New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance

*Luca Belli**

Abstract *This paper explores the recent data protection evolutions in three leading emerging economies, Brazil, China, and India, to identify the contours of what may become a new post-Western Model of Data Governance.*

The paper stresses that recent innovations introduced by these countries are particularly relevant for two reasons. First, the considerable geopolitical and economic weight they have at both regional and international level. In this perspective, the policy choices of these leading emerging economies are likely to be considered as models to which national and international frameworks may adapt in the future, especially in the Global South context. Second, for the pragmatic approach they adopt, to tackle the limits of dominant data protection models, using some of their strongest assets: namely, the Brazilian multistakeholder governance, the Chinese cybersecurity regulation, and the Indian technological expertise.

Importantly, the countries' approaches bring significant elements of novelty to data protection. The paper identifies the main characteristics of the three national data architectures and the elements of novelty that are likely to inspire other frameworks: the new multistakeholder advisory body for the Brazilian data protection authority, the new Chinese data security framework, and the new Data Empowerment and Protection Architecture of

* Dr Luca Belli is Professor of Internet Governance and Regulation at Fundação Getulio Vargas (FGV) Law School, where he directs the Center for Technology and Society (CTS-FGV) and the CyberBRICS project. He is also editor of the International Data Privacy Law Journal, published by Oxford University Press.

The author would like to sincerely thank a group of extremely talented research assistants from the Indian Journal of Law and Technology for their support during the elaboration of this paper. Special thanks go to Anhad Kaur Mehta, Chiranth S., Dhruv Holla, and Shubh Mittal.

India. It argues that the study of the data architectures of these countries is necessary not only to grasp how these very different giants are evolving, but also to understand the influence they will have on other countries at both regional and global levels.

The paper concludes by emphasising that, while Brazil, China, and India are not renowned for their commitment to data privacy, their approaches and their global relevance have the potential to give rise to a new "third way" in data governance, shaped by Global South leaders. Such a new approach can facilitate the emergence of a post-Western model of data governance.

Introduction

This paper explores the recent data protection evolutions in three leading emerging economies: Brazil, China, and India. Members of the BRICS grouping, projected to be amongst the largest economies in the world by 2030[1], the BIC of BRICS provide some particularly interesting examples of innovative approaches to data governance. While Brazil, China, and India

[1] Jim O'Neill, 'Building Better Global Economic BRICs' (2001) Goldman Sachs Global Economics Paper 66. <www.goldmansachs.com/our-thinking/archive/archive-pdfs/build-better-brics.pdf> accessed 10 January 2023; Dominic Wilson and Roopa Purushothaman, 'Dreaming with BRICs: The Path to 2050' (2003) Goldman Sachs Global Economic Papers 99. <www.goldmansachs.com/insights/archive/archive-pdfs/brics-dream.pdf> accessed 10 January 2023.

are not renowned for their commitment to (data) privacy[2], the recent innovations introduced by these countries are particularly relevant. Indeed, due to their considerable geopolitical and economic weight at both regional and international levels, their policy choices are likely to be considered as models to which national and international frameworks may adapt in the future.

On the one hand, Brazil, China, and India are becoming increasingly relevant technological players whose software applications, hardware, and artificial intelligence (AI) systems are gradually adopted well beyond their national borders. On the other hand, having some of the largest populations and economies in the world, these countries can afford the luxury of foreseeing an extraterritorial scope for their regulations in their data protection frameworks. Until recently, only the European Union had dared to include the "privilege" of extraterritorial reach in its data protection framework. Indeed, extraterritorial scope seems to be a path chosen primarily[3] by last-generation data regulations of large countries or regional blocks, such as the European Union, which have the bargaining power and institutional capacity necessary to afford imposing such extraterritorial reach.

In this perspective, this paper argues that the policy and institutional choices of Brazil, China and India will either act as a model for neighbours and commercial partners, or these latter countries will need to adapt to the new extraterritorial reach of national frameworks to maintain trade flows. Therefore, these countries are likely to become both regional and global leaders in data regulation, having the potential to give rise to a new "third way" in data governance. Analysing the emergence of an alternative "post-Western" option of data architecture, shaped by leading emerging economies, is particularly important for Global South countries, for which Brazil, China and India might be particularly relevant – or even essential – trade partners.

Crucially, the countries have been chosen not only because of their size and relevance but also for their substantially innovative approaches to data

---

[2] Although Brazil, China, and India have structured increasingly sophisticated data protection frameworks, their human rights track records have been declining over the past years. This regression has been emphasised by several international rankings, which may even categorise some of them as "partly free", "not free" or "authoritarian regimes". As an instance, see the Global Freedom Scores, the Internet Freedom Scores, and the Democracy Scores elaborated by annually by Freedom House: "Countries and Territories" (*Freedom House*) <https://freedomhouse.org/countries/freedom-world/scores> accessed December 31, 2022.

[3] A notable exception to this general rule is the extraterritorial scope of the data protection law of tiny Uruguay Decree No. 64/020 regulation of arts 37 to 40 of Law 19, 670 and art 12 of Law 18, 331, Referring to the Protection of Personal Data (*IMPO*) <www.impo.com.uy/bases/decretos/64-2020> accessed 25 December 2022

governance. Besides being the largest countries on Earth to shape data protection regimes, they have brought significant elements of novelty to the traditional "mainstream" data protection models, which are primarily moulded on European frameworks or on a very minimalist US approach.[4] While Brazil, China and India have indubitably been influenced by the US and European models, and by the OECD framework, I argue that the considerable elements of innovation they are introducing may compose a new breed of post-Western approaches to data governance.

Being large and complex developing countries with very recent data privacy cultures, Brazil, China, and India offer very relevant teachings for other low- and middle-income countries as they face challenges shared by the entire Global South. Conspicuously, such challenges include a very limited "data protection culture"[5], which makes it extremely difficult to comply with a European-like framework as data subjects do not know their rights, public and public entities do not know how to correctly comply and regulators themselves may face an enormous shortage of intellectual and financial resources necessary to build a data protection culture.

While taking inspiration and transplanting from leading models and framework is completely understandable, developing countries face many challenges that most developed countries are not used to dealing with. In this sense, the Brazilian, Chinese, and Indian experiences provide much more realistic illustrations of how data protection plays out in the Global South, both in terms of the problems that need to be talked about and the innovations that could be introduced to improve existing models towards a post-Western approach to data governance.

---

[4] The US approach has been characterised by a sectorial and minimalist approach to personal data regulation. Despite having been one of the first countries in the world to adopt data protection legislation aimed at the public sector, through the 1974 US Privacy Act, to date the US have not adopted a general data protection law to avoid interfering with competing – and so far, prevailing – interests, such as commerce, national security, and free speech. Alan Charles, Rauland Snezhana, Stadnik Tapia, 'United States' (2021) 8 Privacy, Data Protection and Cybersecurity Law Review 449; Shawn Marie Boyne, 'Data Protection in the United States' (2018) 66 The American Journal of Comparative Law 299.

[5] Professor Stefano Rodotà, one of the most renown data protection thinkers, defined "data protection culture" as the assimilation by society of the crucial importance of data protection. This process consists in the gradual understanding of the instrumental value that data protection plays for the realisation of citizenship and the sustainable development of economy and democracy. See Lucca Belli and Danilo Doneda , 'O Que Falta ao Brasil e à América Latina Para Uma Proteção De Dados Efetiva?' (*JOTA* September 2, 2021) <www.jota.info/opiniao-e-analise/artigos/o-que-falta-ao-brasil-e-a-america-latina-para-uma-protecao-de-dados-efetiva-02092021> accessed December 31, 2022

Three elements are particularly interesting to construct this new post-Western vision of data governance. First, the multistakeholder approach that characterises the Brazilian Internet governance and digital policy making which is embedded in its new data protection framework. Second, the strong relevance of cybersecurity and, consequently, data security, which is a cornerstone of the Chinese data protection approach. Third, the Indian willingness to experiment with the development of technical tools to implement data protection, especially through its new Data Empowerment and Protection Architecture.

Furthermore, it is important to note that the normative regimes and approaches to digital governance of the countries present an interesting degree of convergence. The similarities seem to be facilitated both by their willingness to transplant into their national frameworks some key elements of foreign systems which act as common sources of inspiration, and by their shared membership of the BRICS grouping, which increasingly acts as a "pentalateral" digital governance forum.[6] Curiously, despite the existence of relevant scholarship exploring the economic and geopolitical relevance of the BRICS countries[7] and the BIC part of BRICS, their digital policies and particularly their data architectures, are remarkably underexplored. Hence, this paper should be seen as part of a broader effort aimed at providing further insight and visibility to non-Western approaches to digital policies driven by leading emerging countries, especially the members of the BRICS grouping.[8]

Due to the very recent, yet intense, attention that these countries have paid to digital issues, their enormously relevant policy and institutional updates have attracted the interest of scholars, policymakers, and business leaders. Yet, having become some of the world's largest economies only over the past three decades, these countries and their regulatory systems are still largely unknown, frequently misunderstood, and only compared in the context of the rare BRICS studies emerging over the past fifteen years.

---

[6] See e.g., Lucca Belli and Danilo Doneda, 'Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence' [2022] International Data Privacy Law; Luca Belli, 'Data Protection in the BRICS Countries: Enhanced Cooperation and Convergence towards Legal Interoperability' [2021] New Media Journal Luca Belli (ed), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries* (1st edn, Springer 2021).

[7] See e.g., Oliver Stuenkel, *Post-Western World: How Emerging Powers are Remaking Global Order* (Polity Press 2017); Renato Baumann and others, *BRICS Studies and Documents* (Alexandre de Gusmão Foundation 2017); Yao Ouyang, Xianzhong Yi and Lingxiao Tang, *Growth and Transformation of Emerging Powers: Research on BRICS Economies* (Palgrave Macmillan 2020).

[8] For an ample range of analyses on the matter, see (*CyberBRICS*) <https://cyberbrics.info/> accessed December 31, 2022

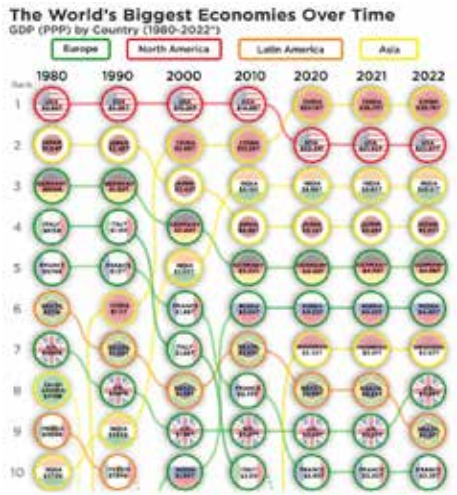

Table 1: Largest Economies in The World Over the Last 40 Years. Source Howmuch.net[9], estimates by International Monetary Fund.

To bridge this research gap, this paper starts by providing a historical overview of how national data protection frameworks evolved in Brazil, China, and India. Subsequently the paper identifies the main characteristics of the national data architectures, focusing on the key elements of novelty that these countries have introduced in their new national systems: the new multistakeholder advisory body for the Brazilian data protection authority, the developmental approach and the new data security framework of China, and the new Indian Data Empowerment and Protection Architecture.

Finally, the concluding section argues that understanding the countries' approaches to data governance seems necessary to grasp not only how these very different giants evolve but also the influence they will have on other countries at both regional and global levels. In this sense, their innovations and their relevance have the potential to give rise to a new third way in data governance, witnessing the emergence of a post-Western data architecture option, which may be better suited to meet the needs of Global South countries. However, the article also suggests that researchers and policymakers analyse these changes with caution and pragmatism. While the approach emerging from the combination of these novel features may offer some interesting solutions to tackle shortcomings of the existing models, the BIC frameworks are not exempted form criticisms, especially as regards the very

[9] Irena, 'Ranking the World's Biggest Economies over the Last 40 Years' (*HowMuch*) <https://howmuch.net/articles/worlds-biggest-economies-over-time> accessed January 1, 2023

light safeguards they offer against abusive data processing practices perpetrated by public organs.

A new third way of framing data governance may be useful to provide an alternative and palatable option other than the usual European or US models. On the one hand, the US approach is frequently criticised for it excessively minimalist stance, which de facto equals to failure to regulate even when regulatory intervention is needed. On the other hand, the European approach suffers a double problem. It seems both overconfident in the capacity of traditional regulatory strategies to regulate a highly complex field and it appears – almost hubristically – blind to the limits of the existing approach, especially regarding the complexity of compliance with data protection law. This latter problem is reflected in the frequently poor levels of enforcement, either because the regulated subjects do not know how to comply or find it too costly to do so, or because the regulators themselves have no sufficient – intellectual and financial – resources to guide and ensure correct compliance.

The novelties brought by Brazil, China and India aim at coping with such limits, exploiting some of the greatest assets that characterise their national approaches to technology: namely, the Brazilian multistakeholder governance, the Chinese cybersecurity and developmental approach, and the Indian technological expertise. Multistakeholder governance can be very useful to enhance the quality of both policymaking and implementation through the involvement of an ample gage of stakeholders of different natures.[10] Sound and detailed cybersecurity governance, providing well-structured guidance on how to comply with data security obligations, developing technology that embeds the desired normative values, and fostering stakeholder coordination to achieve the desired goals, are essential to cope with omnipresent cyber threats. Going beyond the mere normative and institutional approach to data protection, creating open protocols and open-source software that directly translate legal obligations into technical tools is the new evolutionary step in data protection.

Of course, the enthusiasm for the above-mentioned innovative approaches must be tempered with a good dose of pragmatism, understanding that such approaches, as any other regulatory strategy or governance mechanism, need safeguards to make sure they are used for the greatest benefit of society. Multistakeholder processes can easily become mere talking shops,

[10] Luca Belli and others, 'Exploring Multistakeholder Internet Governance: Towards the Identification of a Model Advisory Body on Internet Policy' CyberBRICS <https://cyberbrics.info/wp-content/uploads/2020/04/01-Belli-et-al-Exploring-Multistakeholder-Internet-Governance.pdf> accessed 27 December 2022.

cybersecurity often rhymes with surveillance, and the use of technology to achieve regulatory objectives may easily mutate into so-called "techno-solutionism" or even worst "techno-authoritarianism". No institution, no law, and no technology are exempt from vulnerabilities, and they all need appropriate checks and balances to perform in a sustainable fashion.

These risks are concrete and, as in any other regulatory choice, they must be considered from the conception to the implementation of the regulatory strategy. It is also important to remember that enthusiasm must be tempered with a certain degree of objectivity when analysing the policy, governance and technological strategies of countries that several observers often categorise as "partly free", "not free" or even "authoritarian regimes,"[11] However, if well-conceived and properly implemented, the innovations brought by the Brazilian, Chinese, and Indian systems can be incredibly useful to foster meaningful data protection in the Global South and beyond, building a new post-Western model of data governance.

I. Background: The Rise of Data Architectures in Brazil, China, and India

The juridical systems of Brazil, China, and India present both similarities and differences. This general observation is applicable also to the special case of data protection, if we consider the Indian (Digital) Data Protection Bill as the country's data governance standard. In this area, the three countries have enjoyed similar sources of inspiration and even engaged in "transplanting"[12] good practices issued from foreign systems in their national frameworks. Indeed, being relative latecomers as regards the comprehensive regulation of personal data, Brazil, China, and India have enjoyed the privilege of learning from previous experience of existing frameworks.

