BEYOND DIGITAL PROTECTION(ISM)

Comparing Data Governance Frameworks in Asia

Rohan Grover, Kyooeun Jang, and Li Wen Su

ABSTRACT

What values and conceptualizations of data are being advanced through new data protection regulations in Asia? This article answers this question with a comparative analysis of data protection regulations in China, India, and South Korea. The article identifies four key dimensions of divergence: conceptualizations of personal and sensitive information, cross-border data transfer restrictions, state exceptions, and considerations for platforms. This leads to three conclusions: local notions of "privacy" are animated by complex domestic priorities and geopolitics, data protection regulations contribute to platform governance, and local exceptions to data protection regulations reveal diverse political strategies to manage citizen-state relations.
Keywords: data protection, digital protectionism, privacy, comparative policy analysis, data localization

Personal data are increasingly a site of political and economic contestation. As of 2022, 157 countries have implemented data protection regulations.[1] While many are modeled after the European Union's (EU) General Data Protection Regulation (GDPR), these regulations represent various data governance frameworks based on various premises such as human rights, innovation, economic opportunity, cybersecurity, and privacy rights.

Rohan Grover: Annenberg School for Communication and Journalism, University of Southern California

Kyooeun Jang: Annenberg School for Communication and Journalism, University of Southern California

Li Wen Su: Annenberg School for Communication and Journalism, University of Southern California

https://doi.org/10.5325/jinfopoli.14.2024.0005

1. Graham Greenleaf, "Now 157 Countries: Twelve Data Privacy Laws in 2021/22," *Privacy Laws & Business*, April 7, 2022, https://www.privacylaws.com/reports-gateway/articles/int176/int176newdplaws/.

Consequently, trends have emerged that indicate potential policy convergence from alternative sources in addition to the GDPR.

One trend is for states to implement restrictions on cross-border data transfers, especially data localization requirements. In response, some have criticized these regulations as *protectionist*, especially under authoritarian regimes, while others have defended them for advancing *digital sovereignty*. However, these terms may represent vague discursive practices rather than specific regulatory policies;[2] therefore, it is important to situate these disagreements within specific contexts to unpack precisely how these ideas are interpreted and operationalized. This requires closely and critically examining the most recently evolved data protection regulations within their local contexts.

Thus, we do ask: how do diverse sociotechnical and geopolitical contexts and relations animate different approaches to data governance? We explore this question by comparing personal data protection regulations in three Asian states with significant IT industries: the Personal Information Protection Act (PIPA) in South Korea, the Personal Information Protection Law (PIPL) in China, and the Digital Personal Data Protection Act (DPDPA) in India. In this article, we present a descriptive background of each law and outline a comparative analysis based on four key themes: conceptualizations of "personal data," cross-border data transfers, state exemptions for data access, and special considerations for platforms and businesses. We then discuss the implications of these comparisons for the ongoing debate about data governance and digital protectionism. We conclude that personal data protection regulations must be understood within the context of each state's specific conceptualization of privacy, its relationships with major tech platforms, and its approach to citizen–state relations. These findings carry implications for evaluating data protection regulations within specific contexts and not within a simple binary distinction between an open or fragmented internet.

Data Governance: Somewhere between Protectionism and Sovereignty

Regulating Personal Data

Scholarship on the proliferation of data protection regulations often centers on the EU's GDPR, which was adopted in 2016 and went into

2. Julia Pohle, and Thorsten Thiel, "Digital Sovereignty," *Internet Policy Review* 9, no. 4 (2020), https://doi.org/10.14763/2020.4.1532.

effect in 2018. Its legal basis can be found in the EU's right to privacy, which was developed in response to the Nazi regime's atrocities.[3] Since then, the EU has embraced a distinct right to data protection, as codified through Directive 95/46/EC (Data Protection Directive) in 1995, which sought to harmonize data protection practices across the EU member states.[4] However, enforcement was weak and uneven; therefore, the GDPR was an attempt to address these issues primarily to support the European economy by promoting the free flow of data within the EU.[5] In practice, however, the GDPR has been interpreted and enforced to a greater degree as a tool to protect personal data.[6] For example, the courts have limited cross-border transfers of personal data primarily on the basis of the potential for violating people's fundamental right to privacy in other jurisdictions—not necessarily to protect the EU's economic interests.[7] Thus, the GDPR only permits cross-border data transfers of personal data to jurisdictions with "adequate" data protection or to organizations with contractual agreements to offer equivalent data protections.

The spread of personal data protection regulations around the world since 2016 has been interpreted as evidence of policy diffusion or policy transfer of the GDPR. Specifically, Colin Bennett characterizes three ways in which the GDPR has shaped other regulations: as a basis for harmonization, providing a template for other states to adopt; as an exemplar, creating a hierarchy of states according to EU standards; and through coercion, by restricting cross-border data transfers without equivalent or adequate protections.[8] Anu Bradford, therefore, argues that the EU has immense unilateral power to shape and regulate global markets through its own market

3. Alvar Freude and Trixy Freude, "Echoes of History: Understanding German Data Protection," *Newpolitik* (2016): 85–91, https://www.astrid-online.it/static/upload/freu/freude_newpolitik_german_policy_translated_10_2016-9.pdf.

4. Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Brussels, Belgium: Spring, 2014).

5. Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, "The European Union General Data Protection Regulation: What It Is and What It Means," *Information & Communications Technology Law* 28, no. 1 (2019): 65–98, https://doi.org/10.1080/13600834.2019.1573501.

6. Ibid.

7. Ibid.

8. Colin J. Bennett, "European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?" *Information Polity* 23, no. 2 (2018): 239–46, https://doi.org/10.3233/IP-180002.

power.[9] However, recent data protection regulations have diverged from the GDPR in important ways. For example, recent regulations have featured registration systems, granted rights to deceased persons, and enacted data localization practices guided by various principles, including human rights, innovation, cultivating domestic industry, and privacy rights.[10]

Data Localization

One prominent feature of many data governance regulations is *data localization*. Richard Taylor defines data localization as regulations that require data "to be maintained and processed within the geographic boundaries of its state of origin."[11] He situates data localization initiatives within the broader policy framework of cross-border data transfer (CBDT) regulations, which were originally enacted by European states in the 1970s and later by the Organisation for Economic Co-operation and Development (OECD), the EU, and the Asia-Pacific Economic Cooperation (APEC). Today, CBDT regulations can be found in more than 100 countries, and they are based on a variety of legal foundations, including human rights, privacy rights, national security, and international trade.[12] According to Taylor, the US has attempted to stymie CBDT restrictions by other countries by incorporating the "free flow of information" as a policy principle in international trade agreements, provoking concern from other states.[13] However, public awareness of the National Security Agency's global surveillance regime, as disclosed by Edward Snowden in 2013, marked a turning point in CBDT regulations.[14] Many states were alarmed by the extent to which the US government was able to access data stored on domestic servers, and these concerns were exacerbated by the US's dominance in e-commerce and internet governance.[15] In response, states have increasingly adopted enhanced CBDT restrictions.

9. Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020).

10. Greenleaf, "157 Countries."

11. Richard D. Taylor, "Data Localization: The Internet in the Balance," *Telecommunications Policy* 44, no. 8 (2020): 1, https://doi.org/10.1016/j.telpol.2020.102003.

12. Ibid.

13. Ibid.

14. Ibid.

15. Susan Ariel Aaronson, "What Are We Talking about When We Talk about Digital Protectionism?" *World Trade Review* 18, no. 4 (2019): 541–77, https://doi.org/10.1017/S1474745618000198.

CBDT restrictions do not refer to a single policy but rather to a broad regulatory strategy that can manifest in different ways. At least thirteen types of CBDT restrictions have been identified, including those requiring local data storage and data protection features (e.g., privacy adequacy thresholds or consent requirements), limiting state access to data, preventing certain data from leaving the country, and providing incentives for using local content.[16]

Different CBDT mechanisms reflect the variety of underlying legal and policy frameworks and goals. In particular, data localization has attracted criticism for constraining or preventing certain uses of the internet to create, distribute, or access information resources.[17] For example, data localization has been criticized for impairing e-commerce by fragmenting the internet,[18] favoring large companies that are better equipped to handle diverse localization requirements in different countries, disrupting cloud services by disabling companies from utilizing global storage infrastructure, and curtailing innovation by limiting businesses' access to insights.[19] These criticisms are often used to characterize data localization policies as either "democratic" or "authoritarian" in asserting digital sovereignty. Scholars have argued that there is no single approach to either model.[20]

Overall, the widespread adoption of data localization policies challenges two normative framings in internet governance: a global, deterritorialized internet with an open flow of data and the GDPR as a template for global data protection regulations. They, therefore, highlight how internet architecture is inherently bordered despite conceptions of de-territoriality—and how those borders differentially affect internet policy and economic activity in different sociotechnical and geopolitical contexts.

