, refers to data processing in a way that it cannot be directly linked to a particular individual without utilizing additional information, or hidden code taken separately. While, pseudonymized data can be re-identified by combining it with separately held additional information, it may be considered personal data. Therefore, data protection laws generally apply to pseudonymized data.[123]

117 TIB (n 44).

118 PDPA 2023 (n 43).

119 Organization for Economic Co-operation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (adopted 23 September 1980) [OECD Privacy Guidelines] <https://legalinstruments.oecd.org/public/doc/114/114.en.pdf> accessed 25 December 2023.

120 Asia-Pacific Economic Cooperation (APEC), APEC Privacy Framework (2005, amended 2015) [APEC Privacy Framework] <https://www.apec.org/docs/default-source/publications/2005/12/apec-privacy-framework/05_ecsg_privacyframewk.pdf?sfvrsn=d3de361d_1> accessed 25 December 2023.

121 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq. (Westlaw California Code Annotated) <https://theccpa.org/> accessed 15 February 2024.

122 European Commission, 'What is Personal Data?' (n.d.) <https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en> accessed 15 February 2024.

123 ICO (Information Commissioner's Office), 'Chapter 3: pseudonymisation Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance' (2022) <https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf> accessed 15 February 2024.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University Bangladesh user on 09 July 2024

In essence, data protection laws specifically apply to pseudonymized data, not anonymized data. However, all previous PDPA drafts treated pseudonymized and anonymized data equally, failing to recognize their fundamental differences. Sections 2(a) and 2(b) of the current draft of the PDPA, for example, treat them as equivalent, even though the final paragraph of section 2(b) and section 4(2) exempt pseudonymized data from the PDPA's scope. Therefore, the PDPA must explicitly differentiate between anonymized and pseudonymized data to ensure its effectiveness, potentially by providing separate definitions or applying different treatments in relevant sections.[124]

Enhanced cybersecurity measures

Enhancing cybersecurity measures within the national legal framework in Bangladesh can address data security concerns without the need for data localization. Cybersecurity is the capability of individuals or organizations to safeguard their virtual presence, spaces, and assets from a multitude of unauthorized or illegal cyberattacks.[125] Cybersecurity encompasses practical actions adopted to safeguard information, networks, and data against potential threats arising from both internal and external sources.[126] Therefore, the government of Bangladesh should invest in cybersecurity capacity-building initiatives, training and technical support programmes to enhance the overall cybersecurity mechanisms throughout the country. By encouraging the use of strong encryption techniques, Bangladesh can protect data during transmission and storage stages. By promoting encryption standards and supporting encryption technologies, Bangladesh can also ensure the security and confidentiality of data without resorting to data localization.

Breach reporting and response

Bangladesh should emphasize incorporating the provisions of mandatory data breach reporting in the PDPA, as it can enhance transparency and accountability in handling personal data. This approach focuses on quick detection, notification, and remediation of data breaches rather than imposing localization requirements. Besides, implementing stringent data breach notification requirements can ensure timely reporting and response to data breaches. This helps protect individuals' data without the need for data localization.

A company or organization is responsible for a data breach incident that compromises the confidentiality, availability, or integrity of the data they handle. Such incidents have the potential to jeopardize the rights and freedoms of individuals. Detecting and responding to security breaches is essential for maintaining a high level of security, allowing organizations to learn from breaches, preventing future breaches and helping organizations respond to data breaches by notifying customers and taking corrective actions.[127]

It is worth mentioning that the previous draft of the PDPA required data controllers to immediately notify the data protection agency (now the Data Protection Board) about data breaches. However, the term 'immediately' was unclear due to the lack of interpretation of the word in the PDPA. We suggested that data controllers must inform the Data Protection Board of data breaches within 72 hours, as per international best practices. We also suggested that data controllers should promptly inform affected individuals of data breaches that pose a high risk to their rights and freedoms.[128] Even though the timeframe for this notification may be longer, it must be clearly defined. The latest draft of the PDPA now mandates data controllers to notify the Data Protection Board of data breaches within 72 hours, which is a positive step. Nevertheless, the latest draft does not incorporate our suggestion for cases of high risk to data subjects' rights and freedoms. In such instances, data controllers should promptly inform affected data subjects of the breach without undue delay.