Comprehensibly, the most notable sources of inspiration have been the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Council of Europe Convention 108 and its modernised version, the European Union General Data Protection Regulation. The national experiences of the fellow BRICS countries have also played a relevant role.[13]

---

[11] See for instance the Global Freedom Scores, the Internet Freedom Scores, and the Democracy Scores elaborated by annually by Freedom House and available at "Countries and Territories" (*Freedom House*) <https://freedomhouse.org/countries/freedom-world/scores> accessed December 31, 2022

[12] Well-known in comparative law studies, the concept of 'legal transplantation' refers to 'the moving of a rule or system of law from one country to another'. See Alan Watson, Legal Transplants: An Approach to Comparative Law (1974) 21.

[13] See (n 5).

Notably, Russia and South Africa were the first member of the grouping to adopt data protection laws in 2006 and 2013 respectively. Since 2015, the BRICS grouping has promoted the regular exchange of "information and case studies on ICT policies and programs" on a regular basis, through several dedicated Working Groups.[14] Starting from the Xiamen Declaration, resulting from the 9th BRICS Summit held in China in 2017, the countries have also agreed on a joint commitment to "advocate the establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet."[15]

Starting with their respective backgrounds, Brazil, China, and India share a long – and sometimes tortuous – gestation of their personal data law-making processes. Over the past two decades leading to the elaboration of their national frameworks, the three countries established legislation regulating some aspects of data protection in some specific sectors, but such a fragmented approach led to juridical uncertainty, confusion, and inefficiencies. This resulted in spreading a shared yearning for comprehensive and harmonised data governance amongst interested stakeholders.

It is useful to remember that such yearning is the result of several factors spanning from constitutional and jurisprudential considerations to quintessentially geopolitical and economic ones. Each has been seasoned with a good number of global scandals which prompted public outrage and demand for sound data privacy. Notably, the revelations of former National Security Agency (NSA) contractor Edward Snowden may be considered as the most important event, triggering increased attention and consequent policymaking regarding data governance and even "data sovereignty" in the countries.[16]

---

[14] Since 2014, the countries have discussed the creation of the Working Group of Experts of the BRICS States on security in the use of ICTs and the BRICS Working Group on ICT Cooperation, which were formalised with the 2015 BRICS Declaration. See 'BRICS (VII BRICS Summit) "Ufa Declaration" (9 July 2015)' (BRICS) <www.brics2021.gov.in/BRICSDocuments/2015/Ufa-Declaration-2015.pdf> accessed 8 October 2021. The empirical research conducted by the CyberBRICS project provides a useful comparison of an ample range of elements of the BRICS national data protection frameworks. A detailed comparative analysis of such elements is available in "BRICS Data Protection Map" updated by the CyberBRICS Project in December 2021. "Data Protection across BRICS Countries" (*CyberBRICS* March 28, 2022) <https://cyberbrics.info/data-protection-across-brics-countries/> accessed 1 January 2023.

[15] 'BRICS (IX BRICS Summit) "Xiamen Declaration" (4 September 2017)' (MEA) <www.mea.gov.in/uploads/publicationdocs/28912_xiamendeclaratoin.pdf

[16] For an analysis of the concept of data sovereignty see Anja Kovacs and Nayantara Ranganathan, *Data Sovereignty, of Whom? Limits and Suitability of Sovereignty Frameworks for Data in India* (2020) Data Governance Network Working Paper 3 <https://cyberbrics.info/data-sovereignty-of-whom-limits-and-suitability-of-sovereignty-frameworks-for-data-in-india/> accessed 31 December 2022. For a digression on why BRICS countries and emerging economies might be interested in or even need to constructing data

The Snowden disclosures had a particularly dire effect on the countries, confirming with evidence the long-hold suspicions of US global espionage via home grown digital technologies. Such evidence included the illegal wiretapping of the Brazilian President's personal phone[17] and the communications of numerous members of the Brazilian government.[18] The reaction of the then President Dilma Rousseff, eloquently illustrated in her opening statement of the 68th UN General Assembly, is a potent reminder of the NSA scandal consequences:

> *As many other Latin Americans, I fought against authoritarianism and censorship, and I cannot but defend, in an uncompromising fashion, the right to privacy of individuals and the sovereignty of my country.*
>
> *In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy. In the absence of the respect for sovereignty, there is no basis for the relationship among Nations.*
>
> *We face, Mr. President, a situation of grave violation of human rights and of civil liberties; of invasion and capture of confidential information concerning corporate activities, and especially of disrespect to national sovereignty.*[19]

It is important to note that this geopolitical context prompted an unprecedented alignment amongst the unusual BRICS grouping, regarding data-related policies, leading to some of their most ambitious initiatives regarding data governance at the national level, as well as to enhanced cooperation on digital policies at the international level.[20] Indeed, following the scandal, BRICS leaders declared – for the first time since their establishment – an

---

sovereignty or digital sovereignty frameworks, see Luca Belli, 'BRICS Countries to Build Digital Sovereignty' (*Open Democracy* November 18, 2019) <www.opendemocracy.net/en/digitaliberties/brics-countries-build-digital-sovereignty/> accessed 1 January 2023.

[17] Sônia Bridi and Glenn Greenwald, "Documents Reveal US Agency Scheme to Spy on Dilma" (*Fantástico* September 1, 2013) <https://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html> accessed January 1, 2023.

[18] 'US Bugged Dilma, Former Ministers and Presidential Plane, Reveals WikiLeaks' (*Política* July 4, 2015) <http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html> accessed January 1, 2023

[19] Dilma Rousseff, 'Statement by H.E. Dilma Rousseff, President of the Federative Republic of Brazil, at the opening of the general debate of the 68th session of the United Nations General Assembly (UNGA, New York, 25 September 2022) <https://1library.co/document/wye9vl0q-statement-rousseff-president-federative-republic-general-assembly-september.html> accessed 10 January 2023.

[20] Belli and Doneda 'Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence' (n 6).

explicit reference to the "paramount importance" played by the "security in the use of Information and Communication Technologies (ICTs)"[21] in their annual Summit declaration.

The BRICS context needs to be emphasised and understood as, since 2013, it is a stable forum for Brazil, China, and India to continuously discuss and enhance their cooperation in the field. Since the abovementioned 9th BRICS Summit in Xiamen, the countries' commitment to structure and cooperate on cybersecurity and data protection issues has been continuously reiterated.[22] This context, together with the maturation of the long-gestated internal debates and further wake-up calls –such as the Facebook-Cambridge Analytica scandal, which provided a telling example of how the massive collection and misuse of personal data can be weaponised against individuals and societies alike – led Brazil, China, and India to intensify their policy-making efforts, with a renewed interest in their digital sovereignty.[23]

The subsequent subsections provide more country-specific context regarding the major developments undertaken by the countries, in recent years, leading to the elaboration of new data protection legislation and oversight systems.

A. Brazil: Towards the Harmonisation of a Fragmented System

In August 2018, Brazil adopted its new General Data Protection Law 13.709/2018, better known under its Brazilian acronym 'LGPD'[24] that started to enter in force in September 2020 and entered fully into force in August 2021.Before the adoption of LGPD, Brazil had a vast number of sectoral regulations on the federal level which directly and indirectly regulated personal data protection, but were often confusing, redundant, or contradictory.

Data protection was partially and inconsistently addressed in sparse legislation, driven by the logic of sectorial regulation of specific fields rather than being based on the integral protection of the personality through the

---

[21] V BRICS Summit Ethekwini Declaration BRICS and Africa: Partnership for Development, Integration and Industrialisation 2013 (*BRICS 2022*) para 34 <http://brics2022.mfa.gov.cn/eng/hywj/ODS/202203/t20220308_10649513.html> accessed 10 January 2023.

[22] Belli and Doneda 'Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence' (n 6).

[23] Belli "BRICS Countries to Build Digital Sovereignty" (n 16).

[24] 'The Brazilian General Data Protection Law – Unofficial English Version' (*CyberBRICS Project* 2020) <https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/> accessed 31 December 2022.

protection of personal data.[25] As an instance, the Habeas Data Law defined the procedure to exercise the fundamental right to access personal information stored in a public database foreseen by Article 5 of the Federal Constitution, while Article 43 of the Consumer Protection Code established the right to access the personal data of consumers, without defining a procedure to enable the access. The Positive Credit Registry Law defined the financial institutions' capacity to collect consumer information for credit scoring purposes, while the Civil Rights Framework for the Internet, better known as "*Marco Civil da Internet*" ('MCI'), prohibited the collection of Internet users' data "except upon the user's express free and informed consent or as provided by law".[26]

Conspicuously, none of the aforementioned laws defined what was to be considered as personal data in the first place, and key provisions such as the definition of the legal grounds for data processing were typically deferred to future legislation. Such a fragmented and partial approach created notable juridical uncertainty. The LGPD aimed to replace or supplement the enormously heterogeneous and fragmented sectorial regulations that Brazil enacted over the past decades. Indeed, roughly forty federal laws and decrees, directly and indirectly, regulated personal data protection across several sectors, before the entry into force of LGPD. Some of the most relevant federal legislation, which has been complemented, updated, and clarified by LGPD include:

- The General Telecommunications Law (Federal Law n. 9472 of 1997; Art 3, IX) ensuring consumers possess the right to privacy in telecom services.
- The Habeas Data Law (Law No. 9.507/97).
- The Criminal Identification Law (Federal Law n. 12,037 of 2009).
- The Resolution 3/2009 of the Internet Steering Committee in Brazil (CGI.br), establishing principles for ensuring privacy and data protection on the use of the internet in Brazil, mainly regarding activities developed by internet service providers.
- The Law on Free Access to Information (Federal Law 12527/2011, especially regarding its Article 4 IV and Article 31).
- The Civil Rights Framework for the Internet, or *Marco Civil da Internet* (Federal Law n. 12.965 of 2014).

---

[25] Danilo Doneda, *From Privacy to Personal Data Protection* (Thomas Reuters Brazil 2021).

[26] Marco Civil da Internet (Federal Law n. 12.965 of 2014) art 7. VII <https://observatoriolegislativocele.com/en/brazil-law-12-965-civil-internet-framework-2014/> accessed 31 December 2022.

- Positive Credit Register Law (Law No 12.414/2011) together with Decree No.9,936/19 and Central Bank Resolution No. 4/737/19, regulating the establishment and management of databases containing information about the payment history and transaction record of individuals and legal entities, to build credit scoring.[27]

Importantly the process leading to the elaboration of LGPD took almost a decade since the proposal of the first official Draft Bill on the Protection of Personal Data and Privacy.[28] This was based on a proposed model law debated within the Mercosur (the international economic organisation composed of Argentina, Brazil, Paraguay, and Uruguay) working group on electronic commerce.[29] The Brazilian Ministry of Justice opened the first public consultation on a data protection bill in 2010.[30] The Draft Bill was largely moulded on Council of Europe Convention 108 and the EU Directive 95/46/CE,which were the main legal reference at the time and already included some typical Brazilian law features that were maintained until the final text of the LGPD, such as the explicit reference to core elements of consumer law.

However, during the subsequent 8 years, leading to the crystallisation of the LGPD, the provisions and structure evolved enormously, due to the very high number of diverse stakeholder contributions received during a new phase of public consultations. This included both a participatory process organised by the Brazilian Ministry of Justice and multiple Congressional hearings from 2016 to 2018.After the approval of the LGPD, in August 2018, the *vacatio legis*[31] period preceding its entry into force was subsequently extended on multiple occasions, leading to a situation of considerable juridical uncertainty. The COVID-19 pandemic brought more confusion and

---

[27] A detailed overview of the sectorial laws and regulations can be found in Luiza Sato and others, *Data Protection Laws and Regulations Report 2022-2023 Brazil* (*International Comparative Legal Guides International Business Reports*) <https://iclg.com/practice-areas/data-protection-laws-and-regulations/brazil> accessed 13 January 2023.

[28] The original draft submitted to public consultation in 2010 as well as the contributions received during the first consultation phase can be found at (Pensando DIREITO) <http://pensando.mj.gov.br/dadospessoais2011/files/2011/03/PL-Protecao-de-Dados_.pdf> accessed 31 December 2022.

[29] Mercosur, "XII Ordinary meeting of the working subgroup No. 13 – Electronic Commerce" (15 June 2004) <https://documentos.mercosur.int/simfiles/docreuniones/23116_SGT13_2004_ACTA02_ES.pdf> accessed 8 October 2021.

[30] The consultation material contained in the archives of the Brazilian Ministry of Justice is still available on the personal website of Brazilian data protection pioneer, Professor Danilo Doneda: (Doneda) <www.doneda.net/2020/03/08/consultas-publicas-protecao-de-dados/> accessed 1 January 2022.

[31] In civil law systems, vacatio legis refers to the transition period between announcement of the legal act and its moment of entry into force. The purpose of this phase is to offer an adaptive period in which compliance to the new law can be duly organised before the law can be enforced.

attempts to further delay the entry into force of the Law.[32] Finally, the LGPD entered into force in September 2020, except for specific provisions dealing with administrative sanctions for non-compliance with LGPD, which came into force in August 2021, by way of Law 14,010/2020.

Brazil also established a new National Data Protection Authority, better known as 'ANPD'[33] in November 2020, and a new Multistakeholder National Council on Privacy and Data Protection that acts as an advisory body of ANPD. Although the ANPD has a very limited staff, the agency is currently fully functional, and responsible for enforcing the compliance of individuals, corporate and government entities with the LGPD. In January 2021, the ANPD published its initial regulatory agenda, through Decree No. 11. The document defined educational objectives and regulatory priorities. Amongst the most urgent tasks identified by the ANPD are the definition of special procedures for SMEs & start-ups, rules for the application of sanctions, data breach reporting and notifications, and data protection impact assessments. In a subsequent moment, the regulator foresees dealing with procedures for data subject requests, requirements, and tasks of Data Protection Officers (DPOs), and international data transfers.

Unfortunately, ANPD has not included in its regulatory priorities – thus leaving substantially undefined – other pressing issues such as data security and anonymisation criteria or the definition of interoperability standards, which are essential to allow the enjoyment of the right to data portability. Moreover, at the time of writing of this paper, most of the regulatory tasks mentioned above remain unaccomplished,[34] due to the remarkably limited capacity of ANPD, which makes it nearly impossible to operate effectively. Indeed, with a meagre budget and an initial staff of only 36 public servants – which was expanded only recently, to reach a still considerably light total of 75 members –the ANPD seems to have been structured to be unable to properly regulate and oversee data protection effectively, offering an example of what we may define as "ineffectiveness by design."

Last but not the least, the Brazilian Congress adopted a constitutional amendment creating the new fundamental right to data protection in the

---

[32] Luca Belli and Nicolo Zingales, 'Brazilian Data Protection under Covid-19: Legal Certainty is the Main Casualty' (*CyberBRICS* March 28, 2022) <https://cyberbrics.info/brazilian-data-protection-under-covid-19-legal-certainty-is-the-main-casualty/> accessed 1 January 2023.

[33] The official website of the new Brazilian Data Protection Agency is available at (*Autoridade Nacional de Proteção de Dados*) <www.gov.br/anpd/pt-br> accessed 1 January 2023.

[34] Progress regarding ANPD regulation can be monitored at "ANPD Publications" (*Autoridade Nacional de Proteção de Dados*) <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes> accessed 1 January 2023.

Brazilian Constitution, which was enacted in February 2022.[35] By granting personal data protection the rank of a fundamental right, the Brazilian Congress took a landmark step towards the recognition of the importance of personal data and its protection for the Brazilian people, especially considering recent technological developments. However, it is important to stress that the Brazilian Congress failed to seize the opportunity to define what are the essential elements of such a right – e.g., the principle of consent, legality, fairness, transparency, independent overview, etc. – which have been included in other experiences of the fundamental right to data protection, such as in Article 8 of the EU Charter of Fundamental Rights or Article 6 of the Mexican Constitution. Moreover, while the country has made considerable advancements, data protection compliance and a data protection culture are still very far from being achieved.