---

16. Business Roundtable, *Putting Data to Work: Maximizing the Value of Information in an Interconnected World* (Washington, DC: Business Roundtable, 2015), https://s3.amazonaws.com/brt.org/archive/reports/BRT%20PuttingDataToWork.pdf.

17. Neha Mishra, "Data Localization Laws in a Digital World: Data Protection or Data Protectionism?" *The Public Sphere: Journal of Public Policy* 4, no. 1 (2016): 135–58, https://psj.lse.ac.uk/articles/abstract/45/.

18. William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter. "Internet Fragmentation: An Overview." *World Economic Forum*, 2016, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

19. Ibid.

20. Liliya Khasanova, and Katharin Tai. "Authoritarian Approach to Digital Sovereignty? Russian and Chinese Data Localisation Models," *Social Science Research Network* (2023), https://doi.org/10.2139/ssrn.4527052.

Data Protection or Digital Protectionism?

A common criticism of data localization regulations is that they advance the controversial economic goal of *digital protectionism*. Susan Aaronson demonstrates that protectionism, similar to concepts discussed earlier such as digital sovereignty and data localization, does not refer to a specific policy but rather to an ideology and a policy framework.[21] Historically, policies have been classified as protectionist if they "alter market conditions and distort trade in ways that favor domestic producers over their foreign competitors."[22] However, individual policies cannot be easily classified as protectionist or not because they can be assessed either according to their intent or impact. Thus, even when states accuse each other of enacting protectionist policies, debates cannot be easily settled because different criteria may lead to different conclusions. In addition, protectionist policies are often explicitly sanctioned in trade agreements to protect specific national interests. For example, the World Trade Organization (WTO) permits trade restrictions that are justified on the basis of reasons such as national security, public morals, public health, and safety.[23] Thus, even some policies that are protectionist in effect are considered permissible—and indeed, all states enact such policies from time to time. The key takeaway for the present discussion is that protectionism is not a definitive or objective classification of specific policies but rather an expression of a particular assessment of legitimacy that reflects an actor's own policy framework and ideology. In sum, claims of protectionism cannot be separated from an actor's economic and geopolitical positionality.

It is nevertheless important to refine our understanding of protectionism because of its continued centrality in both trade and geopolitics. This is especially true in the case of *digital* protectionism, which Aaronson clarifies is distinct from traditional protectionism in several ways, not least because data exceed the traditional binary between goods and services.[24]

---

21. Aaronson, "What Are We Talking about When We Talk about Digital Protectionism?"

22. Ibid., 546.

23. General Agreement on Trade in Services, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167, April 15, 1994, https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.

24. Aaronson, "What Are We Talking about When We Talk about Digital Protectionism?"; Susan Ariel Aaronson, "Data Is Different, and That's Why the World Needs a New Approach to Governing Cross-Border Data Flows," *Digital Policy, Regulation and Governance* 21, no. 5 (2019): 441–60, https://doi.org/10.1108/DPRG-03-2019-0021.

Crucially for this discussion, she argues that "there is no clear model that policymakers can use to distinguish between legitimate and trade-distorting data flow regulation."[25] She, therefore, turns to the United States' evolving definition of digital protectionism by examining its iterations over multiple trade agreements. Her synthesized conceptualization of digital protectionism includes the following mechanisms that impede digital trade: tariffs on digital goods, data localization requirements, data flow restrictions, intellectual property, national standards, filtering or blocking services, net neutrality, and cybersecurity.[26] This typology of digital protectionism mechanisms serves as a framework for evaluating personal data protection regulations in the present study.

Why focus on personal data protection regulations in particular? Although it shares a common etymological root with digital protectionism (albeit referencing distinct beneficiaries of protection: individuals vs. the state), data protection regulations are relevant to digital protectionism because the balance between promoting economic activity and necessary privacy protections has been controversial. For example, the US has argued that "privacy protections bolster trust in the internet and are essential to stimulating the growth of digital technologies" and the EU has created a regional floor for privacy through the GDPR.[27] According to these approaches, data protection regulations are necessary for a global, secure, and sovereign internet. Indeed, scholars have found that restrictions on data flows could be excepted from WTO limitations based on national security interests, although the efficacy of such restrictions is dubious and potentially minimal.[28] On the other hand, some have argued that data privacy regulations—specifically the GDPR—splinter the internet by effectively censoring certain content on a regional basis and restricting trade based on adequacy requirements.[29] Thus, as more states adopt data

25. Aaronson, "What Are We Talking about When We Talk about Digital Protectionism?" 548.

26. A separate analysis produced a similar typology of digital protectionist strategies with only one unique category: restrictions on electronic payment systems or the use of encryption. Arguably, these could fall under the categories of standards and/or cybersecurity.

27. Aaronson, "What Are We Talking about When We Talk about Digital Protectionism?" 559.

28. Martina Francesca Ferracane, "Data Flows and National Security: A Conceptual Framework to Assess Restrictions on Data Flows under GATS Security Exception," *Digital Policy, Regulation and Governance* 21, no. 1 (2018): 44–70, https://doi.org/10.1108/DPRG-09-2018-0052.

29. Aaronson, "What Are We Talking about When We Talk about Digital Protectionism?"; Ziyang Fan and Anil K. Gupta, "The Dangers of Digital Protectionism," *Harvard Business Review*, August 30, 2018, https://hbr.org/2018/08/the-dangers-of-digital-protectionism.

protection regulations that appear to resemble the GDPR, it is important to evaluate the extent to which such regulations advance protectionist intent and effects.

Within this debate about data protection regulations, the very definition of *personal data* is a key object of debate. Susan Aaronson argues that data regulation in trade agreements should distinguish among five types of data: personal data, confidential data, public data, metadata, and machine-to-machine communication.[30] However, the category of personal data—the primary object of data protection regulations passed to advance individual privacy—is defined differently within each national policy. This illustrates how important it is to define such terms precisely—ideally through comparative analysis to account for conflicting understandings of the fundamental values that motivate such policies rather than adopting definitions and frameworks exclusively from the US and EU. Thus, we contribute to refining the debate on digital protectionism by drawing from alternative sites and conceptualizations of what, specifically, needs to be protected, including privacy, national interests, and trade.

Theoretical Framework

Given that even the definition of personal data itself—the very object of regulation—is unsettled, we mobilize a theoretical framework based on critical policy studies to account for complexity and heterogeneity across national contexts. Critical policy studies, as an approach, is analytically instrumental to defamiliarize and destabilize assumptions about the policy object at hand—in this case, data protection regulations as products of diffusion that need to be classified and harmonized to facilitate implementation. Such assumptions can be found in scholarship that, for example, responds to new data protection regulations by comparing them with the GDPR as a unilateral source of policy diffusion, as discussed previously.[31] Such assumptions risk taking for granted the centrality of EU policy—and the logics that have shaped it over the course of history—and privileging technical operationalization over contextual understanding.[32]

30. Aaronson, "What Are We Talking about When We Talk about Digital Protectionism?" 568.
31. Bradford, *The Brussels Effect*; Bennett, "European General Data Protection Regulation."
32. Freude and Freude, "Echoes of History."

We draw on Fischer et al.'s synthesis of critical policy studies as an interpretive, contextual, and situated analysis of policy.[33] Specifically, this means that we interrogate categories and characterizations (such as protection, protectionism, and sovereignty), compare them in situated ways to discern meaning, and seek to pierce the aura of technical objectivity to uncover how data and technologies mediate relations. While we pursue similar questions in our analysis, such as by comparing different definitions of personal data, we avoid focusing entirely on questions of harmonious implementation, and we begin instead by situating each law in its own context rather than tracing its origins only to the EU. This approach surfaces some relations more readily than others, such as states' relationships with their own digital economies, citizens, states, and platform companies.

This approach—interpretive, contextual, situated critical policy studies—helps us build on a growing body of comparative scholarship that explores how public policy—especially science and technology policy—mediates sociotechnical relations.[34] The comparative approach also helps us "avoid the intellectual trap of taking as universal epistemic and ethical assumptions that turn out, on investigation, to be situated and particular."[35] This is especially important given our epistemic commitment to destabilizing the object of policy by avoiding a direct comparison solely with the GDPR and our interest in interrogating the binary distinction between protectionism vs. sovereignty.

