RINGFENCING DATA? – PERSPECTIVES ON SOVEREIGNTY AND LOCALISATION FROM INDIA

Sai Ramani Garimella

Assistant Professor, Faculty of Legal Studies, South Asian University, New Delhi, India ramani@sau.ac.in

Parthiban B,

Research Student, Faculty of Legal Studies, South Asian University, New Delhi, India.

Abstract

Governance of data, essentially a free-flowing product of the industrial (technology-driven) revolution 4.0, has been the subject of much discussion and policy action amongst States. Such governance, however, has presented questions turning the traditional understanding of the right to regulate, which is based on the geographic location, heads down, given that it is difficult to establish the location of data, and therefore the linkages with the territory. On the other hand, concerns remain with regard to the privacy-related issues of the data, either located or handled overseas, thereby presenting difficulties in access and administration of data. This research addresses the model of governance of data via the path of data sovereignty and, therefore, insistence on data localisation. It further presents the law in India, sparse as it is, through the lens of jurisprudence and law reform efforts, wherein the eagerness to ringfence the data is evident, even in disregard of the contractual obligations.

Introduction

"Therefore, as at present, we deem it apposite to confine our focus on ensuring that there is no breach of confidentiality of the data collected by the State and processed by Sprinklr, and since we are not in a position to conclusively persuade ourselves that the terms of the impugned contract would effectively ensure it, we feel it requisite to issue the following

directions as an interim measure; also to enable this Court to obtain an overall control over the conduct of the parties in terms of the contract concerning data confidentiality."[1]

"All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details/information collected/carried/processed as part of the message/payment instruction,"[2]

The Reserve Bank of India (RBI) has barred Mastercard, American Express and Diners Club from issuing cards in India for their failure to meet data localisation norms prescribed by the regulator in April 2018.[3]

Regulation of human activity has, essentially, been addressed via the concept of geographical delimitation, allowing the assumption that activities are, on the whole, geographically delimited, and they do not exist beyond such limitation. Therefore, on this assumption, a right to regulate is premised whereby geographically defined States share the jurisdiction, again predominantly based on geographic connection. Thus, States regulate the conduct occurring on their territory – location is the deciding factor for exercising jurisdiction. Thus, the idea of allocation of a certain conduct/activity works perfectly if all its aspects are located within a single territory. However, data and the activities related to its management operating on the internet beat this traditional notion of right to regulate because it cannot be linked to any single territory. Does that mean that multiple States could exercise their right to regulate every activity connected with the online generation and handling of data? If not, which State could exercise this right, and when should other States stay away?

Further, and importantly, what is the conceptual legal basis for any State to exercise the right to regulate such data management? Data, as a technological tool and in the form of content, are

[1] Interim orders in *Balu Gopalakrishnan and others v State of Kerala and others* W.P.(C). Temp. NO.84 OF 2020, wherein the Kerala High Court exercised jurisdiction despite the presence of a forum selection clause that vested jurisdiction in the courts of New York.

[2] Circular on Storage of Payment System Data issued by India's central bank, the Reserve Bank of India, dated 6th April, 2018. https://rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=11244 accessed 17/09/2021.

[3] Effective July 2021, the payments firm Mastercard has been barred from adding new customers in India thereby significantly impacting its business which otherwise covered a third of credit and debit card business in India. https://theprint.in/economy/what-is-data-localisation-why-mastercard-amex-diners-club-cant-add-more-customers-in-india/703790/ accessed 17/09/2021

inherently transnational[4], especially in the increasingly global modern society, and online service providers also actively make their service accessible around the world.[5] While the talk of regulation of data gains momentum, one pertinent question that begs clarification relates to identifying the legal location of the data to establish the regulatory right of any specific State. Regulators have for decades been confronting ever-increasing transnationality in the form of global trade and transnational corporations. Therefore, the questions related to applicable law, and the choice of the appropriate forum for dispute resolution[6], the Internet presents an entirely new dimension to the problem of squeezing transnational activity into the national legal straitjacket.[7] While the internet opportunities, especially access, are galore, these opportunities render establishing a legal personality for regulation problematic, for the reason above mentioned. That has not stopped efforts by States to enhanced regulation in the form of governance of data, as has recently been evidenced in the Covid-19 pandemic. States, ostensibly guided by health governance[8], overhauled their privacy-related laws and made health records of their population publicly available, with questionable practices on anonymisation. In India, information about the daily infection spread is made available through twitter and other social media platforms even by officials of the State. Further websites that are crowd-sourced initiatives, often display personal details information, including the geographical location of the infected person, thus exposing such person to potential risk of social ostracism, especially in a multi-racial society like India.

Further States like China moved further and released health and personal details data of even non-citizens required for their pandemic-related governance measures.[9] This research explores the increasing, and therefore alarming, shift in the idea of regulation of data, moving towards what could be called data sovereignty. Towards this, the first part of this research addresses the idea of territorialisation of data, and the models in existence and how these models challenge the traditional contract-based administration of data via the rules of private international law – party autonomy and applicable law. The second part of this research exemplifies the idea of

[4] Haibach, (2015) p. 252, 253–54
[5] Simpson, (2016) P. 669, 670–73
[6] Huang, (2020) p. 1283
[7] Kohl, (2007) p. 1, 4
[8] See, for example, the extensive guidance from Australia requiring much information on personal details being revealed to the State agencies. Mills, (2020), *Travel and COVID-19*, Australian Gov't Dep't Agric. Water & Env't, https://www.agriculture.gov.au/travelling/to-australia/advice-to-travellers/human-health/coronavirus ; on the position in India, https://vidhilegalpolicy.in/blog/indias-covid-19-response-calls-for-urgent-data-disclosure-norms/
[9] Gan, (2020)

territorialisation through a recent attempt by an Indian court ordering interim injunctory relief in a dispute involving data administration related to the covid pandemic, despite not possessing contractual jurisdiction. The third part would further discuss the Indian attempts at domestic regulation of what could be characterised as transnational data management – through policy notifications as well as law reform efforts. The research concludes with poser on whether data localisation alone could and would achieve better data governance when States could pursue the path of trans-nationalisation through hard and soft law regimes, and importantly enhanced cooperation between themselves and via international organisations.