B. China: Building a New Type of Architecture, Blending Policy, Institutional, and Investment Upgrades

Chinese efforts to start regulating personal data processing started in the mid-2000 and were substantially upgraded in 2012, when the National People's Congress decided to initiate the elaboration of sectorial regulations, with the aim to strengthen the data protection rights of consumers[36] while establishing define a new cybersecurity and informatisation framework.[37] The Standing Committee of the National People's Congress updated the Consumer Protection Law (CPL) in 2013, conferring the right of data protection on consumers under Article 14. Since then, data protection principles such as confidentiality, purpose specification and consent, began having fundamental importance through reference in regulations.[38] In this perspective, the CPL was amended to include guidelines for regulating online consumer

---

[35] In May 2020, Brazilian Supreme Court recognized a fundamental right to data protection in the 1988 Brazilian Constitution, derived but not coincident with the right to privacy and the "habeas data" writ.

[36] Emmanuel Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU? (2020) 8 Penn State Journal of Law & International Affairs; M. James Daley, Jason Priebe and Patrick Zeller, "The Impact of Emerging Asia-Pacific Data Protection and Data Residency Requirements on Transnational Information Governance and Cross-Border Discovery" (2015) 16 Sedona Conf J 201, 205; Riccardo Berti, 'Data Protection Law: A Comparison of the Latest Legal Developments in China and European Union' [2020] Eur J Privacy L & Tech 34, 61.

[37] Belli L, Chang S and Chen L *The Great Data Strategy of China. Governance and Regulation with Chinese Characteristics*. (forthcoming).

[38] Min Jiang, 'Cybersecurity Policies in China' in Luca Belli (ed), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries* (Springer 2021) 188; Lingjie Kong L, "Enacting China's Data Protection Act" (2010) 18 International Journal of Law and Information Technology 197, 216-17; Consumers' Rights and Interests Protection Law of the People's Republic of China, 2013, art 14.

transactions, stipulated in Articles 25, 28 and 29[39], demanding that businesses preserve consumer information confidentiality. Thus, it prohibited the illegal disclosure, sale or provision to third parties without the consent of consumers.

Moreover, in case of data losses, companies were expected to provide remedies, with sanctions ranging from fines to criminal liability.[40] Hence, we can observe that consumer protection has been the first vector of strong personal data protection in China. Apart from protecting the data privacy of consumers, the second main pillar upon which data protection has been built in China has been cybersecurity. Notably, as regards the definition of standards regulating cloud computing infrastructure, including both server and information governance.[41]

Importantly, the Cyber Security Multi-Level Protection system comprises three national standards which require companies to carry out their cybersecurity obligations. The scope and application of these obligations vary, depending on the nature of the business.[42] The standards specifying their application have been defined by the Ministry of Industry and Information Technology ('MIIT') since 2011 and enforced in the sector of telecommunication and internet information services.[43] These standards were adopted by the MIIT to substantiate the 2011 Telecommunications and Internet Personal User Data Protection Regulation, which regulated the collection and usage of personal information in the context of telecommunication and Internet information services.[44] These regulations also reflect the principles of notice and minimum data collection, highlighted in the OECD Privacy Guidelines.[45]

In the sphere of cybersecurity, the Cyber Security Law of 2017 (better known as 'CSL') reflected numerous data protection principles largely inspired from the EU General Data Protection Regulation ('GDPR').[46] Importantly, China also put in place non-binding guidelines which facilitate

---

[39] Consumers' Rights and Interests Protection Law of the People's Republic of China, 2013.

[40] Jiang (n 38); Consumers' Rights and Interests Protection Law of the People's Republic of China, 2013, Ch VII.

[41] "China's New Cybersecurity and Privacy Requirements" (*Jones Day*) <https://www.jonesday.com/en/insights/2020/12/new-chinese-cybersecurity-and-data-privacy-requirements> accessed January 1, 2023.

[42] ibid.

[43] Pernot-Leplay (n 36) 72.

[44] ibid; Daley, Priebe and Zeller (n 36) 241-43.

[45] The OECD Privacy Guidelines, 2013, para 7; Pernot-Leplay (n 36) 72-74.

[46] Berti (n 36) 76-77; Shenkuo Wu, 'Cybersecurity Obligations of ICT Companies in P. R. China' [2019] J E-Eur Crim L 77, 79-81.

the interpretation of these sectoral regulations.[47] After adopting its landmark cybersecurity framework in 2017,[48] including a new data governance framework, China adopted the E-Commerce Law of 2018,[49] which included a right of access for individuals to their personal data. The law governed digital commercial transactions in China, extending to three types of e-commerce operators – platform operators like Alibaba, third-party merchants selling products in online stores, like Taobao, and independent sellers transacting through their own website or app.[50]

However, it is essential to emphasise that the Chinese data architecture is not merely based on a normative approach but, on the contrary, it blends normative, institutional and developmental elements, giving equal importance to each of them. Thus, such an approach rests on three fundamental pillars: institutional upgrade, strategic investments, and sound regulatory frameworks.[51] This multidimensional approach deserves to be stressed not only because it is an essential feature of the "governance and regulation with Chinese characteristics"[52] but also because it denotes the Chinese awareness that, despite its level of sophistication, law by itself is imperfect and insufficient as a tool to regulate society, economy, and technology. Law must be necessarily supported by well-performing, well-coordinated and well-funded institutions, as well as by strategic investments baking normative values into industrial policy and promoting the development of technology embedding normative values in its design.

To this end, starting in 2014 China has redesigned its cyber-related institutions to facilitate the elaboration and implementation of digital policies regarding information governance and cybersecurity. In this perspective, China established a new Cybersecurity and Informatization ('CI') *xitong*, created the new Cyberspace Administration of China ('CAC') as a new cyber regulator, and organised the new Central Commission for Cybersecurity and

---

47 Pernot-Leplay (n 36) 74-75.

48 Rogier Creemers, Paul Triolo and Graham Webster, "Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)" (*New America* June 29, 2018) <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/> accessed 1 January 2023.

49 'China: E-Commerce Law Passed' (*The Library of Congress*) <https://www.loc.gov/item/global-legal-monitor/2018-11-21/china-e-commerce-law-passed/> accessed 1 January 2023; 'P.R.C. E-Commerce Law (2018)' (*China Law Translate* January 9, 2020) <https://www.chinalawtranslate.com/en/p-r-c-e-commerce-law-2018/> accessed 1 January 2023.

50 Jiang (n 38) 190.

51 Belli L, Chang S. and Chen L., *The Great Data Strategy of China. Governance and Regulation with Chinese Characteristics* (2023).

52 ibid.

Informatization ('CCCI').[53] A *xitong* is a peculiar Chinese administrative structure,[54] aimed at providing a dedicated "policy system", involving all the public sector stakeholders affected by a specific policy area. Its goal is to deal with the complexity of a multi-layer administration in a gigantic state, thus being able to coordinate and regulate specific sectors efficiently.

These institutional updates were also accompanied by new strategies promoting multi-billion investments in three core areas related to data governance: ubiquitous connectivity, the Internet of Things (IoT), and Artificial Intelligence (AI). In 2015, China adopted the ambitious "Internet Plus" and "Made in China 2025" plans with a large focus on the expansion of Internet access, the IoT and its enablers, followed by a National Plan for Artificial Intelligence Development and the AI Governance Principles, to reap the benefits of connectivity and datafication. These strategic documents were accompanied by the adoption of an overarching Cybersecurity Law, in 2017, followed by two key documents setting the tone of future data-related legislation: the Personal Information Security Specification and the E-Commerce Law, in 2018.

Several major legal developments followed suit. A new Civil Code establishing rights to privacy and personal information protection entered into force in January 2021, a new Data Security Law entered into force in June 2021, a new Personal Information Protection Law entered into force in August 2021, new Regulations on Critical Information Infrastructure entered into force in September 2021 a new Regulation on Algorithm-empowered Online Recommendations entered into force since March 2022, and Provisions on the Management of Automobile Data Security for trial implementation are effective since October 2021.The new framework designed by PIPL will be discussed in section 2. Moreover, the Chinese government has planned the elaboration of several complementary regulations to frame some data-intensive next-generation technologies, perceived as key to the future of the Chinese economy.

Lastly, it is also essential to note, that, while implementing considerable normative and institutional advancements regarding data governance, which deserve to be studied carefully, China has also received considerable criticism for its data governance practices. On the one hand, the human rights issues raised by its digital surveillance programmes have frequently

---

[53] Rogier Creemers, 'China's Cyber Governance Institutions' [2021] Leiden Asia Centre <https://leidenasiacentre.nl/wp-content/uploads/2021/01/Chinas-Cyber-Governance-Institutions-Layout-geconverteerd-1.pdf> accessed 1 January 2023.

[54] A Doak Barnett, *Cadres, Bureaucracy, and Political Power in Communist China* (Columbia University Press 1967).

been emphasised by observers for its unlimited social control capabilities.[55] For instance, several legal scholars have criticised the Chinese social credit system, as an attempt to replace the "rule of law" with the "rule of trust," combining large-scale monitoring with disproportionate punishments.[56] On the other hand, the peculiar constitutional law system of China, which lacks judicial review and is characterised by the cohabitation of two normative systems – one of the Party and one of the state – has frequently been criticised for its reduced separation of powers and ample governmental discretion.[57] In this perspective, the Chinese approach considerably differs from the European one, which is based on the assertion of fundamental rights to define limits on personal data usage from both the private and the public sectors. On the contrary, the Chinese approach has traditionally promoted ample data collection and processing as tools to support statecraft.[58]

At the same time, China has adopted an increasingly assertive stance at the international level, regarding data governance and data security. Since the early 2010s, China has started prioritising IT governance in its political agenda, with the explicit goal of becoming the new "Cyber Power".[59] Such ambitions become more concrete at the end of the 2010s with several international projects of different natures already in the execution phase. In October 2020, China has proposed a Global Data Security Initiative, whose core components have been recently endorsed by the "Data Security Cooperation Initiative of China+Central Asia (C+C5)".[60]

Moreover, several observers have stressed the Chinese appetite to use its multi-trillion Belt and Road Initiative ('BRI'), and particularly its digital-related component, the Digital Silk Road ('DSR'), to deploy a new type of "Beijing effect"[61] consisting of the large-scale supply of Chinese digital

---

[55] See, most notably, Josh Chin and Liza Lin, *Surveillance State: Inside China's Quest to Launch a New Era of Social Control* (St Martin's Press 2022).

[56] Yu-Jie Chen, Ching-Fu Lin and Han-Wei Liu, '"Rule of Trust": The Power and Perils of China's Social Credit Megaproject' (2018) 32 Columbia Journal of Asian Law 1.

[57] Ling Li, '"Rule of Law" in a Party-State: A Conceptual Interpretive Framework of the Constitutional Reality of China' (2015) 2 Asian Journal of Law and Society 93.

[58] See e.g., Belli, Chang and Chen (n 37); Brett Aho and Roberta Duffield, 'Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China' (2020) 49 Economy and Society 187.

[59] For a detailed analysis of China's "Cyber Power Strategy", see Rogier Creemers, "How China Intends to Become a 'Cyber Power'" (2020) N° 177-178 Hérodote 297.

[60] Chris Devonshire-Ellis, "China Lays out Ten Cooperation Points with Central Asian Nations" (*Silk Road Briefing* June 12, 2022) <https://www.silkroadbriefing.com/news/2022/06/12/china-lays-out-ten-cooperation-points-with-central-asian-nations/> accessed 2 January 2023.

[61] See Matthew Steven Erie and Thomas Streinz, 'The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance' (2021) 54 NYU J Int'l L & Pol 1.

infrastructures[62] that enable data governance in DSR countries, according to Chinese technical standards. To these initiatives, one must add the considerable influence exercised by the extraterritorial scope of its recently adopted data-related regulations, notably by PIPL.

C. India: The Unfinished Journey towards a Data Protection Law

To date, India has not adopted yet a general data protection law, although multiple versions of a Data Protection Bill have been discussed over the past five years and several sectoral regulations exist in the country to frame the processing of personal data in areas such as payment systems, telecommunications, and healthcare. Furthermore, it is also important to emphasise that it would be mistaken to argue that privacy is a concept entirely transplanted in India from Western legal cultures. Indeed, the essential elements that compose the notion of privacy existed in both Hindu law and Islamic law.[63] While several religious texts provided a perception of privacy as a concept driven by the imperative of purity, key treatise such as the Arthashastra, Naradsmriti and the Manusmriti constructed the fundamental elements of the privacy of physical space, the respect to bodily integrity, and the privacy of thought.[64] However, the formalisation of this concept and, particularly, of data privacy is extremely recent. Indeed, India consolidated privacy through rulings of the Supreme Court as the Indian constitution does not explicitly mention a right to privacy.

In other words, the recognition of a fundamental right to privacy upon which data privacy can be built had to be done through jurisprudence, which established that the right to privacy is implicitly present in Article 21 of the Indian Constitution. This was seen in the landmark *Puttaswamy* case, by which the Supreme Court of India recognised privacy as a new fundamental right, in August 2017,[65] thus opening the path to the elaboration of a new Data Protection Bill. The bill was introduced in the Parliament in December 2019 and considerably reshaped since then until reaching its latest iterations

---

[62] The term "digital infrastructure" should be considered as any physical and logical asset, as it is generally understood in Science and Technology Studies. As such digital infrastructures encompass both the physical infrastructure aimed at providing connectivity, such as undersea cables, micro and macro cells, routers, connected devices, etc. but also the technical protocols and software applications that facilitate user communication.

[63] Ashna Ashesh and Bhairav Acharya, 'Locating Constructs of Privacy within Classical Hindu Law' (*Centre for Internet & Society*) <https://cis-india.org/internet-governance/blog/loading-constructs-of-privacy-within-classical-hindu-law> accessed 2 January 2023.

[64] ibid.

[65] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.

by a Joint Parliamentary Committee in December 2021 and a new version renamed the Digital Data Protection Bill 2022.

Through this process, India is forging its own data protection model defining several unique features. Although the model is not finalised yet, when implemented it will have the potential to increase individual awareness about their data protection rights, strengthen privacy, and foster accountability. However, it is essential to clarify that the last versions of the Bill have been constantly and harshly criticised for the considerable exceptions allowing the central government to exempt any public body from the application of the Bill on remarkably elastic and vague grounds such as the security of State and public order. Such broad exemptions have been harshly criticised as they contradict the spirit of data privacy whose very purpose is to define clear rules to limit the abusive processing of personal data for the protection of the individual and the well-functioning of democracy.

As mentioned above, the bill follows a long line of privacy jurisprudence in India that has been influenced by global developments as well as the country's own constitutional jurisprudence. Though the constitution does not explicitly mention a right to privacy, Indian courts have held that a right to privacy exists under the right to life guaranteed under Article 21. However, subsequent cases, with a smaller bench, held otherwise, leading to some ambiguity regarding the exact nature of the constitutional protection of privacy. This was particularly due to the long-standing judgment of the Supreme Court in Kharak Singh v State of Uttar Pradesh,[66] where the court held that a right to privacy did not exist under the constitution.

It became necessary to resolve this ambiguity due to two factors that became increasingly relevant: strident claims of loss of privacy in the wake of the government's implementation of its project for unique biometric identification ('Aadhaar'), and global developments, including both the abovementioned scandals and policymaking efforts, all occurring simultaneously.[67] The growth of the Indian information technology industry and the telecom revolution, which started in the late 1990s, led to the proliferation of digital services in India. This has had two significant consequences. First, the country is increasingly interconnected due to the growth of digital services and the adoption of a large number of online platforms. Second, the government has recognised that the digitalisation of public services is a powerful vehicle for achieving policy objectives such as financial inclusion and delivering cash

[66] *Kharak Singh v State of U.P.* AIR 1963 SC 1295: (1964) 1 SCR 332.