Using this framework, we ask: how do sociotechnical and geopolitical contexts and relations animate different approaches to data governance? We address this question by conducting a comparative analysis of personal data protection regulations across three states with significant economies and IT industries: South Korea, China, and India. What are the specific

33. Frank Fischer, Douglas Torgerson, Anna Durnová, and Michael Orsini, "Introduction to Critical Policy Studies," in *Handbook of Critical Policy Studies*, ed. Frank Fischer, Douglas Torgerson, Anna Durnová, and Michael Orsini, 1–24 (Cheltenham: Edward Elgar Publishing, 2015), https://doi.org/10.4337/9781783472352.00005.

34. Maureen McNeil, Michael Arribas-Ayllon, Joan Haran, Adrian Mackenzie, and Richard Tutton, "Conceptualizing Imaginaries of Science, Technology, and Society," in *The Handbook of Science and Technology Studies* (4th edn.), ed. Ulrike Felt, Rayvon Fouché, Clark A. Miller, and Laurel Smith-Doerr, 435–63, 451 (Cambridge, MA: MIT Press, 2016).

35. Sheila Jasanoff, "Future Imperfect: Science, Technology, and the Imaginations of Modernity," in *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*, ed. Sheila Jasanoff and Sang-Hyun Kim, 1–33, 24 (Chicago: University of Chicago Press, 2015), https://doi.org/10.7208/9780226276663-001.

values, conceptualizations, and relations that are advanced with actually existing personal data protection regulations, and how do they help navigate the debate about the relationship between data protection and digital protectionism?

Methodology

We approach this question through a comparative analysis of personal data protection regulations in Asia. Comparative policy analysis is an ideal method not only because we focus on policy translation and sociotechnical imaginaries but also because data governance affects multiple states because of economic interdependence, similar underlying policy problems, and naturally transnational issues.[36] Approaches that prioritize frameworks such as protectionism or sovereignty are inherently transnational because they affect how commerce and trade can be conducted across borders. In this context, comparative analysis is also valuable for illuminating how local circumstances interact with broader dynamics. This is important in the study of digital protectionism and sovereignty because these concepts reflect multiple interpretations that should be precisely grounded in specific empirical contexts to facilitate analytic clarity.

We selected South Korea, China, and India for comparative analysis. Researchers often approach comparative scholarship by selecting cases based on either most similar or most different systems design. However, this study is not intended to produce generalizable or representative findings because we recognize that highly particularistic sociotechnical and geopolitical factors influence how different states approach privacy and data governance. Instead, we seek to problematize the conceptual distinction between digital protectionism and sovereignty through a critical analysis of states with significant IT industries and geopolitical significance that also represent somewhat varied—not necessarily *most* varied—approaches to data governance. India and South Korea have significant tech industries featuring national champions with complementary relationships with US-based tech giants. For example, India has

36. Iris Geva-May, David C. Hoffman, and Joselyn Muhleisen, "Twenty Years of Comparative Policy Analysis: A Survey of the Field and a Discussion of Topics and Methods," *Journal of Comparative Policy Analysis: Research and Practice* 20, no. 1 (2018): 18–35, https://doi.org/10.1080/13876988.2017.1405618.

attracted record-setting investments from Facebook and Google in recent years, while South Korean companies have contested US-based tech giants through regulatory action;[37] meanwhile, China is home to a complementary industry with its own tech giants. In addition to economic stature and prominent tech industries, the third and final criterion was that the state should have recently debated a specific personal data regulatory regulation to provide the study with a common unit of analysis and timeliness. These criteria led us to select South Korea, China, and India.

In terms of empirical objects, we examined one regulatory text per country. For South Korea, we examined the PIPA, which was first enacted in 2011 and amended in 2020 and 2023. For China, we examined the PIPL, which was passed in 2021. For India, we examined the DPDPA, which was first drafted in 2018 and was undergoing revision following a public consultation process during the majority of our research period. Thus, we traced how the law evolved over time across multiple versions while focusing, in particular, on the final text that passed in 2023.

We operationalized our methodology in four evaluative steps. First, we studied the text of each regulation and consulted secondary legal and policy analyses to identify key components, including institutions, terms, processes, and notable clauses. Second, we compared these components across the three regulations and inductively identified themes that captured the primary dimensions of difference. We iterated this process until we reached a consensus on four primary themes. Third, we consulted secondary sources to evaluate the GDPR for each dimension of difference. Finally, we mobilized our theoretical framework to evaluate the extent to which concepts such as "protectionism" and "sovereignty" apply to each regulation in its sociotechnical and geopolitical context. We conducted this analysis by not only considering the key

37. Manish Singh, "Google Invests $4.5 Billion in India's Reliance Jio Platforms," *TechCrunch*, July 15, 2020, https://social.techcrunch.com/2020/07/15/google-invests-4-5-billion-in-indias-reliance-jio-platforms/; Steven Borowiec, "In South Korea, Big Tech's Power Struggle with Regulators Is Way Ahead of the U.S.," *Rest of World*, December 13, 2021, https://restofworld.org/2021/in-south-korea-big-techs-power-struggle-with-regulators-is-way-ahead-of-the-u-s/; Sang Kim, "Netflix and SK Broadband Battle over Who Pays in South Korea," *The Diplomat*, August 6, 2021, https://thediplomat.com/2021/08/netflix-and-sk-broadband-battle-over-who-pays-in-south-korea/.

actors and outputs of the policymaking process in each country but also examining the interests, values, normative assumptions, and silences.[38]

Three Data Protection Regulations in Asia

In this section, we situate each regulation within the particular sociotechnical and geopolitical context in which it has emerged, paying particular attention to the primary motivations behind the regulation, the institutions implicated, and the economic and territorial scope.

South Korea's PIPA

Background

The PIPA is South Korea's main data protection framework that covers both the public and private sectors. It was first enacted in 2011 to unify different standards of collection, usage, and processing of personal information previously housed in individual laws.[39] The PIPA governs the processing, usage, collection, and disclosure of personal information by data handlers, including individuals, governmental entities, and private entities. Article 2.1(a) defines personal information as identifiable information such as an individual's full name, resident registration number, and image and information that "may be easily combined with other information to identify a particular individual," where "the ease of combination" is determined by "the time, cost, technology, etc. used to identify the individual," as cited in Article 2.1(b). Duties related to protecting personal information are performed by the Personal Information Protection Commission (PIPC), which is under the prime minister's office but acts as an independent body.[40] The PIPC's main duties include developing personal information protection regulations, executing systems related to personal

38. Fischer et al., "Introduction to Critical Policy Studies," 1; Carol Bacchi, *Analysing Policy: What's the Problem Represented to Be?* (Frenchs Forest: Pearson, 2009).

39. Kim Sang-gwang, 개인정보보호 2.0 시대의 개막 "개인정보보호법 제정·공포" [The Start of Personal Information Privacy 2.0 Era through PIPA Proclamation], (statement by Ministry of the Interior and Safety, 2011), https://mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=28090.

40. Personal Information Protection Commission, "Background" (agency website, accessed August 6, 2022), https://www.pipc.go.kr/cmt/english/introduction/background.do.

information protection, investigating privacy rights infringements, and overseeing complaints and disputes. Other regulatory bodies that are involved with protecting personal information in South Korea include the Korea Internet & Security Agency (KISA), an organization that helps governmental agencies respond to data breaches and set standards for developing standards and partnerships to strengthen cybersecurity, and the Korea Communications Commission, which focuses on ensuring that broadcasting services and communications businesses comply with personal information laws.[41]

Amendments to the PIPA

In 2020, the PIPA was amended by South Korea's National Assembly. The new amendments were introduced to ensure that the law covered new types of data, such as artificial intelligence, cloud computing, and the Internet of Things.[42] Additionally, the PIPA was amended to ensure that it would offer levels of protection on par with the GDPR that would not only facilitate data exchange between South Korea and the EU but also help Korean businesses avoid the hefty fines associated with breaching the GDPR. Ultimately, in December 2021, South Korea and the European Union announced an adequacy decision that would allow Korean companies to transfer the personal information of EU citizens to South Korea without additional certification. Negotiations had previously been paused twice after official announcements were initially made to engage in an adequacy engagement in 2017 because South Korea lacked an independent body to oversee the PIPA. As a result, the South Korean government created the PIPC,[43] composed of nine commissioners, two of whom are the Chairperson and Vice Chairperson. Three of the other commissioners are appointed directly by the president and require extensive experience as a public official, such as former experience in the legal field or specialization

41. Korea Internet & Security Agency, 소개 [Introducing KISA], (agency website, accessed August 6, 2022), https://www.kisa.or.kr/605; Korea Communications Commission, "Overview" (agency website, accessed August 6, 2022), https://www.kcc.go.kr/user.do?page=E010 10100&dc=E01010100.