Secure cloud computing

Promoting the use of encrypted cloud storage services presents a viable alternative to physical data localization. Cloud computing technology ensures the safety of data stored or transmitted within the cloud, protecting it

124 PDPA 2023 (n 43).

125 Islam, MT and R Karim, 'Cybersecurity and Integrated Business Models' in Sumesh Singh Dadwal, Hamid Jahankhani and Azizul Hassan (eds), *Integrated Business Models in the Digital Age* (Cham Switzerland, Palgrave Macmillan 2022).

126 Yuchong Li, and Qinghui Liu, 'A Comprehensive Review Study of Cyber-attacks and Cyber Security; Emerging Trends and Recent Developments' (2021) 7 Energy Reports 8176–86.

127 FTC (Federal Trade Commission), 'Security Beyond Prevention: The Importance of Effective Breach Disclosures' (2022) <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/05/security-beyond-prevention-importance-effective-breach-disclosures> accessed 15 February 2024.

128 Both authors were invited to the Stakeholder's Consultation on the Draft Data Protection Act 2022, organized by the ICT Division, Post, Telecommunications, and ICT Ministry of the Government of the People's Republic of Bangladesh, held in Dhaka on 17 July 2022. The first author had the opportunity to provide comments from his own capacity, twice in favour of the EU Dhaka Delegation and twice in favour of Transparency International Bangladesh (TIB).

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University Bangladesh user on 09 July 2024

against security threats, unauthorized access, theft, and corruption. It utilizes physical security, technological tools, access management, controls, and organizational policies as essential components.[129] Cloud providers can store and process data in different countries while implementing appropriate security measures. By leveraging this technology and encrypting data, Bangladesh can securely store and access data without requiring physical data storage within its territorial boundary. Hence, the government of Bangladesh can encourage the adoption of secure cloud computing services that comply with rigorous data protection standards, thereby avoiding the necessity of data localization policies.

Employing blockchain technology

Blockchain technology employs an advanced database mechanism to enable secure and transparent information sharing within a business network. It stores data in interconnected blocks, ensuring chronological consistency and immutability without network consensus. With built-in mechanisms to prevent unauthorized transactions and ensure consistency, blockchain distributes identical copies of the database across the network, making it highly resistant to hacking or manipulation.[130] Organizations can utilize this technology to establish an immutable ledger that tracks transactions (orders, payments, and accounts), preventing unauthorized activity and ensuring consistency through distributed copies of the database.[131]

The utilization of blockchain technology for secure and decentralized data storage and management offers another suitable alternative to data localization policies. This approach enhances privacy protection through decentralized identity management, restricted data sharing with trusted third parties, and the potential substitution of contractual solutions like the European Commission's Standard Contractual Clauses for cross-border data transfers.[132] In summary, blockchain is a secure technology that facilitates trustworthy information sharing without data localization requirements.

Recognizing the potential of blockchain technology for secure and private data management, Bangladesh adopted the 'National Blockchain Strategy: Bangladesh' in 2020. This strategy positioned the country as a blockchain-powered nation, prioritizing the secure and private handling of sensitive data (particularly in government, finance, and healthcare) through advanced cryptographic solutions like zero-knowledge proof and privacy overlays. The national blockchain platform aims to safeguard data security across these sectors, fostering transparency and trust in data storage and retrieval.[133]