[67] This background and the associated tensions are eloquently discussed in Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* (HarperCollins 2018).

transfers, in the context of its Digital India umbrella programme for digital transformation.[68]

The second objective has been facilitated largely by the implementation of Aadhaar. Indeed, the word "Aadhaar" which literally means "foundation" is apt since the digitalisation of identity has been deemed as the cornerstone of digital transformation since the early stages of the Digital India implementation. However, the growing ubiquity of Aadhaar came under sustained criticism from various quarters. The debate on the privacy concerns over Aadhaar resulted in a clutch of petitions before the Supreme Court that challenged the validity of the legislation that enabled the system: the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. The five-judge bench of the Supreme Court that heard the petitions stated that, since the petitions claimed infringement of the right to privacy, it was of utmost importance to determine whether this right existed under the Indian Constitution. It referred this issue to a bench of nine judges of the Supreme Court, which held in August 2017 that a right to privacy did exist under Article 21.[69]

In a long line of past cases, privacy was used to protect specific interests, such as privacy from night-time police visits in the Kharak Singh case or privacy from telephone tapping in PUCL v Union of India. The narrative around data protection in India reached a crescendo during the hearings in the *K.S. Puttaswamy v Union of India* (2017) "right to privacy" case.[70] In a landmark verdict, crafted by a rare nine-judge bench, the Supreme Court of India affirmed the right to privacy[71] as a fundamental right. The ruling proclaimed that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution".

Critically, by declaring privacy as an integral component of Part III of the Constitution of India, the Puttaswamy decision explicitly inserts this new fundamental right amongst the group of constitutional rights that cannot be given or taken away by law, and all laws and executive actions must abide by.[72] It held that the Supreme Court had decided the question incorrectly

---

[68] (*Digital India*) <https://digitalindia.gov.in/> accessed 2 January 2023.

[69] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.

[70] ibid.

[71] Agnidipto Tarafder and Arindrajit Basu, 'For the Many and the Few: What a Fundamental Right to Privacy Means for India' (*The Wire*) <https://thewire.in/government/right-to-privacy-supreme-court-2> accessed 2 January 2023.

[72] Besides the new fundamental right to privacy, the constitutional rights protected by Part III of the Constitution of India include the rights relating to equality (arts 14 to 18); freedom of speech and expression (article 19(1)(a)); freedom of movement (art 19(1)(d)); protection

in Kharak Singh, and that informational privacy – which could be seen as encompassing both data privacy and informational self-determination – was a part of the right to privacy. The Supreme Court's judgment marked a departure from prior jurisprudence on two grounds. First, it clearly and unambiguously stated that there was a fundamental right to privacy under the constitution. The more significant ground was that the right to privacy was conceptualised as a right in itself, irrespective of what privacy it helped protect in turn.

In the past decades, India had built a global reputation as an IT powerhouse. The *Puttaswamy* ruling provided a long-awaited moment promoting the elaboration of a comprehensive data governance framework. Indeed, the single most relevant issue that every cross-border project outsourcing technological solution in India had to deal with was the fact that India had no data protection framework.[73] Outsourcing projects involve the transfer of personal data in virtually all cases, and the absence of data privacy provisions in the country where outsourcing takes place is considered either as an unacceptable risk or is explicitly prohibited by several data protection frameworks.

The Government of India took an initial and timid step to address this concern in 2008 when the new section 43A was included in the Information Technology Act.[74] This provision explicitly aimed at reducing international concerns regarding the lack of data protection in the Indian outsourcing industry, coming especially from Europe. However, the amendment was very succinct and provided only limited and general guidance as to how to process sensitive personal data, leaving essential procedural and substantial elements – such as the definition of what are "sensitive personal data and information" –undefined.[75]

When the Supreme Court of India resolved to establish the new fundamental basis of the right to privacy, and consequent data privacy, the Indian government decided to – finally – set up an expert committee to devise India's data protection framework. After a public consultation on a white paper,[76] the committee submitted a draft Personal Data Protection

of life and personal liberty (article 21), etc.Vrinda Bhandari and others, 'An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict' [2017] IndraStra Global <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2> accessed 2 January 2022.

[73] See Matthan (n 67).

[74] ibid 112.

[75] ibid.

[76] White Paper of the Committee of Experts on a Data Protection Framework for India (2017) <www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf> accessed 1 January 2022.

Bill[77] and an accompanying report interestingly entitled 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians'.[78] Ultimately, the Personal Data Protection Bill was introduced into Parliament in December 2019, after more than two years of fierce debate on the bill's provisions.

Importantly, rather than pushing to fast-track this hugely significant bill, India's minister of information technology, Ravi Shankar Prasad, referred it for scrutiny to a Joint Parliamentary Committee ('JPC') on the Personal Data Protection Bill, 2019.[79] The JPC conducted numerous meetings with Government ministries, industry bodies and various stakeholders. It also held meetings for clause-by-clause considerations of the PDP Bill. After two years of deliberation, the JPC tabled its report in December 2021, appending its recommendations to a substantially revised version of the law, named the 'Data Protection Bill, 2021'.

While the consultation process endeavoured by the Committee can be commended for its diversity, it has also received notable criticism as the Committee did not necessarily integrate the full spectrum of opinions and suggestions it received. The process encompassed one of the most comprehensive consultations by a Parliamentary Committee, with stakeholders from all walks providing diverse views and opinions. However, many stakeholders directed remarkably vocal criticism to two specific and highly controversial issues. Firstly, the Committee choice to collapse the distinction between personal and non-personal data, and, secondly, the creation of ample exemptions from the application of the bill to governmental bodies.

To finalise the process, the report published by the Committee proposed a total of ninety-three recommendations. Such a large number of recommendations is indicative of the particularly vast and heterogeneous feedback the Committee received and, while its choices are not exempt from critiques, it is possible to state it has combed over every aspect of the legislation in question. However, this version was not only the largest but also the shortest-lived iteration of the bill, being withdrawn by the government in August 2022, to be subsequently replaced by a new lighter draft, with only thirty clauses, named the Digital Personal Data Protection Bill 2022.

---

[77] Draft of the Personal Data Protection Bill (2018) <www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf> accessed 1 January 2023.

[78] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) <www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 1 January 2023.

[79] Trisha Jalan, 'BJP's Meenakshi Lekhi Appointed Chair of Joint Committee for Personal Data Protection Bill' (*MediaNama* March 25, 2021) <https://www.medianama.com/2019/12/223-personal-data-protection-bill-joint-committee-members-rs-prasad/> accessed 2 January 2023.

While the simplification of the draft is welcome, the criticisms against the previous version seem not to have been addressed.[80] Moreover, the continuous release of new drafts, together with the certainty that the 2022 version is not going to be the final one to be published for comment, make the entire participatory processes extremely complicated and burdensome, thus limiting enormously the number of civil society stakeholders that may have the time and resources necessary to provide comments. At the time of this writing, it is not possible to know when the final version of the Bill will be published, thus making the entire process very questionable from a legal certainty perspective. Table 2 below represents a timeline allowing the reader to visualise the key steps of the bill's elaboration process. A phased implementation timeline of two years has been proposed by the JPC.

Date	Update
July 2018	The Personal Data Protection Bill (PDP) is first drafted by an expert committee headed by Justice BN Srikrishna.
October 2018	The Ministry of Electronics & Information Technology stated that it will be drafting the bill.
December 2019	The bill is referred to a Joint Parliamentary Committee and BJP MP Meenakshi Lekhi is appointed chairperson.
September 2020	The committee requests and obtains an extension of time for the presentation of their report.
December 2020	The committee undertakes a clause-by-clause review of the bill.
November 2021	The Committee holds meetings to discuss the consideration and adoption of its draft report.
December 2021	The report of the Joint Parliamentary Committee is tabled in the Parliament.
August 2021	The Personal Data Protection Bill 2021 is withdrawn.
November 2022	The Digital Personal Data Protection Bill 2022 is published for consultation.

Table 2: Personal Data Protection Bill timeline

It is also relevant to note that, despite lacking a general data protection law, India already enjoys sectorial regulations, directives and licence conditions issued by sectoral regulators in relation to payment systems, telecoms, healthcare, e-pharmacies, etc., that stipulate certain data protection obligations.[81] The Indian legislature did amend the Information Technology Act (2000) to

[80] See s 2.3.1 of this paper.

[81] For a comprehensive analysis as well as a comparison with the personal data regulations of other BRICS countries, see "Data Protection across BRICS Countries" (*CyberBRICS*

include Section 43A and Section 72A, which give a right to compensation for improper disclosure of personal information. The Indian central government subsequently issued the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules under Section 43A of the IT Act. The Rules have imposed additional requirements on commercial and business entities in India, relating to the collection and disclosure of sensitive personal data or information, which have some similarities with the GDPR and the Data Protection Directive.

Companies in regulated sectors such as financial services and telecoms are subject to obligations of confidentiality under sectoral laws which require them to keep customer personal information confidential and use them for prescribed purposes, or only in the manner agreed with the customer.

Lastly, in August 2020, NITI Aayog (a policy think tank run by the Government of India) released a draft framework on the Data Empowerment and Protection Architecture ('DEPA') in consultation with a few industry regulators, banks and fintech players.[82] While the Indian concept of consent managers may recall already existing Personal Data Stores ('PDSs') or Personal Information Management Systems('PIMSs') such as CitizenMe and Solid, it is important to stress that previous PDS and PIMS examples are relatively niche initiatives.[83] The Indian experiment of electronic consent management frameworks within the DEPA, is the first nationwide initiative stemming from the Indian digital transformation plan. DEPA is developed in the context of the so-called "India Stack", has become a new hallmark of the Indian data architecture,[84] and will be explored in section 2.

March 28, 2022) <https://cyberbrics.info/data-protection-across-brics-countries/> accessed 2 January 2023.

82 NITI Aayog, Data Empowerment And Protection Architecture: Draft for Discussion (2020) <https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf>accessed 2 January 2023.

83 Serge Abiteboul, Benjamin André, Daniel Kaplan, 'Managing your Digital Life with a Personal Information Management System'(2015) 58 (5) Communications of the ACM, Association for Computing Machinery 32; Guillaume Brochot and others, 'Study on Personal Data Stores conducted at the Cambridge University Judge Business School'(European Commission 2015) <https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school> accessed 2 January 2023.

84 Belli and Doneda, 'Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence' (n 6).

II. New Data Architectures: Legal Transplants and Innovative Elements

Brazil, China, and India have several similarities and yet also differ in many ways in their data architectures. While India's framework is not definitive yet, its normative provisions resemble in many points those enacted by Brazil and China, thus suggesting the existence of a shared data protection skeleton.[85] The three countries define similarly personal data, which refers to the information related to an identified or identifiable natural person. The three jurisdictions also conceptualise the 'data subject' and 'data controller' similarly, although the terminology utilised varies, as China coined the term 'personal information handler' and India prefers to use the terms "data principal" and "data fiduciary".[86]

While the exact denomination of similar concepts may vary according to the national legal vernacular, the substance of the various normative elements is frequently similar. For instance, the Chinese PIPL tasks a personal information handler to describe any "organizations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods" (art. 73.1). This would be roughly synonymous with the Brazilian (and EU) data controller, while the PIPL's "entrusted party" (art. 21) would reflect the Brazilian (and EU) data processor acting according to the controller's instructions.

It is also important to note that the Indian Bills introduce a remarkably interesting concept of "data fiduciary".[87] The core obligations of the data fiduciary basically overlap with the attributions of the Brazilian data controller and the Chinese data handler i.e., abide by data protection principles, obtain free and informed consent in order to process data, duly communicate information on the data processing, and ensure the security of all personal data under their responsibility.

Interestingly, the data protection frameworks of the three countries are also grounded on the same principles, including consent, purpose limitation,

---

[85] Belli, "Data Protection in the BRICS Countries: Enhanced Cooperation and Convergence towards Legal Interoperability" (n 6).

[86] See the "Definitions" section of the 'BRICS Data Protection Map developed by the *CyberBRICS Project*. "Data Protection across BRICS Countries" (*CyberBRICS* March 28, 2022) <https://cyberbrics.info/data-protection-across-brics-countries/> accessed January 1, 2023.

[87] See Rishab Bailey and Trishee Goyal, 'Fiduciary Relationships as a Means to Protect Privacy: Examining the Use of the Fiduciary Concept in the raft Personal Data Protection Bill, 2019' (The Leap Blog, 13th January 2020) <https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html> accessed 1 January 2023.

fair and lawful processing, necessity, data minimisation, security, and accountability.[88] Furthermore, they establish a similar set of obligations for controllers and provide similar rights to the data subjects, including access to data, data correction, elimination of personal data processed with the consent of the data subject, and revocation of consent.[89]

While several points of the Brazilian, Chinese and Indian Frameworks tend to converge, many elements are unique and characterise the national data architecture. The sections below provide an overview of such architectural elements.

A. Brazil

The LGPD has a very didactic structure, organised in ten chapters, defining: i) preliminary provisions, ii) processing of personal data, iii) rights of the data subject, iv) processing of personal data by public authorities, v) international transfer of data, vi) personal data processing agents, vii) security and good practices, viii) sanctions, ix) the ANPD and the National Data Protection and Privacy Council, x) final and transitional provisions.

Within the LGPD, three articles can be considered as fundamental: article 2, article 5 and article 6. Article 2 enumerates a series of fundamental elements upon which data protection is built in Brazil: i) privacy; ii) informational self-determination; iii) freedom of speech; expression, information, and communication; iv) inviolability of honour and intimacy; v) economic growth, technological development, and innovation; vi) consumer protection, freedom of enterprise and competition; vii) human rights, dignity and exercise of citizenship by natural persons. Article 5 of LGPD acts as a true glossary for Brazilian data protection, as it encompasses the definitions of all the terms used in the LGPD, while article 6 defines the principles that govern data protection, upon which rights and obligations are built.

Importantly, the LGPD also regulates the use of publicly available and accessible personal data. Some examples of such data include data present in databases of government bodies, notary records, official publications, and gazettes, but also data that has been explicitly made public by their respective data subjects (such as public profiles and biographies on social media networks). Interestingly, art. 7 LGPD deals with publicly available personal

[88] "Data Protection across BRICS Countries" (n 81) Policy Question 9.
[89] ibid Policy Question 13.

data imposing certain limitations, although opening the path to usage for additional purposes as long as such purposes are legitimate and specific.[90]

Amongst the ten legal grounds for data processing defined by article 7 LGPD, the ones that deserve closer attention are 'protection to credit' and 'legitimate interest' as they can both give rise to relevant loopholes. The first one is quintessentially a Brazilian peculiarity, derived from the remarkably intense lobbying of the banking and credit bureau sectors, towards the end of the LGPD law-making process, leading to the consideration of legitimate processing of personal data whenever necessary for credit protection.[91] Such legal basis is typically used by credit scoring bureaus, banks, insurance agencies, or FinTechs for assessing consumer solvability and credit risks and monetise such assessment. It is important to stress that the credit protection basis opens the door to an ample range of data misuses, especially when combined with the amended version of the Positive Credit Registry law no. 12.414 of 2011. Indeed, the 2019 amendments to this latter law have reverted the fundamental logic of credit scoring from the original opt-in system to the current opt-out by default. As such, the combination of the LGPD and Positive Credit Registry law provisions authorise all credit scoring entities to collect, process and even share consumer personal data (especially, their credit scoring) with third parties with no need for the data subject's consent.[92]

Hence the protection to credit legal ground, opens the door to processing operations incompatible with the very essence of data protection: the

---

[90] Particularly paragraphs 3 and 7 of art 7 LGPD, provide that:

"3. The processing of personal data whose access is public must consider the purpose, good faith and public interest that justified its availability to the public. […]

7. The subsequent processing of personal data referred to in paragraphs 3 and 4 of this article may be carried out for new purposes, provided that the legitimate and specific purposes for the new treatment and the preservation of the rights of the data subject are observed, as well as the grounds and principles foreseen in this Law." See 'The Brazilian General Data Protection Law – Unofficial English version' (CyberBRICS Project 2020) <https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/> accessed 1 January 2023.