1. From Jurisdictional Clarity to Data Sovereignty

Clarity on competence in dispute resolution is of primordial necessity towards maintaining law and order for States. Writing in the context of international law, and these words hold immense value today in the context of our increasingly connected world, Rosalyn Higgins observed, 'There is a no more important way to avoid conflict than by providing clear norms as to which State can exercise authority over whom, and in what circumstances. Without that allocation of competence, all is rancour and chaos.'[10] This observation cannot be emphasised more in the context of internet and data governance that witnesses increased transnational civil disputes arising from online activity given the extensive internet footprint covering about 4.6 billion global population.[11] The International Telecommunications Union notes that over 4.1 billion people, around 53.6% of the world population, used the Internet in 2019. The World Economic Forum predicts daily data creation of 463 exabytes each day by 2025.[12] Apart from private disputes, governments are increasingly facing pressure from advocacy groups to regulate the online activity of their citizens/persons, natural and legal, for maintaining law and order and protecting local, legally compliant businesses from unfair online competitors.

[10] Higgins, (1994) p. 56. For an extensive discussion on jurisdiction and competence, including a discussion on internet governance the following emblematic literature may be accessed. Thierer and Crews Jr (2003); Snijders and Weatherill (2003); Berman, (2002) p. 311; Smith, (2000) p. 229

[11] As of January 2021, there were 4.66 billion active internet users worldwide - 59.5 percent of the global population. 92.6 percent (4.32 billion) accessed the internet via mobile devices. https://www.statista.com/statistics/617136/digital-population-worldwide/ accessed 18/09/2021.

[12] Desjardins, (2019)

However, such attempts at regulation have to confront the fundamental question – can States exercise jurisdiction in cyberspace? The right to govern cyberspace was perceived to be antithetical to the idea of freedom that is part of its inherent nature and nebulous character.

Regulation by the States?

Matter forms the basis on which jurisdiction could be exercised. Further, State control over matter and, therefore, the exercise of jurisdiction is achieved through erecting borders that define the extent of such control and jurisdiction. Cyberspace is difficult to be explained in the context of these parameters. The nascency and nebulous nature of early activity in cyberspace led pioneers such as Barlow to boastfully declaring that States keep away from cyberspace.[13] Johnson and Post were of the view that the nature of cyberspace meant that the physical sphere laws should not be applied there.[14] This idealism has had much and lasting impact[15] with supporters, including the United States.[16] Early arguments about avoiding the path of regulation referred to the inherently global nature of cyberspace and the impact that such regulation would have on international comity and the foreign policy consequences of any such action, including orders emanating from local judicial action.[17] The 2013 report of the United Nations Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security [GGE] reiterated that international law, especially the UN Charter, applies to cyberspace and that State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and jurisdiction over ICT infrastructure within a State's territory.[18] A subsequent report of the year 2015 listed 11 voluntary, non-binding norms, rules or

[13] Barlow, (2016)
[14] Johnson and Post, (1996) p. 1367, 1402
[15] Mueller, (2019) p. 1, 2; Greenstein, (2000) p. 151.
[16] Clinton and Gore Jr, 'A Framework for Global Electronic Commerce' https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html accessed 21/09/2021.
[17] Brief for Appellant at 3, *Microsoft Corp. v United States* (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 855 F.3d 53 (2d Cir. 2017) (No. 14-2985). Interestingly, the pleadings by Microsoft or the arguments made within the *amicus curiae* brief submitted by Ireland (which argued that Ireland's sovereignty was being threatened) did not refer to any specific law of Ireland being violated by compelling Microsoft to locally store emails in Ireland. Also see, *Google Inc. v Equustek Sols. Inc.*, [2017] 1 S.C.R. 824, 828 (Can.) ("If Google has evidence that complying with such an injunction would require it to violate the laws of another jurisdiction, including interfering with freedom of expression, it is always free to apply to the British Columbia courts to vary the interlocutory order accordingly. To date, Google has made no such application.")
[18] UNGA Doc A/68/98, (2013) p. 19-20

principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment.[19] These norms emphasise cooperation between states in the exchange of information related to any ICT-based activity that could impact each other, respect to the individual's right to privacy in the digital space, responsible reporting of vulnerabilities and share remedies to such vulnerabilities, and desist from conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their teams for malicious international activity, amongst others.

Furthermore, the list of international law principles applicable to cyberspace includes

- state sovereignty;
- sovereign equality;
- the settlement of disputes by peaceful means;
- refraining from the threat or use of force in international relations;
- non-intervention in the internal affairs of other states; and,
- respect for human rights and fundamental freedoms.[20]

Thus, it could be said that principles and norms developed for and applicable to the physical world and linked to territorially bounded spaces are deemed to apply to cyberspace. This phenomenon can be described as the territorialisation of cyberspace, namely the application to cyberspace of territorialist and, by consequence, of sovereign's notions of authority and law.[21]

To explore the possibility of states asserting sovereignty over cyberspace, there were a few attempts to articulate the concept of cyberspace, albeit for the limited purpose of understanding the scope/possibility of regulation. Kuhl defined it as follows,

> […] global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.[22]

Therefore, it could be derived from this definition that cyberspace consists of a physical layer composed of a variety of hardware devices. This logical layer wires all the hardware through the

[19] UNGA Doc A/70/174, (2015) p. 13
[20] *Ibidem*, p. 23
[21] Tsagourias, (2015). Also see, Herrera, (2007)
[22] Kuehl, (2009) p. 1, 28

appropriate software exchanged in the form of data packets. Finally, a social layer involves human intervention in various roles.[23]