42. Korean Law Information Center, 개인정보 보호법 [Personal Information Protection Act], (agency website, 2022), https://www.law.go.kr/LSW/lsRvsRsnListP.do?chrClsCd=010102&lsId =011357.

43. Min-kwon Kil, 한국 개인정보보호법, EU GDPR과 동등한 수준으로 인정 [Korea Personal Information Protection Act recognized as equivalent to EU GDPR]. 데일리시큐, December 21, 2021, https://www.dailysecu.com/news/articleView.html?idxno=132787.

in personal information through experience at relevant public institutions, as cited in Article 7-2. South Korea was also required to add additional standards that require data importers in South Korea to inform EU individuals on how their data are processed and require that data is given equal protection when transferred to another country. As a result, Korean companies operating in the EU no longer have to risk penalties (up to 4% of global earnings) related to GDPR violations. Consequently, South Korea now has the same rights as EU member countries in terms of cross-border personal information transfer. Further, compared with the EU's adequacy decision with Japan, which is limited to the transfer of civilian personal information, the EU's adequacy decision with South Korea also includes the transfer of data from public institutions to facilitate cooperation on a governmental level.[44]

The amended version of the PIPA also introduced the concept of pseudonymous information, which cannot be used to identify an individual without additional information. Although pseudonymous information is a form of personal information, handlers are not required to obtain the data subject's consent when processing pseudonymized information for purposes such as statistical compilation, scientific research, and record preservation for the public interest. In January 2021, additional amendments were proposed for public comment. One area of the proposed update concerns providing additional rights to data subjects, such as the right to data portability and the right to be excluded from automated decision-making.

On September 15, 2023, further amendments came into effect that brought about changes across four domains. First, the law was restructured to prioritize the provision of more "practical" protections to subjects. These exceptions include instances such as emergency rescue operations during public health crises such as COVID-19 or MERS,[45] which South Korea experienced in 2015.[46] An illustrative case prompting this modification occurred in September 2021, involving a rental car company withholding a criminal's address information during an imminent threat of

44. Ibid.

45. Personal Information Protection Commission, "Privacy Commissioner's Press Release," https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9145.

46. World Health Organization, "MERS Outbreak in the Republic of Korea, 2015," https://www.who.int/westernpacific/emergencies/2015-mers-outbreak.

child sexual abuse investigation.[47] Second, the revised legislation sought to harmonize standards for processing personal information in both the online and offline realms. The second change pertained to the regulation of emerging technologies, permitting drones and autonomous vehicles to film for business purposes unless expressly refused by the data subject.[48] Third, heightened measures were instituted to ensure the secure handling of personal information within the public sector, including the analysis and inspection of records, designation of managers for public systems, and notifying the public system of any unauthorized access to the public system. Finally, the amendments addressed the global landscape of privacy regulation by diversifying requirements for the overseas transfer of personal information, aligning them with "global standards."[49]

China's PIPL

The PIPL is China's first comprehensive legal framework that regulates and protects rights and interests related to personal information. The PIPL was first introduced as a bill in October 2020 by the thirteenth Standing Committee of the National People's Congress. After two rounds of public consultation in November 2020 and May 2021, the PIPL was quickly passed in August 2021 and became effective in November 2021.

When introducing the bill to the National People's Congress, the Deputy Director of the Commission of Legislative Affairs outlined that the goals of the PIPL are to strengthen the legal protection of personal information, maintain a healthy cyberspace ecosystem, and promote the healthy development of the digital economy. He highlighted the issues of excessive and arbitrary data collection and use, illegal data acquisition, and selling for commercial gains by corporations, institutions, and individuals in the digital age, which disrupts the everyday lives of citizens and harms their well-being and financial security. He stressed that with China's rapid digital innovations and developments and the growing user base, this bill was responding to the "objective" and "realistic" societal and individual needs of personal information protection.[50]

47. Personal Information Protection Commission, "Privacy Commissioner's Press Release."

48. Ibid.

49. Ibid.

50. Xia Hongzhen, 关于《中华人民共和国个人信息保护法（草案）》的说明 [Explanation on the Personal Information Protection Law of the People's Republic of China (Draft)]

The PIPL is China's third major legislation that specifically regulates digital data and privacy, along with the Cybersecurity Law and Data Security Law. Together, these three laws form a coherent and comprehensive legislative framework that is meant to safeguard China's data protection and cybersecurity. The Chinese Cybersecurity Law (CSL), which became effective in 2017, operates under the general principles of safeguarding cybersecurity, ensuring cyber sovereignty and national security, and protecting China's social and public interests of citizens, legal persons, and organizations. It established general security provisions for network operators and introduced the concept of a "critical information infrastructure operator" (CIIO), which is subject to additional regulations. The concept of CIIO covers public service sectors such as communications, transportation, energy, and networks that contain data and information that can severely endanger national security if leaked or damaged. The Data Security Law (DSL), which became effective in September 2021, builds on the CSL and provides a specific legal framework for data collection, processing, storage, and transfer based on national security impact. It categorizes data based on their impact on national security and establishes the relevant requirements, obligations, and legal liabilities of network operators. Thus, the PIPL complements the CSL and DSL by focusing on data protection at the individual level as opposed to cybersecurity and national security. The PIPL will be coordinated and implemented by the Cyberspace Administration of China (CAC) and supported by the country-level or higher municipal governments. Established in 2011, the CAC primarily functions as a strategic hub of internet security, internet economy promotion, and the main cyberspace regulator of China.[51]

While the PIPL is modeled after the GDPR and, therefore, has many overlapping features, it is perceived to be one of the most stringent personal data protection frameworks in the world.[52] The purpose of the PIPL is to "protect personal information rights and interests, standardize personal information handling activities, and promote the rational

(statement to National People's Congress of China, 2021), http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml.

51. Lilin Kang, 国家互联网信息办公室就办公室设立及其职责答问 [The Establishment of Cyberspace Administration of China and Q&A]. *Xinhua News Agency*, May 5, 2011, http://www.gov.cn/jrzg/2011-05/05/content_1858131.htm.

52. Catherine Zhu, "Is China's New Personal Information Privacy Law the New GDPR?" *Bloomberg Law*, September 17, 2021, https://news.bloomberglaw.com/privacy-and-data-security/is-chinas-new-personal-information-privacy-law-the-new-gdpr.

use of personal information." It is worth highlighting that, as opposed to the GDPR and its legal foundation in the right to privacy articulated in the European Convention on Human Rights, the PIPL prioritizes the need to safeguard personal information interests for the "rational use of personal information" in the digital economy. This echoes the government's prioritization of big data in its national strategy to grow the digital economy and develop a healthy cyber ecosystem. Therefore, one primary purpose of the PIPL is to specifically regulate the increasing abuse of personal information by both international and domestic tech companies because data are deeply incorporated into every aspect of Chinese citizens' lives. Therefore, it establishes regulations for automated decision-making, such as discriminatory pricing, user profiling, and algorithmic recommendations, and features one of the highest penalties—5% of annual global revenue—and corresponding penalties for individuals and businesses. For instance, Didi, China's leading ride-sharing app, was one of the first major platforms to be penalized for breaching the PIPL, along with CSL and DSL, for its illegal use and processing of user data, such as biometric and location data, without consent.[53]

While national and economic security has been a key consideration of China's establishment of the PIPL, China has also recognized the importance of international data flows in growing its sustainable digital and tech sector, especially given the country's economic strains. Thus, in September 2023, the CAC has proposed and consulted on draft provisions to promote cross-border data flow, which will ease certain requirements set out by the PIPL if passed.

India's DPDPA

Background

The DPDPA was initially borne out of a landmark Supreme Court ruling that established a constitutional right to privacy, *Justice K. S. Puttaswamy (Ret'd) v. Union of India* (hereafter, *Puttaswamy*), began in 2012 when Justice K.S. Puttaswamy petitioned against linking state benefits to a

53. J. Lv, 国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问 [Cyberspace Administration of China's Statement and Q&A on Didi's investigation], (statement by Cyberspace Administration of China, 2022), http://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm.

mandatory universal identification card called Aadhaar.[54] In a unanimous ruling, the court held that privacy is a constitutionally protected right. This ruling has significant implications for many issues in Indian society. For example, it contributed to the legal basis for a 2018 landmark ruling that decriminalized consensual sex between people of the same sex, which had previously been outlawed under Section 377. In addition, during the *Puttaswamy* ruling, the government created an expert committee led by Justice B. N. Srikrishna to make recommendations for data protection legislation. The committee submitted its report and a draft bill to the Ministry of Electronics and Information Technology (MeitY) in 2018, which then introduced a draft bill—the first version of the DPDPA—to Parliament in 2019.