[91] According to art 7 LGPD: "*Personal data can only be processed in the following events: […]*

X. for the protection of credit, including with respect to the provisions of the applicable law." See *ibid*.

[92] In April 2019, Complementary Law No. 166/2019 amend some key provisions of the Positive Credit Registry Law No. 12.414 of 2011. Most notably, the logic of the Positive Credit Registry was reverted from opt-in to opt-out. As provided for in the amended article 4 of the law, the authorisation of the data subjects for the use of their data is unnecessary. In addition, all consumers authorise by default the manager of the Positive Credit data bases, to make their credit score note available to consultants. This latter provision has been frequently criticised for directly contradicting the very rationale of informational self-determination, a series of data subject rights, and the principles of transparency, purpose specification and accountability, at the centre of by LGPD.

fundamental principle of informational self-determination. The legal framework created by the Brazilian legislator relies on the juridical fiction according to which all consumers (*de facto* the entire Brazilian population) are aware of the existence of the massive personal data collection orchestrated by the Positive Credit Registry and freely decide not to opt out from the system. However, most Brazilians are totally unaware that the entire population's data can be legally collected and processed for "credit protection" as such processing happens in remarkably opaque ways. Hence, processing data on this ground simply nullifies data subjects' capacity to exercise agency and data control and is antithetical to the informational self-determination rationale underpinning the LGPD.

As mentioned above, it is also relevant to note the introduction of the legitimate interest legal ground, which was not present in earlier Brazilian sectorial laws and has been legally transplanted from EU data protection law, considerably amplifying the spectrum of potentially legal purposes for which data can be processed.[93] Importantly, as in EU law, legitimate interest allows for usage of personal data for other purposes than the original one, as long as such ancillary purposes are compatible with the original one and do not hinder the data subject rights.[94] The performance of a Data Protection Impact Assessment (DPIA) and a proportionality test are the typical instruments used to balance the interests of the controllers and the rights of the data subject, to ascertain whether the legitimate interested base can be used. This legal basis is frequently used to justify big data analytics, artificial intelligence applications, machine learning systems and experimentation of innovative business models based on the (re)usage of personal data.

---

[93] For a detailed analysis, see: Bruno Ricardo Bioni, Mariana Rielli and Marina Kitayama, 'Legitimate Interests under the Brazilian General Data Protection Law: General Framework and concrete examples' (Sau Paulo: Associação Data Privacy Brasil de Pesquisa, 2021).

[94] General Data Protection Law 2018, Article 10. "*The legitimate interest of the controller may only be a reason for the processing of personal data for legitimate purposes, based on concrete situations, which include, without limitation:*

I. support and promotion of activities of the controller; and

II. protection, in relation to the data subjects, of the regular exercise of their rights or provision of services that benefit them, observing their legitimate expectations and the fundamental rights and liberties, pursuant to the provisions of this Law.

Paragraph 1. Whenever processing is based on the legitimate interest of the controller, only the personal data strictly required for the desired purpose may be processed.

Paragraph 2. The controller shall adopt measures to guarantee the transparency of the processing of data based on his or her legitimate interest.

Paragraph 3. The supervisory authority may request to the controller a data protection impact assessment whenever the grounds of the processing are its legitimate interest, subject to business and industrial secrets."

However, the possibility to use the legitimate interest legal base and avoid abuse relies on the controller capability to properly perform a DPIA and a proportionality test, which is currently extraordinarily challenging as the ANPD has not issued any guidance on how to perform such activities, despite having included it in its regulatory agenda. This lack of guidance leads to a situation where good faith controllers are in the dark and unable to properly comply with the LGPD, while bad faith controllers can easily claim that their processing is in their legitimate interest in the lack of precise indications on how to properly assess this situation.

Subsequently, articles 23-32 of the LGPD deal with the data processing activities of public authorities. This chapter offers additional evidence of the preoccupation of the Legislator regarding the correct framing of public bodies' processing of personal data, acknowledging the need for dedicated rules. Notably, article 23.III prescribes the need to appoint a Data Protection Officer to guide and oversee the correct processing of data. Article 25 regulates data structuring and interoperability mandating that personal data processed by public entities "shall be kept in an interoperable and structured manner for the shared use, aiming at the execution of public policies, the provision of public services, the decentralization of public activities and the dissemination and access to information by the general public".

Interoperability is an essential precondition to facilitate (personal) data exchange and usage. Indeed, the concept of interoperability aims at fostering the ability to transfer and use data across heterogeneous technologies and networks, to use services and share information across technically different but compatible and co-operating systems.[95] In light of its structural importance, interoperability has been a policy objective debated by Brazilian policymakers for more than two decades and its insertion in the LGPD reflects a longstanding concern of the Brazilian government with the issue.

Since the early 2000s, when the Brazilian government started to discuss its early digital transformation efforts (at the time labelled as "e-government"), the need for policies for interoperability became clear. Indeed, interoperability plays an instrumental role to cope with the enormous complexity of the Brazilian administrative structure and the multiplicity of the systems each administration may adopt. Given its continental size, Brazil features a wide range of very diverse administrations, including around 200 public bodies in

[95] Luca Belli and Nathalia Foditsch, 'Network Neutrality: An Empirical Approach to Legal Interoperability' in Luca Belli and Primavera De Filippi (eds), *Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet* (Springer 2016); Luca Belli and Nicolo Zingales, 'Interoperability to Foster Open Digital Ecosystems in the BRICS' (World Internet Conference Report, Chinese Academy of Cyberspace Studies 2022).

the Federal Executive alone, several independent agencies at both federal and state level, 27 state-level governments, and more than 5,560 municipalities.

Since 2014, Article 4 of the Civil Rights Framework for Use of the Internet in Brazil has enshrined interoperability into legislation, considering the promotion of "open technology standards that enable communication, accessibility and interoperability between applications and databases" as one of "the objectives of the regulation of Internet use in Brazil".[96] While the Brazilian data protection authority, ANPD, should take the lead[97] as regards the definition of interoperability standards for personal data, in accordance with article 40 of the LGPD,[98] the ANPD has not even clarified when this all-important issue will be regulated. Interoperability, and the right to data portability, whose effective implementation depends on the existence of interoperability standards, exist only on paper so far in Brazil. This is because the ANPD has not even included the definition of interoperability standards in its first regulatory agenda, published in January 2021.[99]

Under Article 26 of the LGPD, the Government must also meet strict conditions and specific purposes relating to the implementation of public policy, and 'legal attribution' by public entities in order to share personal data. Article 26 (1) lays out specific exemptions to the general rule according to which "the Government may not transfer to private entities personal data contained in databases to which it has access". Such exemptions refer to cases involving:

1. The "decentralised execution of public activity that requires the transfer, exclusively for this specific and determined purpose", in accordance with the Access to Information Law 12.527/2011.
2. The release of publicly accessible data.

---

[96] The Civil Rights Framework for the Internet, better known as *Marco Civil da Internet* (MCI), Federal Law n. 12.965 of 2014. Available at: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.html> accessed 1 January 2023.

[97] The Central Committee for Data Governance, created to oversee the interconnection of Brazilian citizens data bases by virtue of Presidential Decree 10.046/2019, subsequently amended by Presidential Decree 11.266/2022, has also mandate to regulate interoperability of public data bases in accordance with the guidelines of the ANPD. See art 5.3.II of Presidential Decree 10.046/2019.

[98] General Data Protection Law 2018, art 10: "The supervisory authority may establish interoperability standards for purposes of portability, free access to data and security, and on the retention time of the registrations, especially in view of the need and transparency." See (n.73).

[99] 'On Data Protection Day, ANPD publishes authority's biannual regulatory agenda for 2021-2022' (gov.br 28 January 2021). <https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-da-protecao-de-dados-anpd-publica-agenda-regulatoria-bianual-da-autoridade-para-2021-2022> accessed 1 January 2023.

3. The execution of agreements, contracts, or legal provisions in an instrument which explicitly allows the sharing of such data, as long as the agreements, contracts are communicated to the ANPD.

4. The protection of the integrity and security of the data subject and to prevent fraud or other financial irregularities.

i. The Brazilian Data Protection Authority (ANPD) and the National Council for the Protection of Personal Data and Privacy

An essential element of the Brazilian data architecture is the national data protection authority ANPD. Although article 55-B of the LGPD states that "technical and decision-making autonomy is assured to the ANPD", the Authority, cannot be considered as an independent body, as it is directly subject to the Presidency of the Republic. ANPD is composed of a Board of Directors, a National Council for Personal Data Protection and Privacy, Internal Affairs office, Legal Advisory Body, Ombudsman, administration, and specialized departments.

Critically, the ANPD is a severely under-resourced body, with a total staff of around forty individuals, including five members of the ANPD Board of Directors, appointed by the President. Hence, it can be argued that the administrative dependency on the Presidency as well as the remarkably limited resources of the ANDP makes it a herculean task for the agency to effectively oversee the implementation and specification of the LGPD.

The ANPD Board of Directors is assisted and advised by a multistakeholder National Council for the Protection of Personal Data and Privacy, which may be seen as one of the most innovative and characteristic elements of the Brazilian data architecture. Indeed, this notable feature has the potential to substantially contribute the achievement of what Stefano Rodotà – one of the fathers of data protection studies – called the 'data protection culture.'[100] This should be the prerogative of any data protection system and is understood as the widespread awareness among the population of the importance of data protection for the proper functioning of society, economy, and democracy.[101]

---

[100] Luca Belli et al. *Proteção de dados na América Latina: Covid19, Democracia, Inovação e Regulação. Arquipelago* (Arquipélago Editorial, 2021) ; Luca Belli and Danilo Doneda, 'What is missing from Brazil and Latin America for effective data protection?' (*Seguranca electronica*, 2 September 2021) <https://revistasegurancaeletronica.com.br/o-que-falta-ao-brasil-e-a-america-latina-para-uma-protecao-de-dados-efetiva/> accessed 1 January 2023.

[101] Luca Belli 'Data Protection Day evokes trauma of Nazism and questions abuse of personal information''(*Folha de S. Paulo*, 28 January 2022) <https://www1.folha.uol.com.br/mercado/2022/01/dia-da-protecao-de-dados-evoca-trauma-do-nazismo-e-questio-

The involvement of a variety of stakeholders into policy elaboration and implementation, in the context of a participatory multistakeholder governance[102] is, indeed, deeply rooted in the DNA of Brazilian digital policymaking[103], and has been baked into the new Brazilian data architecture, shaped by the LGPD. The multistakeholder council advising the ANPD board has a primarily consultative function and is only a supportive body rather than a decision-making one but enshrines the quintessentially Brazilian multistakeholder approach to digital governance.[104]

The Brazilian multistakeholder approach is epitomised by the country's Internet Steering Committee, more commonly referred to as CGI.br from its Portuguese denomination "Comitê Gestor da Internet no Brasil". CGI.br is the first example in history, of a multistakeholder body dedicated to Internet governance issues at the national level and is considered as an international benchmark of how such bodies should be structured. This acknowledgment is the result of its organisational features, enshrining a deeply participatory culture, rooted in the attempt to include all sectors of society, in a truly collaborative effort to provide high quality and diverse inputs to policymakers.

The mandate of the National Council for the Protection of Personal Data and Privacy is defined by article 58-B of LGPD, according to which the Council provides ANPD with suggestions, proposals and support based on

---

na-abuso-de-informacoes-pessoais.shtml> last accessed 1 January 2023; Luca Belli and Danilo Doneda, 'On the anniversary of the LGPD, Brazil needs to celebrate National Data Protection Day' (*Estadão* 13 August 2022) <https://www.estadao.com.br/politica/blog-do-fausto-macedo/no-aniversario-da-lgpd-brasil-precisa-comemorar-dia-nacional-da-protecao-de-dados/> accessed 1 January 2023.

[102] The interest to involve and consult stakeholders in policymaking has been globally acknowledged since the United Nations Conference on Environment and Development (UNCED), held in Rio de Janeiro, in 1992, when the Brazilian multistakeholder participatory culture was transplanted into the UN system. The final UNCED document, the Agenda 21, officially enshrined the need for policymakers to consult and strengthen the role of "major groups" of stakeholders. See <https://sustainabledevelopment.un.org/outcomedocuments/agenda21> accessed 1 January 2023.

[103] A fine example of how this plays out in practices is provided by the process of elaboration of Civil Rights Framework for the Internet, better known as Marco Civil da Internet (MCI), Federal Law n. 12.965 of 2014, considered a symbol of participatory democracy. The open process leading to the creation of the MCI included multiple open consultations, was initiated by the Center for Technology and Society of Fundaçao Getulio Vargas (CTS-FGV) and orchestrated jointly by Brazilian Ministry of Justice of Brazil, the Brazilian Internet Steering Committee (CGI.br) and CTS-FGV. *See*, Brazilian Internet Steering Committee (CGI.br), "Um pouco sobre o Marco Civil da Internet", April 20, 2014. Available at <http://bit.ly/2fQpL3E> accessed 1 January 2023.

[104] Luca Belli et al., 'Exploring Multistakeholder Internet Governance: Towards the Identification of a Model Advisory Body on Internet Policy'. (CyberBRICS, 3 April 2020) <https://cyberbrics.info/exploring-multistakeholder-internet-governance-towards-the-identification-of-a-model-advisory-body-on-internet-policy/> accessed 1 January 2020.

the inputs expressed by the various stakeholders represented in this body. Its aim is to elaborate on the National Data Protection Policy, the annual reports on the ANPD activities, while also promoting studies, debates, and public hearings to foster the establishment of a data protection culture within the Brazilian society.

This multistakeholder body is composed of 23 members: out of which 5 are appointed by the federal government, 2 by the Brazilian Congress (1 by the Federal Senate and 1 by the House of Representatives), 1 by the National Council of Justice, 1 by the National Council of Public Prosecutors, 1 by the Brazilian Internet Steering Committee, 3 chosen amongst representatives of non-governmental organisations, 3 from science and technology institutions, 3 from national business confederations, 2 from the private sector and 2 from unions and worker organisations.[105] Each stakeholder group defines autonomously the process utilised to nominate each candidate to the ANPD Board of Directors, which will choose the most suitable ones and submit the selection to the Presidency of Republic, who ultimately choses amongst the proposed nominees who will compose the Council.

The enthusiasm with the enormous potential of this multistakeholder council, however, must be tempered with a good dose of pragmatism. Having held its first meeting[106] only in November 2021, the National Council for the Protection of Personal Data and Privacy is in its early phase of implementation but, its activities have not received particular attention and even finding basic information about the activities of this body on the ANPD website is a remarkably challenging task. While it is still impossible to measure the impact that such multistakeholder body can have, especially at such an early phase of its experimentation, it is safe to argue that it represents one of the most innovative features, if not the most innovative, of the Brazilian data protection architecture. The Council has indeed the potential to act as a small xitong,[107] dedicated to personal data governance, thus creating a valuable forum for stakeholders to address shared concerns and identify shared solutions.