The Domestication of Regulation of Cyberspace

Nevertheless, recognition of the role of the States was emerging quickly, with the acknowledgment of the existing regulatory action by States, negating[24] averments about the unacceptability of State regulation of cyberspace. Further, there is an increasing recognition amongst States, that United States has had inordinate influence in the cyberspace through various keystones of the architecture[25] despite the vast majority of internet users being non-American.[26] Given the advances made in the aspect of regulation through the methods of extra-territoriality of judicial orders via conflict of laws rules[27], as well as a recognition of the need of regulation and therefore a decoupling from the idealism-driven global cyberspace, there is an assertion of sovereignty over cyberspace, prominent amongst them being the model adopted by China.[28] The decoupling thus allowed States a path to assert cyber-sovereignty, both domestically and externally.[29] Some States have by their regulations (not reaching a decoupling, but may still be considered an excessive exercise of State sovereignty) impede their populations' access to cyberspace or generally caused for cyberspace's alignment within the nexus of the State.[30]

Data-sovereignty disputes usher in concerns related to state sovereignty and the capability of the State to regulate the global internet without presenting conflicts with prerogatives, similar and

[23] Tsagourias, (2018) p. 523, 539

[24] Wu, (1997) p. 647

[25] See, Clinton, (2000); Ironically, the United States pleaded for a regulation-free internet, premised on the inherent difficulty nature of the cyberspace and an idealism-driven motive to keep it free, and also an awareness of the difficulties in regulating cross-border activity. 'In the early days of the Internet, many people globally assumed that cyberspace would elude the state's effort to control it. US President Bill Clinton famously quipped in 2000 that controlling the Internet would be like 'nailing jello to a wall'. 'Liberty will spread by cell phone and phone modem', he proclaimed. 'Imagine how much it could change China.' Laskai, (2016); Segal, (2020) p. 87; Woods, (2016) p. 729, 741

[26] Woods, (2018) p. 328, 352; Kerr, (2015) p. 285, 287-88

[27] *Ibidem*, p. 353

[28] Laskai, cit., see footnote n. 25; "[..] the 'Great Firewall' — a name given to China's multifaceted system of Internet censorship by Geremie R. Barmé and Sang Ye in an article they wrote for Wired magazine in 1997 — is a sophisticated, finely tuned machine. The Great Firewall not only involves blocking external information, but also finding and proscribing politically-sensitive content generated from within China. It is not only capable of censoring content across the Chinese Internet, but also promotes a culture of self-censorship and control. International observers supposed that such control would stifle the ingenuity that led to the rise of IT hubs like Silicon Valley elsewhere in the world. Instead, China's regime of online control has spurred its own form of domestic technological innovation and entrepreneurship, creating mini-Silicon Valleys across the country."

[29] See, generally, Broeders and Berg, (2020); Schia and Gjesvik, (2017)

[30] Mueller, (2017)

otherwise, of other sovereigns. While the data-sovereignty cases come to courts framed as conflicts between a firm and a state, they implicitly involve a conflict between two states, each one seeking to regulate the same internet conduct. As was seen in *Microsoft Ireland*[31] the case implicated inter-sovereign relations, despite being framed before the Court as a dispute between an American firm and American law enforcement.

On a related note, after some initial unsuccessful attempts[32], States were hesitant to move towards international law-making in the context of cyberspace and issues connected with data governance. They were also reluctant to accept specific interpretations of the controversial legal questions and thus to express their opinio juris. Further, instead of interpreting or developing rules, state representatives seek refuge in the vacuous term 'norms'.[33] Thus progress in international law-making was way too slow and has seen only limited success, the notable being the Tallinn Manual.[34] States have therefore indulged in creating domestic 'norms'[35] and norms founded upon insufficiently developed principles in other regimes like, for instance, the conflict of laws that offered primitive tools for complex problems. The downside of activating domestic normative architecture – these norms were much conflicting in their content and purpose, leading some commentators to lament that cyberspace is in a moment of crisis.[36]

Localised Regulation – Issues related to Conflict of Laws

Domestic responses to protecting personal data, varied as they are, demonstrate the need to identify the applicable law to transnational personal data. According to conflict of laws, in finding *lex causae*, there are three stages: First, characterise the issue into one of the established choice of law classifications by identifying the nature of the subject matter. Second, select the rule of conflict of laws which lays down a connecting factor for the issue in question. Third, identify the system of law which is tied by the connecting factor found in stage two to the issue characterised in stage

[31] *Microsoft* cit., see footnote n. 17. Note that this dispute saw amicus curiae briefs being filed on behalf of European Union, New Zealand, Great Britain, apart from Ireland.
[32] Russia and China have been noted within the literature as being the early movers towards a positivist normative regime in international law, but their attempts were unsuccessful. See, Mačák, (2016)
[33] *Ibidem*, 127
[34] Tallinn Manual on International Law Applicable to Cyber Warfare, (2013)
[35] Osula and Rõigas, (2016).