Impact assessment techniques

Alongside raising awareness about privacy through education and targeted campaigns, inspiring stakeholder engagement, ensuring transparency in surveillance practices, and conducting privacy impact assessments (PIA) remain the potential measures for mitigating privacy challenges.[134] A PIA is a process to identify and minimize privacy risks associated with projects, systems, or policies involving personal data, ensuring compliance and evaluating measures to mitigate potential privacy risks.[135] These tools are essential when processing poses a high risk to individuals' rights and freedoms, such as extensive evaluation of personal aspects, processing sensitive data on a large scale, or systematic monitoring of public areas.[136] The government of Bangladesh can make well-informed decisions about data regulation and governance by conducting PIA to assess the impacts of data localization policies across various sectors. Governments in countries like Bangladesh can also incentivize voluntary data localization through tax breaks, grants, or other benefits, allowing organizations to choose based on their needs and circumstances.

129 Google Cloud, 'What is Cloud Data Security? Benefits and Solutions' (n.d.) <https://cloud.google.com/learn/what-is-cloud-data-security#:~:text=Cloud%20data%20security%20protects%20data,and%20controls%2C%20and%20organizational%20policies> accessed 21 July 2023.

130 David Rodeck and Michael Adams, 'Understanding Blockchain Technology' (2023) <https://www.forbes.com/advisor/investing/cryptocurrency/what-is-blockchain/> accessed 21 July 2023.

131 AWS (Amazon Web Services), 'What Is Blockchain Technology?' (n.d.) <https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc> accessed 21 July 2023.

132 Lokke Moerel, 'Blockchain and Data Protection' in Larry A DiMatteo, Michel Cannarsa and Cristina Poncibò (eds), *Smart Contracts, Blockchain Technology and Digital Platforms* (CUP, Cambridge, United Kingdom 2019).

133 For details, see generally ICT Division, Post, Telecommunications, and ICT Ministry of the Government of the People's Republic of Bangladesh, 'National Blockchain Strategy: Bangladesh' <https://ictd.gov.bd/sites/default/files/files/ictd.portal.gov.bd/legislative_information/00560d42_fc92_4ae5_b13a_774a33f864bd/Blockchain%20Strategy%20Bangladesh_4%20March%202020.pdf> accessed 15 February 2024.

134 Islam MT, 'Protection of Privacy in Bangladesh: Issues, Challenges and Way Forward' 28 International Journal of Human Rights (2023) 89–124 <https://doi.org/10.1080/13642987.2023.2234296> accessed 29 October 2023.

135 European Commission, 'When is a Data Protection Impact Assessment (DPIA) Required?' (n.d.) <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en> accessed 15 February 2024.

136 Ibid.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University, Bangladesh user on 09 July 2024

Industry self-regulation

Self-regulation has become a topic of academic interest since the late 1990s.[137] In Europe, self-regulation emerged as a key component of second-generation data protection norms, intending to reduce the administrative burden on government agencies in protecting personal data. Self-regulation refers to a system of data protection governance in which industry or professional entities establish and enforce rules that apply to their members. The content of these rules is primarily determined by members of that industry or profession. In this article, self-regulation refers to regulatory frameworks established and implemented by industry actors, often in collaboration with governments. This approach excludes direct government legislation and regulations delegated to industry for enforcement. Examples of self-regulation include industry-wide regulatory codes, professional bodies' codes of conduct, industry service charters, guidelines, standards, accreditation processes, and complaint-handling schemes.[138]

Industry self-regulation can complement government policies and offer advantages to the government, industry, and consumers. It can address issues where governments have limited authority, reduce enforcement burdens, provide better consumer information, and dispute resolution, combat unfair practices, and enhance consumer rights. The success of self-regulation in data protection depends on sincere commitments, broad industry coverage, participant adherence, and clear consequences for non-compliance.[139] Recognizing the importance of data privacy control, the Bangladesh government has included strengthening self-regulation as a prime objective in the e-Government Master Plan for Digital Bangladesh 2019.[140] This plan outlines a comprehensive strategy for promoting digital governance and data security, focusing specifically on empowering individuals to control their personal information online.