B. China

Until recently, it was often argued that China did not have a consistent mechanism for furthering data protection and privacy, and its data-related laws

[105] See General Data Protection Law 2018 art 58-A; For further information on the Council, see <https://www.gov.br/anpd/pt-br/cnpd-2> accessed 1 January 2023.

[106] The Council meetings' agenda can be consulted at <https://www.gov.br/anpd/pt-br/cnpd-2/reunioes-do-cnpd> accessed 1 January 2023.

[107] See (n 47).

adopted a sectoral approach – based on the US minimalist approach to data governance. However, the considerable policy updates introduced by China since the adoption of the Cyber Security Law, have created a robust regulatory system featuring several innovative elements, while still not being exempt from criticism. However, the new Chinese architecture deserves to be studied as "data governance and regulation with Chinese characteristics"[108] and has the potential to become a new alternative option to the existing minimalist US approach and maximalist EU approach.[109]

The normative framework developed by China since the entry in force of the Cyber Security Law (CSL) to regulate personal data processing stipulates that:

- data should be processed fairly and lawfully;
- the purpose of processing that data should be clearly specified to the individual;
- collected data should be up-to-date and accurate, to preserve data quality;
- the individuals should give their informed consent when data is collected and processed;
- individuals should be aware of their rights that must be communicated transparently to foster accountability.[110]

The traditional data protection principles – which can be found in Convention 108, the GDPR, the OECD Guidelines, etc. – have been introduced in Chinese data architecture not only as tools to regulate how data are processed and provide rights to individuals but, chiefly, as means to thus thwart threats to public security which could manifest through foreign intelligence espionage.[111] Importantly, in the context of China, the data protection field is inextricably linked to national security concerns. Over the past decade, China has pursued two intimately intertwined goals: on the one hand, the "informatisation" of the country, by expanding its digital infrastructures, technological capabilities, and IT productivity.

---

[108] See Belli, Chang, and Chen (n 51).

[109] See Jet Deng and Ken Dai, 'The Comparison Between China's PIPL And EU's GDPR: Practitioners' Perspective' (*Mondaq*, 19 October 2021) <https://www.mondaq.com/china/data-protection/1122748/the-comparison-between-china39s-pipl-and-eu39s-gdpr-practitioners39-perspective> accessed 1 January 2023.

[110] See Leplay (n 36) 63.

[111] ibid.

On the other hand, China has been keen on asserting its sovereignty on cyberspace, exerting control, and protecting from foreign threats its national digital assets, while developing solid cybersecurity governance. It is important to emphasise that the expansion and control over digital infrastructures as well as the use of technology to maintain social stability and detect potential threats are highest priorities for the Chinese government and have always been considered as complementary dimensions and pursued jointly. The high relevance of these goals and their interdependence have been tellingly highlighted by President Xi Jinping himself, stressing that "cybersecurity and informatisation are two wings of one bird, two wheels of one cart, we must uniformly plan, uniformly deploy, uniformly move forward, and uniformly implement matters."[112]

The strong cybersecurity component is indeed a key feature of the Chinese data architecture, emphasised since the 2012 decision of the National People's Congress to consider information security as an extension of public order and national security.[113] In this perspective, the Cybersecurity Law prescribes that the State is responsible for establishing and improving a system of cybersecurity standards,[114] including rules for a "graded protection of cybersecurity."[115] Moreover, by mandating that providers "explicitly stat[e] the purposes, means, and scope for collecting or using information, and

---

[112] See Rogier Creemers, 'Central Leading Group for Internet Security and Informatization Established' (China Copyright and Media, 1 March 2014). <https://chinacopyrightandmedia.wordpress.com/2014/03/01/central-leading-group-for-internet-security-and-informatization-established/> accessed 1 January 2023.

[113] ibid; Zhizheng Wang, 'Systematic Government Access to Private-Sector Data in China' (2012) 2(4) International Data Privacy Law 220, 221-224.

[114] Cybersecurity Law of China 2017, art 15.

[115] Cybersecurity Law of China 2017, art 21; The "graded protection of cybersecurity" refers to the Multi-Level Protection Scheme (MLPS), a concept which can be dated back to administrative rules from 1994 and 2007, and turned into a statutory obligation with the Cybersecurity Law's art 21, and reinforced by the 2022 Data Security Law's art 27 ("…in data processing by making use of the internet or any other information networks, the abovementioned data security obligations shall be fulfilled on the basis of the classified protection system for cyber security."). According to the MLPS scheme, information systems need to be graded on a range from 1 to 5, and network operators must apply the cybersecurity measures according to the system's grade. 'Cyber Security Law – Addressing the Compliance Complexities' (*PwC*, 30 November 2022), <https://www.pwc.de/en/international-markets/german-business-groups/china-business-group/cyber-security-law-addressing-the-compliance-complexities.html> accessed 1 January 2023. Furthermore, in May 2019, three national standards were issued by Chinese regulators: Information Security Technology - Baseline for Cybersecurity Classification Protection (GB/T 22239-2019), known as the "MLPS 2.0 Baseline", Information Security Technology - Technical Requirements of Security Design for Cybersecurity Classification Protection (GB/T 25070-2019); and Information Security Technology - Evaluation Requirements for Cybersecurity Classification Protection (GB/T 28448-2019). Together, they provide detailed and technical and administrative requirements on how to implement the MLPS. Li, B. 'China: MLPS 2.0 - Baseline Requirements and Practical Takeaways for Businesses' (*DataGuidance*, 22

obtain the consent of the users whose data is being collected"[116] the Chinese Cybersecurity Law achieves three simultaneous goals: it provides clear and foreseeable rules for businesses, it creates new rights for the Chinese population; and it enhances national security through sound cybersecurity and data governance.

Building on the bases set by the Cybersecurity Law, the Personal Information Security Specification of 2018 foresaw that it is obligatory to "disclose the scope, purpose, and rules for processing personal information in a clear and comprehensible manner and accept external oversight."[117] The introduction of the Specification was considered as necessary to fill many normative gaps, providing guidance on how to improve data subject awareness, corporate compliance, national oversight, and business good practices, setting new guidelines for personal data processing. It is also important to stress that, despite the non-binding status of specifications in the Chinese legal system, the Personal Information Security Specification must be seen as a cornerstone of the Chinese data regulation, as it supplemented legislation with technical standards that can be easily updated. In this perspective, shortly after the adoption of the Specification, the Chinese National Information Security Standardisation Technical Committee, a key standard-setting body typically referred to as "TC260",[118] started to update the specification to amend several requirements for personal information controllers in order to make them clearer and more easily implementable. On 6 March 2020, TC260 and the State Administration for Market Regulation issued the 2020 amended version (GB/T 35273-2020), which took effect on 1 October 2020.

The Specification provides guidance on the i) scope, ii) normative references, iii) terms and definitions iv) basic principles of personal information security, v) personal information collection, vi) personal information retention, vii) use of personal information, viii) rights of personal information subjects, ix) entrusted processing, sharing, transfer, and public disclosure of personal information, x) handling of personal information security incident, xi) and personal information security management requirements for organisations. Critically, the Specification adopts a remarkably didactic

August 2022) <https://www.dataguidance.com/opinion/china-mlps-20-baseline-requirements-and-practical> accessed 1 January 2023.

[116] See 'Cybersecurity Law of the People's Republic of China', art 41. <https://www.dataguidance.com/sites/default/files/en_cybersecurity_law_of_the_peoples_republic_of_china_1.pdf> last accessed 1 January 2023.

[117] Personal Information Security Specification, 2018, art 4e.

[118] The TC260 website can be accessed at: <https://www.tc260.org.cn/> accessed 1 January 2023.

approach[119], offering detailed instructions and concrete examples – especially in its appendix – illustrating how to comply with normative provisions. Notably, the Specification Annexes provide examples of what is to be considered personal information (annex A); a guide on how to identify sensitive personal information (Annex B); methods to safeguard independent choice of personal information subject (Annex C); and a model explaining how to draft a Personal information protection policy (Annex D).[120]

Importantly, the Chinese regulations, standards, and recent legislations lay considerable emphasis on consent. Thus, personal data cannot be collected or utilised without the express consent of individuals, unless legal provisions explicitly foresee so. This consideration is also reiterated by articles 25, 26 and 27 of the Personal Information Protection Law, which establish the obligation to obtain the informed consent of individuals before processing their data.

While this might sound peculiar to Western observers, generally suspicious of Chinese data protection practices, it is important to remind that, since the introduction of the CSL, consent has acquired an increasingly important role in the Chinese data architecture and has been further specified by several norms. Notably, Article 25 of the Personal Information Security Specification mentions that the personal information processor cannot disclose the information of an individual without their consent and in consonance with laws and administrative regulations.[121] Article 26 stipulates how image capturing can be used only for public security and, whenever this type of surveillance technology is used for any other purpose, the individual's consent must be obtained.[122] Article 27 stipulates that when processing individuals' personal information can have an adverse impact on their interests and rights, the same cannot be done without their consent.[123] Further, under Article 29, sensitive personal information – which include biometric information, health records, financial data, and any other information which if abused would infringe the dignity of individuals or cause harm to their person and property[124] – cannot be processed without the explicit consent of individuals.[125]

Another element worth notice is the remarkably antithetical approach the Chinese and Brazilian legislation adopt regarding financial records. Whereas

[119] Belli, Chang and Chen (n 51).
[120] Personal Information Security Specification, 2020, annex A, B, C, D.
[121] Protection of Personal Information Law 2021, art 25.
[122] Protection of Personal Information Law 2021, art 26.
[123] Protection of Personal Information Law 2021, art 27.
[124] Protection of Personal Information Law 2021, art 28.
[125] Protection of Personal Information Law 2021, art 29.

China considers such data as sensitive data, which require additional care to be processed only with the explicit consent of the data subject, the Brazilian framework does not consider such data as sensitive and allows collecting and processing them without consent via the highly questionable "protection to credit" legal basis, typically used by credit scoring bureaus, banks etc.[126] Clearly, the Chinese preference for stronger protection of financial data does not only reflect the stronger resistance of the Chinese legislators to the lobbying of the financial sector, but also the deeper understanding of the key relevance of financial records with regard to national sovereignty and digital sovereignty.[127]

Indeed, as mentioned above, the entire data architecture of China has been structured since its inception to adhere to the goal of maintaining national security. This brings in another dimension to this discussion: how the Chinese data governance system primarily targets private businesses and companies, while adopting a much more flexible stance towards the State, which is the fundamental guarantor of national security. Tellingly, article 28 of the Chinese constitution states that "all behaviours that endanger public order, public security and national security should be punished". This conception founds a particularly evident digital version in article 28 of the Cybersecurity Law, prescribing that "[n]etwork operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[128] Indeed, from a Chinese perspective it is acceptable that the State utilises personal information for surveillance purposes since public interest outweighs individual privacy. Interestingly, human rights in China are conceptualised as being derived from the state, which effectively places the interests of the State over that of an individual.[129] It is important to stress that the deregulation of personal data processing for public order and security purposes is not a Chinese peculiarity. An example in this sense is that the exemption of public safety and security activities from the application of general data protection frameworks is very common practices in all Latin America.[130]

It is also important to note that, while China has surely a more ample and flexible conception of state surveillance and its limits than most Western

---

[126] See s 2.1 of this paper.
[127] See (n 8).
[128] Cybersecurity Law of China, 2017, art 28.
[129] See Leplay (n 36).
[130] Lorena Abbas da Silva, Bruna Diniz Franqueira and Ivar A. Hartmann, 'What the Eyes don't See, the Cameras Monitor' (2021) 8(1) Digital Journal of Administrative Law 171, 204.

countries, the entry in force of PIPL has also regulated data collection from State institutions. PIPL makes a distinction between entities which process personal data in their private capacity and State institutions which deal with personal data for the purpose of public order or national security. Generally, article 73 of PIPL defines personal information handlers (i.e. processors) as: "organisations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods."[131] Moreover, Section III of the Act includes provisions stipulating the duties of public institutions.

For instance, Article 34 of the Act discusses how State organs processing personal information due to statutory duties should be within the ambit of laws and administrative regulations,[132] and should not process data in an excessive or arbitrary fashion. Similarly, Article 35 mentions that State organs which are dealing with personal information need to notify individuals implicated in that matter, except in cases "where laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary".[133] Moreover, Article 37 extends the specific regimes for State organs to any organisation processing personal information to fulfil statutory duties and "manage public affairs functions"[134] while article 61 defines the responsibilities of public departments dealing with personal information.[135]

The general principles which are usually applicable in the context of data protection and investigation can also be seen in some constitutional provisions and relevant regulations. Article 40 of the Chinese constitution mentions "freedom and confidentiality of correspondence of citizens of the People's Republic of China which shall be protected by law." The important exemption to this provision rests in a necessity for national security or criminal investigation wherein it is imperative to access correspondence of individuals by public prosecution organs. However, such an examination cannot be in violation of laws.[136] Hence, it can be construed that the scrutiny of private correspondence will have to adhere to provisions of the Personal Information Protection law.

Lastly, it is relevant to mention that the *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases*

[131] Personal Information Protection Law 2021, art 73.
[132] Personal Information Protection Law 2021, art 34.
[133] Personal Information Protection Law 2021, arts 35 and 18.
[134] Personal Information Protection Law 2021, art 37.
[135] Personal Information Protection Law 2021, art 61.
[136] Constitution of the People's Republic of China 1982, art 40.

Involving Infringement on Citizens' Personal Information prescribes the need to legally protect the rights of citizens and their personal information utilised for the purposes of investigations in criminal cases.[137] The *Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases* also aim to protect "state secrets, police work secrets, trade secrets, individual privacy, and confidentiality" while collecting and processing forensic electronic data.[138]

i. Data Security with Chinese Characteristics

As mentioned above, the cybersecurity component is particularly relevant in Chinese data governance and can be seen as one of the most relevant features – if not the most – of the new data architecture of China. Particularly, the country has enacted its new Data Security Law in 2021 which seeks to strengthen provisions pertaining to cybersecurity of several categories of data.[139] The law defines more stringent requirements for processing 'important data'[140] and 'core state data'[141] extending to all automated data-processing of these categories of data the obligation to comply with the

---

[137] Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement on Citizens' Personal Information, 2017.

[138] Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases, 2019, art 4.

[139] See the unofficial English version of China's Data Security Law: <https://www.cov.com/-/media/files/corporate/publications/file_repository/data-security-law-bilingual.pdf> accessed 1 January 2023.

[140] Article 21 of the DSL prescribes that "[e]ach region and department, shall stipulate a regional, departmental, as well as relevant industrial and sectoral important data specified catalogue, according to the data categorization." Important data listed in such catalogues may encompass an enormous spectrum of data linked to economic development, national security, the public interest, individuals' rights, and corporates' interests. Such important data are subject to special security requirements as well as international transfer restrictions Appendix A of the Draft Guidelines for Cross-Border Data Transfer Security Assessments provides a detailed list of "important data" in different sectors. For instance, in the military sector, "important data" encompass information on the name, quantity, source and agent of purchased components, software, materials, industrial control equipment test instruments, geographical location, construction plans, security planning, secrecy level, plant drawings, storage volume, reserves of military research, and production institutions. See <https://www.cac.gov.cn/2021-10/29/c_1637102874600858.html> accessed 1 January 2023.