[36] Macak, cit., see footnote n. 33

one.[37] The connecting factors could relate to the parties (their nationality/place of business at the time of conclusion of the contract), the place of conclusion of the contract, the place of performance of the contract, amongst others. Therein lies the concern – identifying the appropriate connecting factors in any dispute, even in the traditional disputes. The problem is much accentuated in disputes concerning data and cyberspace wherein it is difficult to identify the place of performance of the contract, when the contract is performed through a web of sub-contracts, as seen in contracts related to outsourcing of database management.[38] Given the scale and volume of data transfers across jurisdictions[39], the concern of addressing and complying with multiple regulatory regimes addressing a variety of asset classes and clients, conflicts in the nature and content of regulation pose a heightened challenge. It becomes therefore necessary to ensure that the law, domestic as well international, is up and ready to address the requirements of the digital society, and not be mired in sovereignty-related issues alone. Towards this, the conflict of laws mechanisms should be empowered to address beyond the traditional issues of personal law and civil and commercial matters that it is currently equipped to address. A significant concern to be noted here that disputes related to data technologies are characterised differently under the variety of regimes, national, regional and as well as the global norms.[40] For example, differences exist in the way China, the US, and the EU characterise the right to personal data, the connecting factors they consider, and the law applied to personal data protection. These are significant issues for legislators tasked with law reform but they are equally important for businesses to design their global service, and provide the background material for international organisations engaged in preparation of treaties and model laws. A common feature noticeable amongst these three jurisdictions commend their law on personal data protection to its territorial nature, hence the application of *lex fori*. Alternatively, they consider the personal data protection law as a mandatory law and as a curtailment of party autonomy.[41] However the characterisation of the right to personal data is differently articulated in three regimes. The EU has accorded protection to personal data as

[37] *Macmillan Inc. v Bishopsgate* [1996] 1 WLR 387 (Eng.). see, Huang cit., see footnote n. 6, p. 1285
[38] Marcus, (2020)
[39] McKinsey, (2016), According to McKinsey, it is estimated some 900 million people have international connections on social media, and 360 million take part in cross-border e-commerce. While digital technologies significantly enhanced the response mechanisms in combating the pandemic, they are also of immense value to the economic recovery. See, Marcus, cit., see footnote n. 38
[40] Huang, cit., see footnote n. 6, p. 1286
[41] *Idem.*

a fundamental human right[42], a data subject's right to his or her personal data is characterised as a "right to privacy with respect to the processing of personal data."[43] Similarly, the TFEU also provided for a right to data protection.[44]

In the United States, privacy, a right, is a civil liberty. Warren and Brandies explained privacy as the "right to be alone".[45] Today, it exists in the form of a constitutionally protected right.[46] The Fourth Amendment to the US constitution has implications for data-related activity, however it is limited to government and state institutions, and therefore has little relevance to the issues arising from transnational data-related activity, managed by corporate entities. The Supreme Court ratio in *Roe v Wade*, premised the right to privacy on the "Fourteenth Amendment's Concept of personal liberty and restrictions on state action."[47] Other cases have been less deferential to information privacy as a protectable civil liberty interest,[48] thus leaving the right in a shroud of uncertainty.[49] However, the First Amendment's free speech provision allows for a free flow of information,[50] which could be characterised as a fundamental human right to privacy and data protection in the US. The right to free flow of information was reiterated in *Sorrell v IMS Health Care*[51] wherein the Court held the Vermont law related to confidentiality as unconstitutional and did not advance the policy goals, howsoever appropriate they were, in a permissible way. It

[42] Cole and Fabbrini, (2016) p. 223.

[43] GDPR, Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 (EU), at art. 1.2; *see* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 1(1), 1995 O.J. (L 281) 31; Huang (n 6) 1287.

[44] Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 16, Oct. 26, 2012, 2012 O.J. (C 326) 47.

[45] Warren and Brandeis, (1890) p. 193, 195–96

[46] US Privacy Act, 5 U.S.C. § 552 (2018); Raul, et. al, (2014) p. 268, 269

[47] *Roe v Wade*, 410 U.S. 113, 153 (1973). In *Whalen v Roe* 429 U.S. 589, 605–06 (1977) although the Supreme Court of the United States identified a general right to "information privacy" in the Fourteenth Amendment, the Court upheld a New York statute requiring identification of physicians and patients in dangerous legitimate drug prescription records. https://supreme.justia.com/cases/federal/us/429/589/ accessed 24/09/2021.

[48] See, *Am. Fed'n of Gov't Emps. v Dep't of Hous. & Urban Dev*., 118 F.3d 789, 791 (D.C. Cir. 1997) https://casetext.com/case/american-federation-of-gov-employees-v-hud?__cf_chl_jschl_tk__=pmd_9eSHLg6DS0D01ybjR66cJ_aoCoqugd3bo0IwftuNnNg-1632570610-0-gqNtZGzNAlCjcnBszQuR accessed 25/09/2021.

[49] See, generally, Paul M. Schwartz, (1995) p. 553, 574–82

[50] *Liquormart, Inc. v Rhode Island*, 517 U.S. 484, 503, 116 S. Ct. 1459 (Opinion of Stevens, J.) (''The First Amendment directs us to be especially sceptical of regulations that seek to keep people in the dark for what the government perceives to be their own good.")

[51] *Sorrell v IMS Health Care*, 564 U.S. 552, 561 (2011) wherein the Court heard a plea of first amendment violation by the Vermont Prescription Confidentiality Law that prohibited disclosure or otherwise allowing pharmacies to share prescriber-identity information with anyone except for marketing reason. https://www.supremecourt.gov/opinions/10pdf/10-779.pdf accessed 24/09/2021.

observed that […] "the fear that people would make bad decisions if given truthful information" cannot justify content-based burdens on speech.[52]