Since then, the bill that eventually became the DPDPA has evolved considerably. The 2019 bill was immediately passed on to an ad hoc Joint Parliamentary Committee (JPC) to review the text. The JPC initiated a public consultation process that resulted in 234 memorandum submissions, seventy-eight committee meetings, and multiple briefings with MeitY and other agencies, regulators, and private data and cybersecurity experts.[55] In December 2021, the JPC submitted its long-awaited report and draft bill to Parliament, which featured eighty-one amendments and twelve recommendations to develop a comprehensive legal framework for data protection. Notably, the draft bill significantly expanded the scope to include regulating non-personal data—a unique feature among data protection regulations worldwide; hence, one amendment was to rename the bill "Data Protection Bill," striking the word "Personal" from the title. Once the JPC's report and the draft bill were submitted in December 2021, the bill was returned to MeitY, which was expected to revise the bill for consideration by Parliament. However, on August 3, 2022, MeitY made a surprising decision to withdraw the bill from Parliament. According to MeitY's minister, the bill was withdrawn from Parliament in order to redraft a "comprehensive legal framework."[56] In November 2022, MeitY released a new

54. *K. S. Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012 (Sup. Ct. India August 24, 2017).

55. Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, "Report on the Joint Committee on the Personal Data Protection Bill, 2019." (Committee Report, 2021), https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

56. ET Bureau, "Government Withdraws Data Protection Bill," *The Economic Times*, August 4, 2022, https://economictimes.indiatimes.com/news/india/government-pulls-out-data-protection-bill/articleshow/93324823.cms.

bill, the Digital Personal Data Protection Bill, for public consultation, which was then further revised and ultimately passed in August 2023 as the DPDPA.[57]

Evolution of the DPDPA

This section focuses on the evolution of the DPDPA across four iterations as responsibility was transferred from the Srikrishna Committee in 2017 to 2018 ("Srikrishna Report") to MeitY in 2018 to 2019 ("2019 Bill"), to the JPC in 2019 to 2021 ("JPC report" and "draft DPB"), and ultimately to the DPDPA.[58] In general, the Srikrishna Report articulated a personal data protection framework modeled after the GDPR, but successive bills have increasingly diverged from it. One key difference is that the motivations cited in government documents regarding the DPDPA generally focus on growing the digital economy rather than on the individual right to privacy.

Each iteration of the DPDPA recommends establishing a data protection authority or board to oversee its implementation and enforcement, but its evolving composition and jurisdiction have attracted critical attention. The Srikrishna Report recommended that the authority be appointed by the central government on the recommendation of a selection committee that would consist of representatives from the judicial and executive branches and a private expert. It stressed that the appointment process should be fair and transparent "because it is expected that government agencies will be regulated as data fiduciaries under the data protection law."[59] However, the 2019 bill granted the executive branch exclusive control over the board by appointing the Cabinet Secretary as chair and selecting the other members. The draft DPB reinforced the executive branch's authority, although it also expanded the committee to include private experts. The enacted DPDPA ultimately retained the Center's control over the board and upheld its authority to initiate inquiries, investigate complaints, and resolve disputes, but curtailed its ability to issue directives or regulations.

57. Neha Madan, Vinod Joseph, Udit Mendiratta, Jitendra Soni, Shivkrit Rai, Rohan Aneja, and Shravya Karanth, "The Digital Personal Data Protection Bill, 2022—An Analysis," *Lexology*, April 12, 2023, https://www.lexology.com/library/detail.aspx?g=22006942-bb22-4be8-98c4-f4b5ef2186b4.

58. The Digital Personal Data Protection Bill, 2022, is excluded from this analysis because it was released after submission.

59. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (Parliamentary Report, 2018: 153), https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

Critical Comparative Policy Analysis

This section compares South Korea's PIPA, China's PIPL, and India's DPDPA in terms of four key themes: conceptualizations of personal and sensitive information, CBDT restrictions, state exceptions for data access, and considerations for platforms.

Conceptualizations of Personal Information

Each country defines personal information with different degrees of specificity. China's PIPL is the broadest in scope, covering any type of information found online and offline that may identify an individual. Article 4 of the PIPL defines personal information as "all kinds of information, recorded by electronic or other means, related to [an] identified or identifiable natural person." Meanwhile, South Korea's PIPA provides the most specific examples of "personal information," including an individual's full name, resident registration number, and image. Finally, India's DPDA does not identify any examples; instead, it defines "personal data" broadly in section 2(t) as "any data about an individual who is identifiable by or in relation to such data."

Both China's PIPL and South Korea's PIPA exclude anonymized information from their scope. Article 4 of China's PIPL defines anonymization as "the process of personal information undergoing handling to make it impossible to distinguish specific natural persons and impossible to restore." Meanwhile, in South Korea, anonymized information refers to any information that cannot identify an individual, even when combined with other information. In India's case, the question of including anonymized data in the DPDPA was contested in prior versions but was ultimately excluded from the final text, which only applies to personal data.

China's PIPL and South Korea's PIPA also specify exceptions to the collection of personal information. For example, both laws identify exceptions for data collected by visual data processing equipment installed in public spaces, as stated in PIPL Article 26 and PIPA Article 58(2). South Korea's PIPA further specifies a category of *pseudonymized* information as a type of personal information that is exempt from obtaining the data subject's consent when used for specific purposes such as "statistical purposes, scientific research purposes, and archiving purposes in the public interest" in Article 28-2. India's DPDPA allows exceptions for various actors and uses similar to South Korea's PIPA: Section 17(2)(a) generally exempts the

central government, and Section 17(2)(b) exempts processing personal data for "research, archiving, or statistical purposes."

The three countries' approaches to *sensitive* personal information vary widely. While both South Korea's and China's regulations' interpretations of sensitive information include religious belief and health-related data, only South Korea enumerates specific types of demographic information such as sex life and political belief and affiliation. In contrast, China's definition of sensitive personal information contains fewer demographic identifiers but includes location-tracking information, personal information of minors under fourteen years of age, and biometric data. Finally, India's DPDPA departs from the other laws by not distinguishing between categories of personal data. While prior versions of the DPDA enumerated specific categories of sensitive data, such as financial, health, biometric, religious, and political data, as well as sexual orientation and transgender status, these are omitted in the final text. Instead, Section 10(1)(a) indicates that certain liable organizations may be subject to heightened requirements based on "the volume and sensitivity of personal data processed" while leaving sensitivity open for the central government to define.

CBDT Restrictions

The three data protection regulations vary with respect to their territorial jurisdiction. China's PIPL stipulates that data protection rules apply not only to businesses within China but also to products and services targeting citizens that are based outside the country. Cross-border transfer of personal data must meet one of four requirements for security assessment: personal information protection certification, a CAC-approved contract with a foreign receiver, or other obligations and regulations set out by the State Cybersecurity and Informatization Department according to PIPL Article 38. In addition, the PIPL has a strong data localization component where CIIO or personal information handlers that handle personal data over a certain threshold, which is undefined in the legislation, must store data within the borders of the country according to Article 40. The key motivations for the stringent territorial restrictions stem from the government's recognition of data as a vital national asset and China's concern about data security risks, given the scale of its data resources.[60] However, a key challenge that

60. Huang Peng, 专家解读｜防范数据出境安全风险保护国家数据安全 [Expert interpretation|Preventing Data Export Security Risks, Protecting National Data Security], (Statement by

China has to navigate is striking the right balance between its national security objectives and its goal of encouraging business and innovation, as we can see from its draft proposals to scale back certain cross-border data flow requirements in the PIPL.

However, in South Korea, the territorial scope of the PIPA is not specified. While large-scale internet communications service providers (ICSP) and third parties that receive personal information from ICSPs established within the country must abide by the law, the law does not specify whether foreign companies targeting users in South Korea are included in the scope. The definition of "large" includes criteria such as global sales that exceed ₩1 trillion (approximately $775 million) and a user base exceeding one million users.[61] According to PIPA Article 31-2, foreign companies that do not have an address or business office in Korea must designate a local agent in South Korea who can act on their behalf. When information is to be transferred abroad (Article 28-8), businesses must notify users about the type of information that will be transferred, the country to which the information will be transferred (including the date and method of transfer), the name of the business entity, and the purpose of the transfer. These rules, however, are not applied when "cross-border transfer is necessary to implement a pact or other international arrangements," as stipulated in PIPA Article 18-2.