Conclusion

Data localization policies have significant implications for the free flow of data, a critical element for businesses, innovation, and economic growth. This free flow of data enables global collaboration, fuels the development of new technologies, and drives economic prosperity across industries. Governments worldwide have different views on data localization policies, with some supporting them and others opposing them. Given the substantial impacts of data localization policies on privacy, security, and innovation, careful consideration is essential before implementing them. This article argues that adopting data localization policies can hinder economic growth, restrict data accessibility, and increase compliance costs for businesses in Bangladesh.

Data localization policies of some countries still adhere to the misconception that storing data within a country's borders is the most effective way to protect it. The popular assumption that storing data in local data centres benefits everyone is not only misleading but also counterproductive. Data security is independent of physical storage location, as evidenced by numerous cloud breaches and vulnerabilities in local servers. While data localization may seem appealing, countries like Bangladesh can achieve their desired security goals through alternative approaches by implementing robust encryption protocols, adopting comprehensive data security frameworks, and promoting international data-sharing agreements. These alternative measures offer greater flexibility, strengthen data protection, and foster a thriving digital economy.

Although advocates of data localization policies emphasize national sovereignty, security, protectionism, and digital data protection, these policies often enable authoritarian governments to gain greater control over the personal data of individuals, compromising privacy, data protection, and freedom of expression.[141] Data security relies on implementing both logical and physical techniques. Logical techniques involve using strong encryption methods on devices to protect data from unauthorized access. Physical techniques, on the other hand, focus on safeguarding the external perimeter of data centres to prevent intrusions. Instead of resorting to data localization measures, countries like Bangladesh should also prioritize the accountability principle and implement compatible safeguard measures that comply with national standards, even in cross-border data transfers. Additionally, organizations involved in global

137 Jedidiah Bracy, 'Will Industry Self-Regulation Be Privacy's Way Forward?' (2014) <https://iapp.org/news/a/will-industry-self-regulation-be-privacys-way-forward/> accessed 21 July 2023.

138 Commonwealth of Australia, 'Industry Self-Regulation in Consumer Markets' (2020) <https://treasury.gov.au/sites/default/files/2019-03/final_report.pdf> accessed 15 February 2024.

139 OECD (Organisation for Economic Co-operation and Development), 'Industry Self-Regulation: Role and Use in Supporting Consumer Interests' (2015) <https://one.oecd.org/document/DSTI/CP(2014)4/FINAL/En/pdf> accessed 15 February 2024.

140 Bangladesh Computer Council (BCC), 'e-Government Master Plan for Digital Bangladesh' (2019) <https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/publications/3f9cd471_9905_4122_96ee_ced02b7598a9/2020-05-24-15-54-43f3d2b8b4523b5b62157b069302c4db.pdf> accessed 15 February 2024.

141 Fraser (n 75) 359.

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University Bangladesh user on 09 July 2024

data transfers should implement internationally recognized best practices and robust internal controls throughout the process to ensure comprehensive data protection.

In essence, data localization presents a complex dilemma with multifaceted impacts on businesses, governments, and individuals. While arguments exist for both localization and global data flows, a universal solution remains elusive. For Bangladesh, navigating this landscape requires a nuanced approach, carefully weighing its specific needs, objectives, and risks. Balancing potential impacts on privacy, security, and innovation is crucial, aiming for a harmonious outcome for all stakeholders. Alternative measures like MLATs, adequacy decisions, data protection principles, anonymization and pseudonymization techniques, enhanced cybersecurity measures, breach reporting and response, secure cloud computing, employing blockchain, data protection impact assessments, and industry self-regulation offer viable options to bypass data localization policies while upholding data security. By embracing these approaches, Bangladesh can ensure data protection without the potential drawbacks of localization.

https://doi.org/10.1093/idpl/ipae002

Downloaded from https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipae002/7618944 by Independent University Bangladesh user on 09 July 2024