The Chinese legal system presents the right to personal data as a personality right, unlike the EU and the US which view it as a fundamental human right. This is because the Chinese Government as the largest data controller reserves the authority to collect, process, save, and use personal information.[53] Despite a decentralised system, the Chinese government, via the Great Firewall, remains the ultimate controller because it controls the Internet connections between its territory and the outside world. It censors the flow of information through its borders and is known to have penalised people for their usage of VPNs.[54] Further, despite constitutional limitations Chinese law has walked farther to include provisions that allow acquisition of data from private companies about their businesses, including personal data of their clients. Article 25 of the Chinese Ecommerce Law allows government departments to require e-commerce operators to provide e-commerce data—which includes personal information, privacy, and business secrets—according to provisions of laws and administrative regulations, and the ecommerce operators shall provide this information as required.[55] Chinese constitution provides protection to individuals in the context of freedom and privacy of correspondence, however the protection to personal data of the individual is unclear, as the law does not view privacy and the right to personal data similarly. The Chinese Civil Code, enacted in May 2020, views the content and the reach of both these provisions differently. Article 1032 of the Chinese Civil Code defines privacy as "the tranquility of the private life of a natural person, and the private space, private activities, and private information that he is unwilling to be known to others"; and Article 1033 provides that the right to privacy should be protected as *erga omnes*. However, Articles 111 and 1034–37 address personal data, but, focus on collection and processing of personal data according to principles of legality, proportionality, and necessity. Namely, the provisions for privacy focus on non-instruction of privacy, while those for personal data highlight how to legally use personal data.[56] Judicial opinion in China also subscribes to the view that these two are distinct rights. Sherry Gong and Nolan Shaw[57] commenting upon

[52] *Ibidem*, 560
[53] Huang, cit., see footnote n. 6, p. 1289
[54] Benjamin Haas, (2017)
[55] Huang, cit., see footnote n. 6, p. 1289
[56] *Ibidem*, 1290
[57] Gong and Shaw, (2015)

the decision in *Ye Zhu v Baidu,* concerning China's search engine Baidu.com explained how the Chinese Court articulated the difference between the two – the records of keyword searches of any user on the internet is a part of their user history and hence a subject of privacy attributes, however, if separated from the data subject, they could not identify the data subject, so they were not personal data. Further, while the Chinese law allows trade in consumer data, the law is unclear – the amount of consumer data that could be processed is not clearly specified in the law, neither is it clearly explainable through the principles of competence, necessity, and proportionality.[58]

The abovementioned narrative is but an example of the differences within the three legal systems with regard to explaining the legal relationship between the data controller and the data processor. While all three systems subscribe to the lex fori, their characterisation of the right to personal data and the connecting factors present much difference.

2. The Indian Perspective

The following narrative will explain the Indian law, nascent as it is, in its progression towards a law on data protection. As identified in the introduction, Indian law seems to be in favour of territorialisation, and data localisation as well. While it could be founded on concerns like safeguarding privacy and security[59], digital protectionism could also be at play. This is achieved by the promotion of local ICT enterprise either directly, by providing preferential treatment to domestic cloud computing businesses, or indirectly coercing foreign companies to locate their servers domestically. These restrictions tend to reduce market access for foreign suppliers of digital services, impeding trade and investment opportunities and increasing the costs and service choice of individual businesses.[60] The India story will present two recent developments – an order from one of the constitutional courts of India emphasising upon local holding of the data and jurisdiction to the lex fori, and the much-expected law reform on personal data protection.

In *Balu Gopalakrishnan and others v State of Kerala and others*[61] the Kerala High Court was hearing a writ petition in the matter related to the handling of covid-19 patient data contracted to a New York business entity Sprnklr, (with its registered office located in Bangalore, India). The

[58] Huang, cit., see footnote n. 6, p. 1294
[59] Kuner, (2011)
[60] Mitchell and Hepburn, (2017) p. 182, 186; Azmeh and Foster, (2016) p. 11
[61] *Gopalakrishnan et. al. v State of Kerala et. al.* cit., see footnote n. 1

petitioners, *ad vindictam publicam,* contended that the Union of India, Government of Kerala contracted with Sprnklr LLC and its Indian entities to manage the patient data during the pandemic and that the said contract raised certain confidentiality concerns. It must be stated here that the contract had a forum selection clause, which vested the power of dispute resolution in the courts at New York. This fact was also the basis of an apprehension of the petitioners presented in their arguments to the Court.

> The petitioners also project an apprehension – based on certain terms of the contract, a copy of which has been appended to some of these writ petitions as an exhibit – that, in the event of breach of data confidentiality or any other dispute, the Government of Kerala will obtain no legal recourse through any courts in Kerala – or for that matter in India – since it postulates that the jurisdiction with respect to such is exclusively vested in the courts in New York, United States of America.

In its interim orders, the Court observed,

> 2. Prefatorily, data confidentiality is, in its ultimate sense, about protecting data from unlawful, unauthorised as also from unintentional access and disclosure

It maybe noted that the petitioners primarily alleged that the contract in question has little or no safeguards against the commercial and unauthorised exploitation of the data entrusted to Sprinklr for processing by the Government of Kerala. This contention was refuted within the arguments of the counsel,

> 10. [..] Sprinklr is not in possession of any data at present and that they have re-transmitted all such to the Government of Kerala, which is presently in its full custody and control.

Regarding the apprehension related to access to justice given the existence of forum selection clause, the counsel for the respondents averred,

> 11. […] that "the data resides in India" and therefore, that the breach of its confidentiality would expose Sprinklr to action in India, both at the hands of individual citizens and the State. They, however, expressly admitted that the "mandate of the New York jurisdiction" binds the Government of Kerala with respect to the breach of the terms of the contract.

The petitioners further submitted [..] that the Government of Kerala, by ceding to the jurisdiction of courts outside India, has rendered recourse to law, both for the citizens and itself, illusory in the event of breach of the contract by Sprinklr.

The Court in its interim orders based its observation on the fact that the data is located in India and is in the possession of the Government of Kerala. Exercising jurisdiction on the substantive issue of confidentiality of data[62], the Court ordered respondents 1, 2 and 3 to ensure anonymisation of the data and take all necessary steps to prevent breach of the confidentiality clause in the Masters Services Agreement between Respondent 1 and Respondent 3, Sprnklr LLC.