[141] Art. 21 of DSL has introduced the concept of "core state data" that are defined as "data concerning national security, lifelines of the national economy, important aspects of people's lives, major public interests, etc." For such data a stricter management system shall be implemented. Illegal transfer of national core data outside of the country is subject to a fine of up to RMB10 million, and other sanctions, such as the revocation of licences, and may even trigger criminal liabilities in the most severe cases.

notorious Multi-Level Protection Scheme (MLPS)[142] mandated by the 2017 Cybersecurity Law.[143]

Hence the Data Security Law can be seen as an extension of the Cybersecurity Law of 2017, which provided far-reaching mechanisms for data protection and cybersecurity in the country. Indeed, for the Chinese State, cybersecurity is an essential facet of national security[144] and the introduction of the Data Security Law can be deemed as one of the most relevant elements of the new data architecture of China. The Law is based on the Chinse conceptualisation of information security, which is deemed as an essential tool to preserve and guarantee the stability and sustainability of the Chinese State, Communist Party, and nation.

The Cybersecurity Law of 2017, coupled with the Personal Information Security Specification, already provided mechanisms for protecting personal data as well as provisions allowing to sanction – not only with fines but also with imprisonment – critical information operators in case of violations.[145] Further, the Cybersecurity Law also broadened the ambit of cybercrimes to include managerial negligence by network operators.[146] Additionally, the Cybersecurity Law also focused on the preservation of "public order" online, establishing several measures in this sense. One of the most relevant measures in this regard is the establishment of an emergency monitoring and response information communication system and the possibility to shut down Internet connectivity in emergency circumstances for protecting national security and social public order.

At the same time, the law mandates real-name registration policies and self-regulation by network operators.[147] Conspicuously, the cybersecurity domain is under the remit of the Cyberspace Administration of China, the

---

[142] The MLPS is a cybersecurity compliance scheme that applies to virtually all organisations in China. It was first introduced in 1994 and subsequently updated in 2019, in accordance with Article 21 of the Cybersecurity Law. The MLPS classifies systems based on the damage that a hypothetical vulnerability of the system may pose to China's cybersecurity. The scheme requires all network operators to ensure that their networks are protected against interference, damage, or unauthorised access. Under MLPS, all network operators are required to classify their infrastructure and application systems on a 1 to 5 scale, and fulfil protection obligations accordingly. Systems ranked at 3 or higher are considered higher-stake, and are subject to notably stricter obligations, including on data security. See <https://www.protiviti.com/HK-en/insights/pov-multiple-level-protection-scheme> accessed 1 January 2023. Jiang

[143] For a detailed explanation of the Multi-Level Protection Scheme, see <http://lawinfochina.com/display.aspx?id=22826&lib=law> accessed 1 January 2023.

[144] See Jiang (n 38) 183-226.

[145] ibid.

[146] ibid.

[147] ibid.

national regulator for digital matters, with the primary function of oversight. Importantly, the regulator is accountable to the Central Cyberspace Affairs Commission, which is an inter-ministerial government body, headed by President Xi and composed of Chinese leaders at the highest level.[148]

The Data Security Law of 2021 specifically focuses on data security but also incorporates principles of data protection like confidentiality and privacy in its provisions. The first article of the law delineates the principles which the law seeks to uphold – primarily, state security and sovereignty, protection of lawful rights and interests, and development of the Chinese economy and society.[149] Critically, the law has extra-territorial application as well, a deviation from the 2017 Cybersecurity Law, which did not include such broad scope. In fact, article 2 of the Data Security Law stipulates that if data handling activities outside the territory of China harm the national interests of China or the lawful rights and interests of Chinese citizens, then legal responsibility would be imposed.[150]

Furthermore, Article 4 mentions how "the preservation of data security shall adhere to the overall national security perspective, establish and complete data security governance systems, and increase capacity to ensure data security."[151] Additionally, the law places the Central Leading Institution on National Security as the decision-making body which formulates and implements different policies pertaining to cyber security and coordinates work on national data security.[152] The law establishes that *inter alia* public and state security organs have to undertake data security regulation duties. State internet information departments are responsible for coordinating online data security and other regulatory efforts in consonance with this legislation, other relevant laws (which now include also the PIPL), and administrative regulations.[153]

Article 10 prescribes that relevant industry organisations must draft data security conduct specifications and standards that adhere to law and help strengthening industry self-discipline. Further, these specifications should guide members of such organisations to make data protection mechanisms robust, while promoting a conducive and healthy environment for the development of industries.[154] Relevant industries must also ensure confidentiality

---

[148] ibid.
[149] Data Security Law 2021, art 1.
[150] Data Security Law 2021, art 2.
[151] Data Security Law 2021, art 4.
[152] Data Security Law 2021, art 5.
[153] Data Security Law 2021, art 6.
[154] Data Security Law 2021, art 10.

of complainants and informants to protect their lawful rights and interests.[155] Furthermore, Article 17 of the Law requires the development of standards for data exploitation technologies in furtherance of data security. These standards must be approved by the State Council Departments which oversee each specific approval process.

Moreover, these departments should also organize formulation and appropriate revision of standards, to make sure they are continuously updated and improved, considering the latest technological and policy developments. To facilitate the emergence of well-structured and harmonious self-regulation, the State is tasked with the encouragement and support of enterprises, consortia, research bodies etc. which participate in the exercise of drafting data security standards.[156] The State also has the duty of promoting the development of services, such as data security testing and certification. They must also support institutions which are providing these services which are deemed as instrumental to foster a sound data security environment.[157]

The law places an obligation on the State to develop a categorical and hierarchical system pertaining to data protection, categorising data, and defining category-based requirements and protections. This taxonomy and hierarchisation should be based on the perceived importance of the specific type of data, especially in the context of social and economic development, extent of harm of national security, public interest, extent of harm to the lawful rights and interests of the citizens if the collected data is altered, destroyed or illegally used.[158] The ambit of core state data is said to constitute data pertaining to national security, national economy, people's livelihoods, and major public interests. However, the Law does not stipulate what constitutes a major public interest or what is the distinction between public interest and major public interest, so we may assume this will be defined by future regulation.

Further, each regional administration also has the discretion to define what constitutes important data in the regional context.[159] The law also mandates that the State establish a data security emergency response and handling system. In this context, each relevant governmental department will have to initiate emergency response plans which would be utilised during data security incidents. This would help diminish the harm which could

[155] Data Security Law 2021, art 12.
[156] Data Security Law 2021, art 17.
[157] Data Security Law 2021, art 18.
[158] See (n 108).
[159] Data Security Law 2021, art 21.

be caused from security risks while issuing alerts to the public.[160] This should be accompanied with data security reviews at the national level which would help in revisiting security review decisions.[161]

Interestingly, the law includes a so-called 'sovereignty clause' The clause provides protections and retaliatory tools in case any foreign country or supranational organisation – such as the EU – were to make use of discriminatory, restrictive, or similar measures against China. The sovereignty clause concerns specifically the areas of investment or trade in data, technology for exploitation and development of data and empowers the Chinses government to utilise similar retaliatory measures against hostile country or organisation.[162]

Importantly, Article 29 of the Law stipulates the procedure which must be followed for handling data security threats and other relevant activities. For instance, when data security vulnerabilities would be found, measures to remedy the situation must be immediately carried out. Simultaneously, users would be notified and reports would be sent to relevant regulatory departments.[163] Moreover, Article 30 stipulates what elements must be included in the risk assessment reports, such as, the type and amount of important data being handled, circumstances of data handling activities, data risks faced, methods for addressing the risks and relevant concerns.[164]

Lastly, it is important to remember that data protection principles as stipulated in Article 7 of PIPL are also reflected in the provisions of the Data Security Law. For instance, Article 32 of the Data Security Law mentions how organisations or individuals collecting data should do so in a lawful manner and avoid obtaining data through illegal means. Further, data must be used for a specified purpose only, according to the normative frameworks defined in relevant laws and administrative regulations.[165] The Data Security Law also imposes an explicit duty on public and state security organs, which collect data to preserve national security or to investigate crimes, to follow appropriate provisions and stringent approval formalities.[166]

In addition, State organs which are collecting data within the ambit of their legally prescribed duties need to do so within the requirements of said

---

[160] Data Security Law 2021, art 23.
[161] Data Security Law 2021, art 24.
[162] Data Security Law 2021, art 26.
[163] Data Security Law 2021, art 29.
[164] Data Security Law 2021, art 30.
[165] Data Security Law 2021, art 32.
[166] Data Security Law 2021, art 35.

legal duties, laws and administrative regulations.[167] Particularly, Article 41 posits how even State organs need to follow data protection principles of justness, fairness, while disclosing government affairs data. Moreover, State organs which are entrusting other institutions to establish or maintain electronic government affairs systems, or store and process government affairs data must follow strict approval procedures. These State organs would be responsible for supervising the work of the institutions to which it has delegated some of its functions. These institutions cannot store, use, leak or provide government affairs data to third parties without the State organ's authorisation.[168]

Apart from stipulating that the State should have a transparent platform for disclosing data related to government affairs,[169] the Law also posits that should State organs fail to perform their duties, the managers and personnel directly responsible for such failure will be subject to sanctions.[170] Further, the state personnel who derelict their duties, abuse their authority or try to use the law for personal gains would be sanctioned as per law.[171] The law also envisages civil and criminal liability apart from public security administrative sanctions for violations of the statutory provisions under the Act.[172]

C. India

The current Indian data protection framework is primarily shaped by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ('SPDI Rules') notified under the Information Technology Act, 2000 ('IT Act'), together with the sectorial laws mentioned in section 1.[173] The Data Protection Rules impose certain obligations and compliance requirements on organisations that collect, process, store and transfer sensitive personal data or information of

[167] Data Security Law 2021, art 38.
[168] Data Security Law 2021, art 40.
[169] Data Security Law 2021, art 42.
[170] Data Security Law 2021, art 49.
[171] Data Security Law 2021, art 50.
[172] Data Security Law 2021, art 52.
[173] Besides the SPDI Rules, sectorial laws include the Information Technology Act, 2000 (IT Act); the Consumer Protection Act, 2019 (CPA) and Consumer Protection (E-Commerce) Rules 2020; the rules issued by the Reserve Bank of India; the rules imposed by the Telecom Regulatory Authority of India; the rules imposed by the Insurance Regulatory and Development Authority of India; the rules imposed by the Securities and Exchange Board of India; the Unified Licence Agreements issued pursuant to the National Telecom Policy, 2012 by the Department of Telecommunications; and various decisions of Indian courts. See 'India: Data Protection Overview' (Data Guidance November 2022) <https://www.dataguidance.com/notes/india-data-protection-overview> accessed 1 January 2023.

individuals such as obtaining consent, publishing a privacy policy, responding to requests from individuals, disclosure, and transfer restrictions.

The Data Protection Rules further provide for the implementation of certain reasonable security practices and procedures ('RSPPs') by organizations dealing with sensitive personal data or information of individuals. The Data Protection Rules provide as follows:

- Organizations may demonstrate compliance with the RSPP requirement via implementing security practices and procedures and having a documented information security programme and information security policies. These information security policies must contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected.
- The international standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System – Requirements" is prescribed as one such standard that would help demonstrate compliance with the RSPP requirement.
- Codes of conduct elaborated by any organisation as a self-regulatory tool must be notified to and approved by the Central Government; and
- Organisations who have implemented standards according to the abovementioned options would be deemed compliant with the requirement to implement RSPPs upon having audits performed periodically by independent Government-empanelled auditors.

In addition, much like the General Data Protection regulation (GDPR), and in line with the Puttaswamy decision, the Data Protection Bill provides for a consent-based approach while processing data, which is also necessary to process sensitive personal data. In the absence of consent, the Bill also provides for the following grounds of processing:

- For the necessary functioning of the State, the Parliament, or State Legislatures.
- To comply with orders or judgments of courts or tribunals.
- For purposes related to employment.
- For prompt action, such as in events of medical emergencies, disasters, and breakdowns of law and order; and
- For reasonable purposes, such as whistleblowing, mergers and acquisitions, credit scoring, debt recovery, etc.

As regards the processing of sensitive data, the Information Technology SPDI Rules, 2011 prescribe that consent is the primary form of processing data. Importantly, the nature of consent is defined by Rule 5(1), SPDI, but this standard has been frequently criticised for being too vague and requiring further clarification through contract law.[174] Hence, businesses commonly rely on general principles of contract law to determine how, when, and through which means consent ought to be obtained. If consent is obtained freely and without undue influence, then there are few limitations on the process and method of obtaining consent. However, if such consent is obtained by virtue of a standard form contract, then the terms of the contract must be reasonable.

Under the SPDI Rules, the provider of data should have an option to opt out of providing the data or information that is being sought by body corporates.[175] Providers of information should always have this option, while availing themselves of services from body corporates, as well as have an option to withdraw consent that may have been given earlier.[176] Importantly, unlike many other jurisdictions, should providers not consent to the collection of information or otherwise withdraw their consent, the SPDI Rules allow body corporates not to provide goods or services for which the information was sought.[177] In addition to the right to opt out of sharing information, information providers have the right to review the information they have provided and to seek the correction or amendment of such information if incorrect.[178]

i. The Personal Data Protection Bill 2021, the Digital Personal Data Protection Bill 2022, and a New Bill with Consultation in 2023

As noted above, the Personal Data Protection Bill 2021 played a particularly relevant role as it reframed the Indian data architecture in a comprehensive fashion. However, the recent introduction of the Digital Personal Data Protection (DPDP) Bill 2022, in its consultation period, and the relatively upcoming presentation of new – likely final version – for a new consultation in 2023 lead observers to be quite disappointed with a the very lengthy and time-consuming consultation process. In this perspective, to date it is not possible to be sure about what will be the final outlook of the Indian data

[174] See Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
[175] See SPDI Rules 2011, r 5(7).
[176] ibid.
[177] ibid.
[178] See SPDI Rules, 2011, r 5(6).

protection law, but it is possible to identify the main elements and characteristic of the future Indian framework.

Interestingly, the Indian legislator seems to have taken inspiration from the Chinese neighbour, as regards the need to couple its normative framework with a didactic approach, introducing 'illustrations' aimed at exemplifying concepts that might be new for Indian stakeholder. This is indeed a very useful technique explored by the Chinese legislator by annexing examples to the regulatory standards, such as the Personal Information Security Specification, which proves to be extremely useful to facilitate compliance.[179] Consent is the primary legal basis for processing personal data under the Bills and, to be valid, it must be free (that is, free from coercion, undue influence, fraud, misrepresentation, or mistakes), informed, specific, clear, and capable of being withdrawn.[180] Further, the Bill clarifies that provision of goods or services, or their quality, the performance of a contract, or the enjoyment of a legal right or claim cannot be conditional on consent for processing of personal data that is necessary.[181]

Hence, the Bill allows personal data to be processed in the absence of consent under certain legal grounds.[182] First, such processing grounds include the performance of certain State functions, such as public service or benefit provision, which are not listed exhaustively. Other legitimate bases for processing include compliance with law or court order, medical emergencies, force majeure, or preservation of public order.[183] Importantly, DPDP Bill 2022 clauses 8(6), (7), and (8) foresee that consent for data processing will be deemed as lawfully obtained in situations including for the maintenance of public order, purposes related to employment, and in public interest respectively. These lawful bases have been unanimously criticised by observers for their vagueness, which can allow for unlimited data processing in the absence of the data principal specific and informed consent.[184]

Other legally admitted purposes are fraud detection and prevention, whistle blowing, mergers and acquisitions or other corporate restructuring transactions, network and information security, credit scoring, recovery of debt, processing of publicly available personal data and the operation of search

---

[179] See s 2.2.

[180] Personal Data Protection Bill 2021, s 11; Digital Personal Data Protection Bill 2021, s 7

[181] Personal Data Protection Bill 2021, s 11(4); Digital Personal Data Protection Bill 2021, s 7(4).

[182] Personal Data Protection Bill 2021, s 12; Digital Personal Data Protection Bill 2021, s 8.

[183] ibid.