Similarly, there is generally no data localization requirement in India's DPDPA, although the central government may restrict specific jurisdictions in the future. This represents a dilution of the data localization provisions in earlier drafts of the law: the first draft (Personal Data Protection Bill, 2018) required a copy of all personal data to be stored within India, while the next draft (Digital Personal Data Protection Bill, 2021) permitted data transfer only to certain whitelisted jurisdictions.[62] In contrast, the DPDPA permits

---

Cyberspace Administration of China, 2022), http://www.cac.gov.cn/2022-07/08/c_1658903426889066.htm.

61. Iris Hyejin Hwang and Hye In Lee, "Data protection Laws and Regulations Korea 2022," *International Comparative Legal Guides* (blog), August 7, 2022, https://iclg.com/practice-areas/data-protection-laws-and-regulations/korea.

62. The Srikrishna Report emphatically asserted the logic of data localization: "The vision of several national internets entirely walled to the outside world is currently a caricatured characterisation that evokes fear of changing the status quo . . . Acting on a nostalgic understanding of what the internet was like when it started to defer a mandate to store and process personal data locally will be myopic. There is no principled or practical reason to believe that the very fact of local storage or restriction to local processing itself will make the digital economy any less free or fair." Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair

data transfer outside India to countries other than those blacklisted by the central government. Despite these differences across the life of the DPDPA, each version asserted the value of supporting domestic economic growth, with the final version leaving open the opportunity for sectoral regulation.

State Exceptions for Data Access

National and public security is a top concern that is generally approached as an exception to the domain of data governance. For example, the GDPR's Article 23 makes exceptions to Union or Member State laws that conflict with the GDPR. However, there are important limitations. For example, in Schrems I and II, the Court of Justice of the EU (CJEU) ruled that the US's data access practices under the name of national security violated the safe harbor guarantee provided by Privacy Shield. Therefore, examining the specific enumerated national security exceptions can be instructive.

In Article 13 of China's PIPL, processing data without the data subject's consent is enumerated as an exception "to protect the life, health, and property of natural persons in emergency situations" or public interests. Furthermore, there is a strong emphasis on the exception of public health incidents and journalism and public opinion supervision "within a reasonable scope," although the scope and threshold for "reasonable" is undefined. This arguably grants data processors, state agencies, and local municipal governments more regulatory power, especially given China's strict COVID policies. This emphasis on public health has been crucial in implementing China's COVID-related restrictions and protocols, which include sharing patients' anonymized travel histories. PIPL Article 34 also contains a new attempt to provide guidelines for state organizations to purposefully and rightfully handle personal information.

Meanwhile, in South Korea's PIPA, exceptions have been made for job performance at public institutions and special restrictions on visual data in public. This is closer to the GDPR, which specifies in Article 23 restricting the obligations related to processing personal information if it is important to safeguard the "rights and freedoms" needed in a democratic society. PIPA Article 18 specifies that personal information may be used "beyond the scope" stipulated in Article 15 (Collection and Use of Personal Information), which requires the controller to obtain consent from data subjects in several cases.

Digital Economy: Protecting Privacy, Empowering Indians" (Parliamentary Report, 2018: 95), https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

These include cases where personal information is required by the government to perform an international treaty or convention with a foreign government and for the administration of punishment for criminal activity, as cited in Article 18(2). The processing of visual data processing devices in public spaces is also specified as an exception to personal data processing regulations when the processing is for investigating criminal activity, is necessary for ensuring the safety of the facility, or is required for regulating traffic, as cited in Article 25(1). These exceptions are similar to those found in GDPR Article 23, which permits member states to restrict the application of GDPR obligations for, among other reasons, national and public security or investigating criminal offenses. Thus, both laws state that interests related to national security and public interests (i.e., related to criminal activity) are exempt from the PIPA. A unique exception includes personal information used to assess job performance at public institutions, presumably to curb governmental corruption. The PIPA also prohibits the installation of visual processing devices in bathrooms, saunas, and changing rooms, which may be closely tied to the ongoing surge in illegal filming since 2015, such as the proliferation of online spycam videos that mostly involved women being filmed in restrooms, offices, and on the subway in South Korea.[63]

In India's DPDPA, the broad authority of the central government and data protection agency is especially evident in its ability to modify the regulation in response to suspected incitement against the state. Each draft of the DPDPA has granted increasing power to exempt government agencies. The Srikrishna Report explicitly asserted that the bill should not distinguish between government and private entities because a citizen's right to privacy is fundamental. Earlier versions of the bill drew from the original *Puttaswamy* ruling to recommend permitting government exemptions that are "necessary and proportionate" only in narrow circumstances when there is a legitimate state interest (e.g., national security and violations of law). However, over its life, the DPDPA was modified to eventually embrace a broad exemption for the central government for a range of reasons, including maintaining public order, preventing incitement, and upholding national security—the same rationales that are used to justify other exceptional acts of technology policy, such as internet shutdowns.[64]

63. Birru Dereje Teshome, "Spy Camera Epidemic in Korea: A Situational Analysis," *Asian Journal of Sociological Research* 2 (2019): 1–13, https://globalpresshub.com/index.php/AJSR/article/view/782/727.

64. R. Grover, "Contingent Connectivity: Internet Shutdowns and the Infrastructural Precarity of Digital Citizenship," *New Media & Society* (2023), https://doi.org/10.1177/14614448231176552.

Considerations for Platforms and Businesses

South Korea, China, and India have adopted unique designations for platforms and businesses in their personal data regulations. While the GDPR has generally referred to platforms and businesses as controllers and processors, China has a specific data localization rule for CIIO, defined by the CAC based on sector, user base, and revenue. Major platform companies such as Didi and Tencent qualify as CIIOs because of their size and deep integration into the Chinese digital infrastructure. Thus, platform companies in China that are supported by the global financial system must be mindful of their global operations because listing as a public company abroad is often accompanied by data disclosure requirements that may conflict with CBDT restrictions and data localization requirements. Ant Financial, Alibaba's fintech subsidiary, and Didi both faced regulatory scrutiny from financial and cyberspace regulators due to these concerns.[65]

However, the focus on internet platforms is not restricted to protecting national and public interests; it is also closely related to China's commitment to fostering a healthy digital economy and empowering digital users, given the growing conflict between users and platforms. For example, PIPL Article 24 establishes restrictions on automated decision-making in commercial activities and explicitly bans platforms from offering differential pricing and treatment of users using their personal data. It also requires platforms to provide users with an "easily accessible" opt-out option for commercial marketing. Overall, these rules contribute to the PIPL's goal of establishing checks and balances on digital monopolies in China to maintain a competitive digital landscape while accounting for the national security risks the 'borderless' global digital economy could pose.

In India's case, the DPDPA allows the central government to identify two exceptional categories of companies. First, it invites the central government to exempt categories of liable companies. Specifically, Section 17(3) specifically enumerates "startups" as a category of companies that may be exempt from some or all compliance requirements. Second,

65. Jasper Jolly, "Ant Group Forced to Suspend Biggest Share Offering in History," *The Guardian*, November 3, 2020, https://www.theguardian.com/business/2020/nov/03/biggest-share-offering-in-history-on-hold-as-ant-group-suspends-launch; Ryan McMorrow, Sun Yu, and Tom Mitchell. "China's Didi to delist from New York and switch to Hong Kong," *Financial Times*, December 3, 2021, https://www.ft.com/content/c30cf911-51da-4b40-a969-161351de6f04.

Section 10(1) also empowers the central government to single out specific companies or categories of companies as "significant data fiduciaries" (roughly equivalent to "data controllers" under the GDPR). The criteria for identifying significant data fiduciaries are not fixed but may include the volume and sensitivity of personal data processed, risk to users' rights, potential impact on the sovereignty and integrity of India, risk to electoral democracy, security of the state, and public order. In prior draft bills, this category was called "social media intermediaries" or "social media platforms," alluding to both the type of companies that may be targeted as significant data fiduciaries and the ways in which the DPDPA has evolved to expand the central government's power to subject specific companies to higher scrutiny.

Finally, while South Korea's PIPA does not directly emphasize tech platforms, there have been related efforts to regulate online platforms and address their implications. The PIPA features a chapter on governing ICSPs, an area previously governed by the Act on Promotion of Information and Communication Network Utilization and Information Protection, which is likely to extend personal information regulations to online platforms. Article 37-2, concerning the rights of data subjects in the context of automated decision-making, is anticipated to have a specific impact on prominent search engines and e-commerce platforms operating in South Korea. This prediction is based on the understanding that these platforms extensively employ artificial intelligence for content or product promotion. Additionally, it is expected to extend its influence over generative AI and cloud services, particularly in safeguarding artists' copyrighted materials.[66]

Discussion

This article explored how sociotechnical and geopolitical contexts and imaginaries animate different approaches to data governance—and how our findings can help navigate the debate between digital protectionism and sovereignty. We conducted a comparative analysis of recent debates about data protection regulations in South Korea, China, and India,

66. H. Kim, "이커머스 추천도 개인정보보호법 위반?" . . . 자동화 결정 대응법 '논란' ["Do E-commerce Recommendations Violate Privacy Laws?" . . . The Automated Decision Response Act Controversy], https://www.edaily.co.kr/news/read?newsId=03463686638760672&mediaCodeNo=257.

focusing in particular on key differences along four dimensions: conceptualizations of personal data, restrictions on CBDT, state exemptions for data access, and considerations for platforms and other businesses. This analysis led to three conclusions regarding the notion of privacy, the differential role of platforms in different national concepts, and the relevance of different citizen–state dynamics.