The Court ordered,

> We hereby injunct Sprinklr from committing any act which will be, directly or indirectly, in breach of confidentiality of the data entrusted to them for analysis/processing by the Government of Kerala under the impugned contract/s; and that they shall not disclose or part with any such data to any third party/person/entity – of whatever nature or composition – anywhere in the world.[63]

It needs to be noted here in the context of India's tryst with regulating data protection and data governance, that the Court felt that the presence of data in India, attributed a jurisdiction to the courts in India, and secondly the data concerning Indian population, there is a vested interest in the local courts exercising jurisdiction. This interim order therefore demonstrates the tendencies of territorialisation of jurisdiction based upon localisation of data.

The *Puttaswamy* judgment – a watershed statement on digital footprint

On 24th August 2017, a nine-judge bench of the Supreme Court in *Justice K.S. Puttaswamy v Union of India*[64] passed a historic judgment affirming the constitutional right to privacy. It declared privacy to be an integral component of Part III of the Constitution of India.[65] The key features derived from the ratio of the decision encapsulated hereinbelow, reiterate a recognition of privacy

[62] *Ibidem*, 21
[63] *Ibidem*, 23
[64] *Justice K.S. Puttaswamy (Retd.) v Union of India & Ors*. 2017 (10) SCALE 1.

[65] Constitution of India, (1950)

as an intrinsic right, and the judicial standards of review that would be applied to actions that allegedly impinge upon privacy.

- Privacy is intrinsic to and inseparable from human element in human being.

- Right to Privacy is not just a common law right but a fundamental right guaranteed by Part III of the Constitution.

- Privacy is not an absolute right, subject to permissible restrictions.

- Action must be sanctioned by law, it must be necessary to fulfil a legitimate aim of the State and the interference must be 'proportionate to the need for such interference'.

- Recognition and enforcement of claims for breach qua non-state actors will require legislative intervention by the State.

- Right to privacy was grounded in rights to freedom under both Article 21 and Article 19 of the Constitution encompassing freedom of the body as well as the mind.

The four elements of the judicial review standard are as follows,

Legality: The existence of a law

Legitimate Goal: The law should seek to achieve a legitimate state aim (Chandrachud J.). The proposed action must be necessary for a democratic society for a legitimate aim (Kaul J.). Justice Kaul's opinion can be read to espouse the EU narrow tailoring test.

Proportionality: There should be a rational nexus between the objects and the means adopted to achieve them (Chandrachud J.). The extent of interference must be proportionate to its need (Kaul J.).

Procedural Guarantees: To check against the abuse of State interference (Kaul J.)

Despite being a unanimous decision, there were differences with regard to the articulation of the review standards, as shown above, wherein Justice Kaul's opinion seemed to lean closer to the EU model.

The Normative Content

Protection of data is addressed via the Information Technology Act, 2000 ("IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011 (the "IT Rules").[66] Personal information is defined under Rule 2(i) defines personal information as follows,

> "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person".

Further, following the *Puttaswamy* judgment, the Government of India in 2018 proposed a legislation that aims a comprehensive regulation of data protection. The bill a result of extensive research reports submitted by Justice Sri Krishna Committee[67], The TRAI Report[68], and the Justice AP Shah Report[69]. The Personal Data Protection Bill[70] is now for consideration and scrutiny before a Select Committee of the Parliament, before being returned to the Parliament for vote. The following section discusses the rights envisaged under the SDPI Rules and how they compare with the content under the Data Protection Bill, 2018 (hereinafter, "the Draft Bill").

The IT Act mandates that a body corporate responsible for handling sensitive personal data or information liable for compensating loss based upon a fault liability arising from negligence in implementing and maintaining reasonable security practices and procedures. Such reasonable security practices and procedures have been specified in the SPDI Rules as minimum standards of data protection for sensitive personal data. A non-exhaustive set of guidelines these SPDI Rules require companies to have a privacy policy, to obtain consent when collecting or transferring

[66] Other regulatory mechanisms addressing data governance in India include,
- Consumer Protection Act, 2019 ('CPA') and Consumer Protection (E-Commerce) Rules, 2020;
- rules made by the Reserve Bank of India ('RBI');
- rules imposed by the Telecom Regulatory Authority of India ('TRAI');
- rules imposed by the Insurance Regulatory and Development Authority of India;
- rules imposed by the Securities and Exchange Board of India ('SEBI');
- various decisions of Indian courts; and
- Unified Licence Agreements issued pursuant to the National Telecom Policy, 2012 by the Department of Telecommunications ('DOT').

[67] The Committee of Experts on a Data Protection Framework for India, (2018)
[68] Telecom Regulatory Authority of India Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector (2018)
[69] Report of the Group of Experts on Privacy, (2012)
[70] The Personal Data Protection Bill, (2019)

sensitive personal data or information, and to inform data subjects of recipients of such collected data. The SPDI Rules identified the following rights for the data subjects.

1. Right to be informed – applicable for all personal information, including sensitive personal data. The Rules insist on a privacy policy that will address, apart from the information so collected, the security procedures adopted to prevent leakage and misuse of such information. In comparison, the Draft Bill requires data fiduciaries to provide notice to data principals, at the time of collection of personal data, including the procedure related to consent and its withdrawal, information about the processing of such data and any cross-border transfers as well as procedures related to grievance redressal.
2. Right to access – The Rules allow the individuals to review the information that body corporates possess about them. The Draft Bill also provides for data principals to request copies or summaries of the personal data processed by the data fiduciaries, including how and with whom the data has been shared.
3. Right to Rectification – The Rules and the Draft Bill allow for the data principals to rectify any inaccurate information about themselves in possession of the data fiduciaries including updating any such outdated data.
4. Right to erasure – while the SPDI did not refer to a right to erasure, the Draft Bill empowered the data principal with a right to request erasure of any personal information that may no longer be required for the purpose for which it was procured. Further, the data principals have a right to be forgotten with regard to preventing any disclosure of data made by them if such disclosure is no longer necessary in the context of the purpose for which the data has been collected, or if such disclosure is contrary to the applicable laws.
5. Right to object/opt-out – Withdrawal of the consent by the data principals is possible under the SPDI Rules as well as the Draft Bill.
6. The Draft Bill provides for a Right to portability for the data principals with respect to personal data that is processed through automated means, including transfer of such data among data fiduciaries.
7. However, the Draft Bill does not make place for a right to the data principals not to be subjected to automated decision-making.