[184] See e.g., Sarvesh Mathi, 'State Surveillance, Reduced Obligations, and Eight other Issues with the 2022 Data Protection Bill: IFF' (*Medianama* 21 November 2022).

engines.[185] While the PDP Bill 2021 prescribed that these latter grounds for reasonable processing needed to be specified by regulations, the DPDP Bill 2022 has withdrawn such requirement. Moreover, like its predecessors, the 2022 version of the proposed framework states that, when seeking consent, data fiduciaries must present a notice to users describing what data is collected and for what purposes but, unlike the previous iterations, the DPDP Bill 2022 does not require data fiduciaries to inform principals about what third-parties data are shared with, nor the duration for which data will be stored and whether data will be transferred outside Indian borders.

The PDB Bill 2021 systematised the principles that govern the processing of personal data by any person, which are: i) fair and reasonable processing, that respects the privacy of the data subject;[186] ii) purpose limitation, meaning that the purposes are clear, specific and lawful, although incidental purposes that the data subject would 'reasonably expect the data to be used for' are allowed as well;[187] iii) data minimisation, meaning that only data that is necessary for the purpose of processing should be collected;[188] iv) transparency regarding information on the data processing and data rights provided by the data fiduciary to the data principal at the time of the collection of the personal data;[189] v) data quality, prescribing the adoption of all necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed;[190] vi) necessity, according to which the fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing;[191] vii) accountability, according to which the data fiduciary is responsible for complying with the bill and the rules and regulations made there under;[192] viii) necessity of consent of the principal for the commencement of data processing.[193] Such useful systematisation has been removed by the DPDP Bill 2022 but, given the core relevance of the explicit definition of data protection principles in virtually all existing data protection frameworks, it seems reasonable to expect that they will be reintroduced in the future version of the Bill.

---

[185] Personal Data Protection Bill 2021, s 14; Digital Personal Data Protection Bill 2021, s 8(8).
[186] Personal Data Protection Bill 2021, s 5(a)
[187] Personal Data Protection Bill 2021, s 5(b).
[188] Personal Data Protection Bill 2021, s 6.
[189] Personal Data Protection Bill 2021, s 7.
[190] Personal Data Protection Bill 2021, s 8.
[191] Personal Data Protection Bill 2021, s 9.
[192] Personal Data Protection Bill 2021, s 10.
[193] Personal Data Protection Bill 2021, s 11.

Importantly, the Bill applies to the processing of personal data, where such data has been collected, disclosed, shared, or otherwise processed within India, as well as personal data by the State, companies or any person or body of persons created under Indian law, as long as the processing is digital.[194] It also includes the processing of personal data outside Indian territory if it is connected to any Indian business or systematic activity or if it involves profiling of data principals within the territory of India.[195] However, the Indian data regulation is not applicable to: non-automated and offline processing, personal data processed by an individual for any personal or domestic purpose, and "personal data about an individual that is contained in a record that has been in existence for at least 100 years."[196] and does not cover the processing of non-personal data as its predecessor did.[197]

As its predecessors, the DPDP Bill also includes exceptions for law enforcement agencies allowing the central government to exempt any public body from the application of the Bill on grounds like the national security and public order, and largely undefined purposes such as "interests of sovereignty and integrity of India" and "friendly relations with foreign States."[198]

Lastly, it is essential to emphasise that, should they be maintained in the final version of the law, the inclusion of very broad exceptions to the application of the Bill, and the lack of an independent Data protection Regulator have the potential to strongly undermine the very rational of the new Indian framework. Indeed, besides conferring enormous leverage to the Union Government as regards when the law should be applied, clause 19(3) of the current Bill foresees that the Chief Executive of the Data Protection Board of India will be appointed by the Union Government, which will also define the "terms and conditions of her service." Such a configuration may hardly be considered as independent and it is likely to create considerable governmental influence. To shape an independent Board, India should look at fellow BRICS country South Africa which stands out internationally for having designed a procedure aimed not only at identifying competent individuals as members of the Information Regulator's Board, but also at guaranteeing an open, democratic and transparent appointment process, prescribing that the South African Parliament shall issue an open Call for Applications or Nominations.[199]

---

[194] Digital Personal Data Protection Bill 2022, s 4(1).
[195] Digital Personal Data Protection Bill 2022, s 4(2).
[196] Digital Personal Data Protection Bill 2022, s 4(3).
[197] Personal Data Protection Bill 2021, s 2(d).
[198] Digital Personal Data Protection Bill 2022, s 18(2).
[199] Belli and Doneda, 'Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence' (n 6).

ii. The Data Empowerment and Protection Architecture

As mentioned in section 1, in August 2020, NITI Aayog released a draft framework on the Data Empowerment and Protection Architecture ('DEPA') with the aim to institute a mechanism for secure consent-based data sharing in the fintech sector.[200] While the proposed Indian framework is much more complex than the mere DEPA, this important element deserves particular attention, as it represents not only one of the core novelties of the new Indian Architecture, but also one of the few innovative elements which have already been adopted and in phase of implementation.

DEPA is a system of digital consent management, constituted by a set of protocols, which have been operationalised across sectors. Finance was the first sector to concretely implement the DEPA introducing the "Account Aggregator" model, in 2020, under the joint leadership of the Ministry of Finance, the Reserve Bank of India (RBI), Pension Fund Regulatory and Development Authority (PFRDA), Insurance Regulatory and Development Authority (IRDAI), and Securities and Exchange Board of India (SEBI). This system enables individuals to share their financial data across banks, insurers, lenders, mutual fund houses, investors, tax collectors, and pension funds in a supposedly secure manner. While the document released by NITI Aayog is focused on the implementation of DEPA in the financial sector alone, DEPA is also proposed to be introduced as a similar framework beyond just financial data, and across all sectors, beginning with the health and telecom sectors.

Importantly DEPA needs to be considered in the context of the Digital India programme[201], launched by the Indian Government in 2015, to foster a radical digital transformation of the country. The three main pillars of Digital India are connectivity, eGovernment, and the establishment of a Digital Public Infrastructure. This last pillar is fundamental to understand DEPA as well as the Indian government vision consisting in the development of technology to implement regulation. Indeed, the Digital Public Infrastructure is a set of Application Programming Interfaces (APIs)[202] commonly referred to as the 'Indian Stack'[203] which the Indian Government sees

---

The most recent call for Applications or Nominations issued by the South African Parliament is available at <https://www.parliament.gov.za/press-releases/media-statement-justice-and-correctional-services-committee-calls-nominations-information-regulator> accessed 1 January 2023.

[200] See NITI Aayog (n 82).

[201] Digital India, available at <https://www.digitalindia.gov.in/> accessed 8 October 2021.

[202] An API is a piece of software that allows different software applications to interact and exchange data, according to the specifications established by the API.

[203] See <https://www.indiastack.org/> accessed 1 January 2023.

as instrumental to achieve digital transformation through the development of digital public goods.[204] The India Stack is composed of multiple layers and DEPA fits into the so-called 'consent layer' of the architecture. In this context, DEPA is supposed to be one of such digital public goods having been presented as a "secure consent-based data sharing framework to accelerate financial inclusion [based on] an evolvable regulatory, institutional, and technology design for secure data sharing [which] empower individuals with control over their personal data."[205]

The DEPA Framework represents an evolution of Privacy by Design from being passive to active. This approach aimed at backing regulation into technology is probably the most ambitious and characteristic trait of the new Indian data architecture, aspiring to give 1.3 billion Indians control of their data, and it progressed with three pillars.[206] DEPA's underlying technology is designed on open standards and open protocols. These standards establish technical rules to frame concepts like consent and define consent itself, informed consent, and how to revoke, provide, and make consent granular. Indeed, DEPA is particularly interesting as its goal is to encode many of the legal principles that frame informed consent.

It is important to clarify how users concretely express consent with DEPA. The Account Aggregator (AA) framework is a consent manager for financial data. A consent manager[207] may exist for a variety of data, like health or telecom. This is the real institutional innovation that India has come up with. These fiduciaries exist in the Indian technical and legal ecosystem today, where the user may discover where their data resides. Data are stored in a decentralised manner and the identity behind it is also federated, with no unique ID creation unless the user decides to collate data and create one.

There is no use of even Aadhar in the entire architecture. The user has a choice to facilitate the flow of data. As such the goal of the Indian

---

[204] Importantly, such vision is not exempted from critique, notably considering that India Stack has been essentially designed by iSPIRT (the Indian Software Products Industry Round Table), a think tank for the Indian software products industry which has been criticized for its close ties with both government and large corporations, raising concerns related to conflict of interests, transparency and accountability.

[205] See NITI Aayog (n 82) 26-27.

[206] Nandan Nilekani, 'How To Empower 1.3 Billion Citizens With Their Data' (iSPIRT.in, 6 August 2018) <https://pn.ispirt.in/empowercitizenswiththierdata/> accessed 1 January 2023.

[207] Consistently with the previous definition provided by sec 3(11) of the PDP Bill 2021, the DPDP Bill 2022 defines the consent manager as "a Data Fiduciary which enables a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform." See Digital Personal Data Protection Bill 2022, sec7(6).

architecture is to shift from data protection to data empowerment, using technology as a vector of regulation. The second is a shift from a purely legal approach (resulting in market failures) towards a techno-legal approach. The third is a shift from each nation-state taking a siloed approach that has created jurisdictional arbitrage by different companies, much like in the world of taxation, to the need to take a coordinated approach using coordinated technology protocols while allowing for regulatory extensions that are local to each country.

The principles underlying the entire consent model are called ORGANS, which is the acronym of Open standard, Revocable, Granular consent, Auditable, Notice, and Security of consent. These principles form the foundation of India's data protection bill as well. Once the Bill will be passed, it will extend the system to many other data categories from the ones already framed such as financial and health data to others like e-commerce and social media data. Importantly, DEPA is conceived to be double-blind, a feature that allows segregation of consent and data flows. To give this powerful feature some perspective, we note that the data travels paths with stops – consent, authorisation, transfer, etc., and actors holding these stops are unaware of each other.

Hence, DEPA can be built in a way where the information requester and provider are unaware of each other's identities. The middleman, the consent manager, also has no information on the data passing through. This double-blind standard aims at providing strong confidentiality and is used in clinical trials. It essentially puts a third, anonymous person in charge of constructing confidentiality taking consent away from the purview of the two principles or the file transfer protocol. For these reasons, DEPA has the potential to become one of the single most revolutionary elements of the Indian data architecture. However, a certain degree of caution and scepticism is also needed as DEPA is far from maturity and the potential pitfalls, vulnerabilities, and negative externalities that such system may deploy are still unknown and, likely, strongly underappreciated.[208]

III. Conclusion: The Emergence of a Post-Western Model of Data Governance

This paper has explored the recent data protection evolutions in Brazil, China, and India to highlight the complexity of their systems, while focusing

[208] For an interesting review of DEPA, the benefits it brings, and its potential pitfalls, see Vikas Kathuria, 'Data Empowerment and Protection Architecture: Concept and Assessment' (ORF Issue Brief No. 487, Observer Research Foundation August 2021).

on some of their most salient features that will, likely, become core elements of the most innovative approaches to data protection. Having developed their data architectures very recently, these countries have benefited from existing knowledge and experiences regarding data protection at the global level but have also managed to bake into their new data architectures some key features of their national identities.

It is important to reiterate that, in light of their relevance, these countries are likely to become not only regional but global leaders in data regulation, and their national innovations may become core elements of what could be defined as new post-Western approach to data governance. This represents a credible alternative to the traditional dichotomy between a minimalist US approach and maximalist EU approach. As argued in the introduction of this paper, the US approach suffer from an excessively laissez-faire approach, which has led an increasingly absolute majority of countries (currently 145 countries[209]) to adopt data protection laws de facto preferring a European approach based on comprehensive regulation. However, the European approach is not exempt from criticism, giving rise to a particularly complex and burdensome compliance, while simultaneously failing to tackle major data protection and data security problems and create effective protections for individuals.

The post-Western model that this paper argues is taking shape thanks to Brazilian, Chinese, and Indian innovations may be helpful to cope with the aforementioned problems, especially for Global South countries in need of pragmatic solutions. Involving and coordinating a variety of stakeholders into policymaking, strengthening cybersecurity governance, and going beyond a mere normative approach, betting on open-source privacy enhancing technologies, seem to be essential steps to build meaningful data protection. It is also necessary, however, to maintain a pragmatic pasture also regarding the definition of necessary checks and balances that need to be defined to frame or overview multistakeholder bodies, cybersecurity processes and technologies alike.

This article has strived to present in a succinct and objective fashion the complex and numerous traits of the new Brazilian, Chinese, and Indian data architectures, focusing primarily on their innovative elements. The main purpose of this document is indeed to allow the user to understand both the complexity of such architectures and the value of their innovative elements. The incredible economic and geopolitical relevance of these countries makes

[209] Graham Greenleaf, 'Global Tables of Data Privacy Laws and Bills', (7th edn, Privacy Laws & Business International Report 11 February 2021).

them suitable candidates to become likely examples for their neighbours and trade partners in search for inspiration, when designing new data protection systems. Such inspiration becomes even more pressing, when considering the extraterritorial scope of the new data framework of Brazil, China, and India, which *de facto* obliges all potential partners to adapt to their frameworks.

Importantly, the elements of novelty that these countries have included into their data architectures reflect concerns and sensitivities that are likely to become extremely relevant for many other countries, well beyond the Global South. The participation of a multiplicity of stakeholders with diverse backgrounds into the activities of the data protection regulator has the potential to increase considerably, the quality of the regulation and of the regulator. The Brazilian experience will serve as a useful pilot to test how such multistakeholder governance can be integrated in the most effective way within personal data regulation. The definition of sound data security frameworks is one of the most pressing and needed issues, which most countries are struggling to achieve. The Chinese approach is likely to become a global reference and, possibly, a model for most countries, currently struggling to cope with mounting cyberthreats, endemic lack of data security, and astronomic number of data breaches.[210] Moreover, the Chinese approach is likely to trigger increasing interest, or even necessity of harmonisation, from its trade partners, as the Asian giant continuously expand it Belt and Road Initiative, thus triggering a new type of 'Beijing effect'.[211]

The awareness of the regulatory value of technology and the willingness to promote technological tools to provide concrete implementation to data protection norms is a ground-breaking advancement. However, the fact that technology can be used – and is used – as a tool of regulation does not mean that this is exempt from risk or should not require the same or even stronger rule-of-law and due process guarantees foreseen for traditional forms of regulation. The Indian experience, while still in its early phase, represents one of the most interesting and large-scale experiments in data privacy by design ever conducted and the success or failure of such experiment have the potential to reshape data protection and the use of technology for regulatory purposes well beyond Indian borders.

---

[210] According to cybersecurity research firm Identity Theft Resource Center, "the number of 2021 data compromises is 23 per cent over the previous all-time high". See Identity Theft Resource Center, *Data Breach Annual Report 2021 in Review* (January 2022); See also 'Data Breaches Rise Globally in Q3 of 2022' (*Surfshark* 19 October 2022). <https://surfshark.com/blog/data-breach-statistics-2022-q3> accessed 1 January 2023.

[211] See Erie and Streinz (n 61); Belli, Chang and Chen (n 51).

Ultimately, the new data architectures introduced by these three very different giants will play a crucial role in the evolution of data governance at the global level. In this perspective, understanding the countries' background, innovations and aspirations becomes essential to foresee new trends in some of the most relevant (emerging) economies in the world, as well as to grasp how a post-Western data architecture may reasonably look like. What can already be stated with reasonable certainty is that, while not a silver bullet, the core elements of the post-Western model of data governance, combining increased multistakeholder participation, sound data security, and the use of technology to effectively regulate data protection, are likely to considerably increase the maturity – and hopefully the quality – of data protection frameworks of any country.