First, the comparative analysis demonstrates that local notions of privacy are animated by complex domestic issues and geopolitical anxieties in addition to responding to the GDPR. This complicates presumptions about a straightforward process of policy diffusion or transfer from the GDPR to other states. For example, on the surface, it may seem like South Korea's amendments to the PIPA represent an instance of policy diffusion because they bring the PIPA closer in line with the GDPR. However, our analysis demonstrates that the amendments also represent South Korea's attempt to maintain relevance on the global stage by, for instance, allowing the use of pseudonymized personal information for research and science. This has, therefore, led the state to capitalize on digital trade by imposing "non-tariff barriers" to digital trade in the form of localization requirements, CBDT restrictions, and restrictions on certain payment systems. These efforts can be read as attempts to regulate South Korea's own corporate entities abroad and therefore an attempt to promote—rather than impede—a global internet by building a common understanding of privacy. Such decisions, therefore, illustrate how data protection regulations can not only resemble policy diffusion in effect but also reflect alternative goals in intent.

Similarly, we find that analyzing conceptualizations of privacy in a state must be evaluated in relation to its local sociotechnical context, not only in comparison to US or EU standards. This can be seen in cases such as South Korea's prohibition of visual processing devices because of concerns about illegal filming, as discussed earlier. Furthermore, a closer examination of how data protection is operationalized reveals a blurred boundary between promoting surveillance and promoting individual privacy. For example, a recent data breach in China reveals how the focus on expanding privacy rights by protecting data under the oversight of a single government can expose individuals to a heightened risk of surveillance.[67]

67. Karen Hao, "China Has a Problem with Data Leaks. One Reason Is Its Surveillance State," *The Wall Street Journal*, July 21, 2022, https://www.wsj.com/articles/china-has-a-problem-with-data-leaks-one-reason-is-its-surveillance-state-11658410752.

Second, data protection regulations represent a vehicle for platform governance. We found different approaches to regulating tech platforms in these regulations, ranging from the open-ended definition of "significant data fiduciaries" in India to a more precise designation of "critical information infrastructure operators" in China. This range reflects different relationships with technology companies—especially geopolitical anxieties about US-based platforms and related to domestic industries—which complicates the assumption that digital protectionism primarily reflects intentions related to international data mobility.[68] This perspective either obfuscates or completely omits the complicated dynamics of contestation between governments and *local* digital platforms. For instance, in China's example, the personal privacy legal framework specifically targets local firms, and India's DPDPA similarly seeks to stabilize state control over large platforms. This calls attention to the issue of positionality when unpacking digital protectionism; for example, in these three countries, local digital platforms such as Naver, Bytedance, and Didi are not simply beneficiaries but also subjects of regulation. This demonstrates how personal data regulations are increasingly employed as a tool for platform governance at both national and international levels.[69] For instance, the 2023 debate about domesticating TikTok in the US is justified on the grounds of data privacy concerns, demonstrating how protectionism is both animated and complicated by multifaceted relationships between states and increasingly powerful platforms.

Third, conceptualizations of data and privacy reflect different relationships between citizens and states. These varied relationships are not fully captured by the framework of digital protectionism, which focuses on international political economy. Our analysis reveals how states broker their relationships with both local and global platforms and people—especially their own citizens. We find this not only in the common narrative that the state is protecting its citizens' data and privacy through data localization requirements but also in how states use regulatory strategies to enhance law enforcement efforts, pursue a national security agenda, and discipline its citizens in general. Thus, data protectionism is an insufficient

68. Altug Yalcintas and Naseraddin Alizadeh, "Digital Protectionism and National Planning in the Age of the Internet: The Case of Iran," *Journal of Institutional Economics* 16, no. 4 (2020): 519–36, 520, https://doi.org/10.1017/S1744137420000077.

69. Terry Flew, *Regulating Platforms* (Cambridge: Polity Press, 2021).

analytical tool for understanding how data protection regulations modulate citizens' experiences. In our comparative analysis, we found that each state's characterization falls along a spectrum between a commodity and a personal asset covered by a fundamental right to privacy. These varied approaches reflect different sociocultural norms and citizen–state relations. In particular, these different conceptualizations are best highlighted and reinforced by comparing what is *out* of the scope of each regulation and where the state can make exceptions. We can also see how personal data are embedded in different political-legal frameworks. For instance, in China, while there are two major laws on cybersecurity and data security, personal data have emerged as a separate issue based on an understanding of data being both public and private. Meanwhile, in South Korea, personal data governance is an important conversation about ensuring economic growth for corporations while protecting private citizens' interests.

Collectively, our conclusions reveal divergent sociotechnical relations mediated through personal data governance frameworks in South Korea, China, and India. Our findings suggest that there are real, substantial distinctions in how each state foresees data protection related to its relationship with both regional and global geopolitics, platform companies, and its own citizens. These relations are often in flux and thus inherently unstable, especially given the complexity of networks broader than what we could discuss herein, including social movements, corporations, and others, including those beyond national borders.[70] In the case of Asia, this includes regional formations such as the Association of Southeast Asian Nations (ASEAN) and the South Asian Association for Regional Cooperation (SAARC), in addition to larger supranational entities. Thus, it is important to investigate alternative empirical sites, interactions across actors and implementation processes, and institutional intermediaries in order to further refine sociotechnical relations mediated through data governance.

Conclusion

This comparative study analyzed personal data protection regulations across three Asian states with significant IT industries. We analyzed South Korea's PIPA, China's PIPL, and India's DPDPA through four key dimensions: conceptualizations of "personal data," cross-border data transfers, state

70. Jasanoff, "Future Imperfect," 4 and 22.

exemptions for data access, and considerations for platforms and other businesses. This comparison led to conclusions about the complex interactions between data governance and notions of privacy, platform governance, and citizen–state relations. Together, these findings suggest that examining sociotechnical and geopolitical contexts can provide a more nuanced understanding of how states, platform companies, and individuals interact with each other and constitute sociotechnical imaginations that manifest in personal data regulations.

This analysis demonstrates how a contextualized approach contributes to confirming that discourses that collapse data protection approaches to protectionism or sovereignty are better understood as rhetorical strategies rather than specific policy positions.[71] In addition, they are not only descriptive terms but also political evaluations of data governance strategies that operationalize different conceptualizations of privacy and personal data. Therefore, it is important to evaluate the empirical details of specific regulations in order to clarify the extent to which these evaluative terms should apply to data protection regulations.

Such an exploration would allow us to answer future questions such as: to what extent are these characterizations of personal data protection regulations accurate and fair? Or, more precisely, what specific values are being advanced and prioritized with data governance regulations that inevitably invoke privacy, protectionism, and sovereignty simultaneously? Prior research critically exploring "protectionism" and "sovereignty" often employ economic and political economy analyses, focusing on topics such as trade, innovation, and economic growth. Some of these analyses produce criticisms that apply to some states more than others; for example, states with less developed technological industries may be ill-equipped to provide the infrastructure and security necessary to support localized data storage and processing. Thus, the global prevalence of data localization policies serves as a reminder not to collapse global internet governance policies into a simple binary distinction between an open internet and a fragmented one. Instead, we must pay attention to the particular details of specific cases and contexts as well as interactions with sociotechnical and geopolitical dynamics.

71. Pohle and Thiel, "Digital Sovereignty."

ACKNOWLEDGMENTS

We are grateful to Hernan Galperin for his support and feedback early in the project. We would also like to thank the anonymous reviewers whose feedback greatly improved this article.

BIBLIOGRAPHY

Aaronson, Susan Ariel. "Data Is Different, and That's Why the World Needs a New Approach to Governing Cross-Border Data Flows." *Digital Policy, Regulation and Governance* 21, no. 5 (2019): 441–60. https://doi.org/10.1108/DPRG-03-2019-0021.

Aaronson, Susan Ariel. "What Are We Talking about When We Talk about Digital Protectionism?" *World Trade Review* 18, no. 4 (2019): 541–77. https://doi.org/10.1017/S1474745618000198.