The law in India offers protection only to sensitive personal data (a sub-set of personal data). Rule 5 of the IT Rules prescribes that no body corporate shall collect sensitive personal data or information unless (a) the information is collected for a lawful purpose connected with a function or activity of the body corporate; and (b) the collection of such information is considered necessary for that purpose. Rule 6 of the IT Rules prescribes that no body corporate can disclose sensitive personal information to any third party without permission from the provider of such information.

The Draft Bill retains the distinction between personal data and sensitive personal data. Unlike the SPDI Rules, all identifiable data, with respect to any characteristic, attribute, trait, or other feature of a person's identity, are classified as personal data. It is worth noting that the definition of personal data applies to both online and offline mediums and includes inferences drawn by the profiling of personal data.

Sensitive personal data is a subset of personal data that is subject to enhanced processing requirements. It includes health or financial data, biometric data, sex life, sexual orientation, and religious or political beliefs. The Bill allows the Government to specify further categories of sensitive personal data.[71]

While the Draft Bill does not provide for processing of anonymised data, data fiduciaries could be compelled by the Government to share anonymised or non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies offered by the Government.[72]

The Possible Regulatory Guidance on doing business with/in India

According to a recent paper from the Organization for Economic Cooperation and Development (OECD), regulatory divergence can add between 5 and 10 percent to the cost of doing business.[73] However, empirical evidence also indicates that, where laws are harmonised, foreign direct investment can increase by as much as 15 percent.[74] David Markus used the APAC privacy matrix

[71] Chacko and Misra, 'India - Data Protection Overview
[72] *Idem*.
[73] Regulatory Divergence: Costs, Risks, Impacts: An International Financial Sector Study by Business at OECD and the International Federation of Accountants, (2018) p. 5
[74] Markus, (2020)

to identify the challenges in implementing content similar to the harmonised law, for instance, the GDPR. The Matrix placed India on Category 3 along with few other Asian emerging economies.[75]

Category 3: The GDPR' Push-Pull Late Adopters': 2018 onwards

India, China, Thailand, and Vietnam - the focus with these recent reforms is on adopting a GDPR style framework to achieve data security in the eyes of EU regulators, with some attempts to opt out of data transfer through localised security assessments and onshore servers.[76]

While businesses achieve data centralisation through strategies like private cloud or rent an on-demand cloud, or even adopt a hybrid of both these methods, regulatory structures are increasingly moved towards insisting on localisation through assertions of sovereignty and territorialisation. Cross-border data transfers are increasingly getting exposed to the risk of conflicts with regulatory content that is exponentially expanding.[77] In 2019, it was noted that the total number of regulations on data transfer and localisation storage requirements was over 200 globally.[78]

Given that almost 40% of India's goods and services exports consist of data-related activities in IT and ITES[79], it is only a concern that India is not recognised as a jurisdiction meeting adequacy on the GDPR. The enactment of the Data Protection Bill could lead to a positive change in this regard, but India has to address issues concerned with localisation requirements[80] within its regulations.

3. Conclusion

Standard Contractual Clauses (SCCs) could be a safe way of contracting, they could ensure safe and regulation-compliant data transfers, especially in jurisdictions that have concerns related to adequacy as per the GDPR. They could be reviewed periodically, and their scope needs to be limited or expanded depending on changes to projects or use of other vendors in different locations.

[75] *Idem.*
[76] For a detailed reading of the OECD's work on Privacy law see, *The OECD Privacy Framework*, (2013)
[77] Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective, (2020) p. 28
[78] Casalini, F. and González, (2019)
[79] Mattoo and Wunsch, (2004) p. 765
[80] Article 40 of the draft Personal Data Protection Bill states: 'Every data fiduciary shall ensure the storage, on a server or data centre located in India'

Further, Binding Corporate Rules[81] are a mechanism which often complement SCCs and sit well alongside them.

However, the need of the hour is law reform that would ensure better regulatory compliance. The territorialisation of cyberspace is increasingly becoming a reality, as is the extension of territorial notions of sovereignty and of international law to cyberspace with respect to activities, persons and objects. The question that needs to be addressed is about the scope of state sovereignty over cyberspace and in cyberspace. This is a political question for individual states but also for the society of states, and one way to address it is through enhanced cooperation in all areas that see the digital footprint travelling beyond boundaries. States could draw inspiration from the reports of the United Nations Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security [GGE][82] and strive towards achieving harmonisation in their regulatory activities concerning cyberspace.

Dispute resolution in matters related to data transfer could be exposed to various conflict of laws methods like comity, consistency, and predictability to international civil litigations and discourage forum shopping. However, the foregoing narrative shows that data transfer disputes are decided via the unilateral applicable law, and there is less preference for the application of foreign law, thus centre-staging the role of jurisdiction in disputes related to transnational data breach leaving little role for choice of law issues. However, the ease of dispute resolution could be achieved by cooperating towards an international treaty, or at least a model law on the regulation and choice-of-law issues for transnational personal data. There ought to be rules of the road in cyberspace, which would regulate the conduct of all stakeholders.[83] Adamson charts the passage of dialogue over the last two decades veering from 'possible multilateral treaty to application of existing international law, and to the development and application of cyber norms.'[84] This could go far in ensuring credible legal regimes in a sphere that is inherently global.

Acknowledgment This research is supported by the Indian Development Fund 2020-2021.