Bacchi, Carol. *Analysing Policy: What's the Problem Represented to Be?* Frenchs Forest: Pearson, 2009.

Bennett, Colin J. "The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?" *Information Polity* 23, no. 2 (2018): 239–46. https://doi.org/10.3233/IP-180002.

Borowiec, Steven. "In South Korea, Big Tech's Power Struggle with Regulators Is Way Ahead of the U.S." *Rest of World*, December 13, 2021. https://restofworld.org/2021/in-south-korea-big-techs-power-struggle-with-regulators-is-way-ahead-of-the-u-s/.

Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press, 2020.

Business Roundtable. *Putting Data to Work: Maximizing the Value of Information in an Interconnected World*. Washington, DC: Business Roundtable, 2015. https://s3.amazonaws.com/brt.org/archive/reports/BRT%20PuttingDataToWork.pdf.

Drake, William J., Vinton G. Cerf, and Wolfgang Kleinwächter. "Internet Fragmentation: An Overview." *World Economic Forum*, 2016. https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

ET Bureau. "Government Withdraws Data Protection Bill." *The Economic Times*, August 4, 2022. https://economictimes.indiatimes.com/news/india/government-pulls-out-data-protection-bill/articleshow/93324823.cms.

Fan, Ziyang and Anil K. Gupta. "The Dangers of Digital Protectionism." *Harvard Business Review*, August 30, 2018. https://hbr.org/2018/08/the-dangers-of-digital-protectionism.

Ferracane, Martina Francesca. "Data Flows and National Security: A Conceptual Framework to Assess Restrictions on Data Flows under GATS Security Exception." *Digital Policy, Regulation and Governance* 21, no. 1 (2018): 44–70. https://doi.org/10.1108/DPRG-09-2018-0052.

Fischer, Frank, Douglas Torgerson, Anna Durnová, and Michael Orsini. "Introduction to Critical Policy Studies." In *Handbook of Critical Policy Studies*, edited by Frank Fischer, Douglas Torgerson, Anna Durnová, and Michael Orsini, 1–24. Cheltenham: Edward Elgar Publishing, 2015. https://doi.org/10.4337/9781783472352.00005.

Flew, Terry. *Regulating Platforms*. Cambridge: Polity Press, 2021.

Freude, Alvar and Trixy Freude. "Echoes of History: Understanding German Data Protection." *Newpolitik* (2016): 85–91. https://www.astrid-online.it/static/upload/freu/freude_newpolitik_german_policy_translated_10_2016-9.pdf.

General Agreement on Trade in Services. Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167, April 15, 1994. https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.

Geva-May, Iris, David C. Hoffman, and Joselyn Muhleisen. "Twenty Years of Comparative Policy Analysis: A Survey of the Field and a Discussion of Topics and Methods." *Journal of*

Comparative Policy Analysis: Research and Practice 20, no. 1 (2018): 18–35. https://doi.org/10.1080/13876988.2017.1405618.

González Fuster, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Brussels, Belgium: Spring, 2014.

Greenleaf, Graham. "Now 157 Countries: Twelve Data Privacy Laws in 2021/22." *Privacy Laws & Business*, April 7, 2022. https://www.privacylaws.com/reports-gateway/articles/int176/int176newdplaws/.

Grover, R. "Contingent Connectivity: Internet Shutdowns and the Infrastructural Precarity of Digital Citizenship." *New Media & Society* (2023). https://doi.org/10.1177/14614448231176552.

Hao, Karen. "China Has a Problem with Data Leaks. One Reason Is Its Surveillance State." *The Wall Street Journal*, July 21, 2022. https://www.wsj.com/articles/china-has-a-problem-with-data-leaks-one-reason-is-its-surveillance-state-11658410752.

Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. "The European Union General Data Protection Regulation: What It Is and What It Means." *Information & Communications Technology Law* 28, no. 1 (2019): 65–98. https://doi.org/10.1080/13600834.2019.1573501.

Jasanoff, Sheila. "Future Imperfect: Science, Technology, and the Imaginations of Modernity." In *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*, edited by Sheila Jasanoff and Sang-Hyun Kim, 1–33. Chicago: University of Chicago Press, 2015. https://doi.org/10.7208/chicago/9780226276663.003.0001.

Jolly, Jasper. "Ant Group Forced to Suspend Biggest Share Offering in History." *The Guardian*, November 3, 2020. https://www.theguardian.com/business/2020/nov/03/biggest-share-offering-in-history-on-hold-as-ant-group-suspends-launch.

Kang, Lilin. 国家互联网信息办公室就办公室设立及其职责答问 [The Establishment of Cyberspace Administration of China and Q&A]. *Xinhua News Agency*, May 5, 2011. http://www.gov.cn/jrzg/2011-05/05/content_1858131.htm.

Khasanova, Liliya and Katharin Tai. "An Authoritarian Approach to Digital Sovereignty? Russian and Chinese Data Localisation Models." *Social Science Research Network* (2023). https://doi.org/10.2139/ssrn.4527052.

Kil, Min-kwon. 한국 개인정보보호법, EU GDPR과 동등한 수준으로 인정 [Korea Personal Information Protection Act recognized as equivalent to EU GDPR]. 데일리시큐, December 21, 2021. https://www.dailysecu.com/news/articleView.html?idxno=132787.

Kim, Sang. "Netflix and SK Broadband Battle Over Who Pays in South Korea." *The Diplomat*, August 6, 2021. https://thediplomat.com/2021/08/netflix-and-sk-broadband-battle-over-who-pays-in-south-korea/.

Kim, H, "이커머스 추천도 개인정보보호법 위반?" . . . 자동화 결정 대응법 '논란' ["Do E-commerce Recommendations Violate Privacy Laws?" . . . The Automated Decision Response Act Controversy] Edaily, January 23, 2024. https://www.edaily.co.kr/news/read?newsId=03463686638760672&mediaCodeNo=257.

Madan, Neha, Vinod Joseph, Udit Mendiratta, Jitendra Soni, Shivkrit Rai, Rohan Aneja, and Shravya Karanth. "The Digital Personal Data Protection Bill, 2022 – An Analysis." *Lexology*, April 12, 2023. https://www.lexology.com/library/detail.aspx?g=22006942-bb22-4be8-98c4-f4b5ef2186b4

McMorrow, Ryan, Sun Yu, and Tom Mitchell. "China's Didi to delist from New York and switch to Hong Kong." *Financial Times*, December 3, 2021. https://www.ft.com/content/c30cf911-51da-4b40-a969-161351de6f04.

McNeil, Maureen, Michael Arribas-Ayllon, Joan Haran, Adrian Mackenzie, and Richard Tutton. "Conceptualizing Imaginaries of Science, Technology, and Society." In *The Handbook of Science and Technology Studies* (4th edn.), edited by Ulrike Felt, Rayvon Fouché, Clark A. Miller, and Laurel Smith-Doerr, 435–63. Cambridge, MA: MIT Press, 2016.

Mishra, Neha. "Data Localization Laws in a Digital World: Data Protection or Data Protectionism?" *The Public Sphere: Journal of Public Policy* 4, no. 1 (2016): 135–58. https://psj.lse.ac.uk/articles/abstract/45/.

Personal Information Protection Commission. "Privacy Commissioner's Press Release." https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9145.

Pohle, Julia, and Thorsten Thiel. "Digital Sovereignty." *Internet Policy Review* 9, no. 4 (2020). https://doi.org/10.14763/2020.4.1532.

Singh, Manish. "Google Invests $4.5 Billion in India's Reliance Jio Platforms." *TechCrunch*, July 15, 2020. https://techcrunch.com/2020/07/15/google-invests-4-5-billion-in-indias-reliance-jio-platforms/.

Taylor, Richard D. "'Data Localization': The Internet in the Balance." *Telecommunications Policy* 44, no. 8 (2020). https://doi.org/10.1016/j.telpol.2020.102003.

Teshome, Birru Dereje. "Spy Camera Epidemic in Korea: A Situational Analysis." *Asian Journal of Sociological Research* 2, no. 1 (2019): 1–13. https://globalpresshub.com/index.php/AJSR/article/view/782/727.

Yalcintas, Altug, and Naseraddin Alizadeh. "Digital Protectionism and National Planning in the Age of the Internet: The Case of Iran." *Journal of Institutional Economics* 16, no. 4 (2020): 519–36. https://doi.org/10.1017/S1744137420000077.

Zhu, Catherine. "Is China's New Personal Information Privacy Law the New GDPR?" *Bloomberg Law*, September 17, 2021. https://news.bloomberglaw.com/privacy-and-data-security/is-chinas-new-personal-information-privacy-law-the-new-gdpr.