[81] GDPR, Article 47.
[82] UNGA, cit. footnote n.19&20
[83] Adamson, (2020).
[84] *Idem.*

References:

Articles

Azmeh Shahmel & Foster Christopher, 'The TPP and the digital trade agenda: Digital Industrial Policy and Silicon Valley's influence on new trade agreements' (2016) *LSE International Development, Working Paper* No. 16-175, at page 11. https://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf accessed 25/09/2021.

Berman Paul Schiff, 'The Globalisation of Jurisdiction' (2002) 151 *University of Pennsylvania Law Review* 311

Casalini, F. and J. López González, 'Trade and Cross-Border Data Flows', OECD Trade Policy Papers, No. 220, (OECD, Paris, 2019).

Cole David and Fabbrini Federico, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*, (2016) 14 *ICON* 220, 223.

Greenstein Shane, 'Commercialization of the Internet: The Interaction of Public Policy and Private Choices or Why Introducing the Market Worked so Well' (2000) 1 *Innovation Policy and the Economy* 151.

Haibach Georg, 'Cloud Computing and European Union Private International Law', (2015) 11 Journal of Private International Law 252, 253–54.

Huang Ji, 'Applicable Law to Transnational Personal Data: Trends and Dynamics' (2020) 21 German Law Journal 1283.

Johnson David and Post David, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367, 1402.

Kerr Orin S., 'The Fourth Amendment and the Global Internet' (2015) 67 *Stanford Law Review* 285, 287-88

Marcus D, 'Digital resilience in the age of a global pandemic: how can privacy assist in risk mitigation?' (2020) 17(1&2) *Privacy Law Bulletin* 2.

Markus David, Digital trade and digital sovereignty: navigating best practice for cross border data transfers, Working Paper 2020 (available on file with the authors)

Mattoo A & Wunsch S, 'Pre-empting protectionism in services- the GATS and outsourcing', (2004) 7(4) Journal of International Economic Law 765.

Mitchell Andrew D. & Hepburn Jarrod, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-border Data Transfer' (2017) 19 *Yale Journal of Law and Technology* 182, 186

Mueller Milton L, 'Against Sovereignty in Cyberspace' [2019] *International Studies Review* 1, 2

Schwartz Paul M., 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1995) 80 *Iowa Law Review* 553, 574–82. (Digital copy of the print version available with the author)

Simpson D. Michael, 'All Your Data Are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy', (2016) 87 University of Colorado Law Review 669, 670–73.

Smith Bradford L., 'The Third Industrial Revolution: Law and Policy for the Internet' (2000) 282 *Recueil des Cours* 229

Tsagourias Nicholas, 'Law, borders and the territorialisation of cyberspace' (2018) 18(4) Indonesian Journal of International Law 523, 539.

Warren Samuel D. and Brandeis Louis D., 'The Right to Privacy', (1890) 4 *Harvard Law Review* 193, 195–96.

Woods Andrew Keane, 'Against Data Exceptionalism' (2016) 68 *Stanford Law Review* 729, 741.

Woods Andrew Keane, 'Litigating Data Sovereignty' (2018) 128 Yale Law Journal 328, 352.

Wu Timothy S, 'Cyberspace Sovereignty? - The Internet and The International System' (1997) 10 *Harvard Journal of Law and Technology* 647.

Books

Adamson Liisi, 'International Law and International Cyber Norms: A Continuum?' in D. Broeders and Bibi van den Berg (eds), *Governing cyberspace: behavior, power, and diplomacy* (Rowman & Littlefield 2020)

D Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield, 2020)
D. Broeders and Bibi van den Berg (eds), 'China's Conception of Cyber Sovereignty: Rhetoric and Realisation', *Governing cyberspace: behavior, power, and diplomacy* (Rowman & Littlefield 2020)
Henricus Snijders and Stephen Weatherill (eds.), *E-Commerce Law: National and Transnational Topics and Perspectives* (Kluwer Law International, 2003)
Herrera Geoffrey, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space", in Myriam Dunn Cavelty, Victor Mauer, Sai Felicia Krishna-Hensel (eds), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, (Ashgate, 2007)
Higgins Rosalyn, *Problems and Process: International Law and How We Use It* (Oxford: Clarendon, 1994)
Kohl Uta, *Jurisdiction and the Internet* (CUP, 2007) 1, 4.
Kuehl Daniel T, "From cyberspace to cyberpower: Deining the problem" in Franklin D. Kramer, Stuart H. Starr, Larry K Wentz (eds), *Cyberpower and National Security* (National Defense University Press, 2009) 1, 28.
Osula Anna-Maria and Rõigas Henry, 'Introduction' in Anna-Maria Osula and Henry Rõigas (eds), *International cyber norms: legal, policy & industry perspectives* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016)

Raul Alan Charles, Manoranjan Tasha D. and Mohan Vivek, "*United States", in* Alan Charles Raul (ed), *The Privacy, Data Protection, And Cybersecurity Law Review* (1st edition) (Law Business Research Ltd, 2014)

Thierer Adam and Crews Jr Clyde Wayne (eds.) *Who Rules the Net? Internet Governance and Jurisdiction* (Washington DC: Cato Institute, 2003)
Tsagourias Nicholas, "The Legal Status of Cyberspace" in Nicholas Tsagourias & Russell Buchan (eds), *Research Handbook on International Law and Cyberspace*, (E Elgar, 2015)

Online Documents

Barlow John Perry, 'A Declaration of the Independence of Cyberspace' (Electronic Frontier Foundation, 20 January 2016) https://www.eff.org/cyberspace-independence&gt accessed 20/09/2021.
Chacko Mathew & Misra Aadya, 'India - Data Protection Overview' https://www.dataguidance.com/notes/india-data-protection-overview accessed 26/09/2021.
Clinton William J. and Gore Jr Albert, 'A Framework for Global Electronic Commerce' https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html accessed 21/09/2021.
Clinton William, President of the United States, 'Permanent Normal Trade Relations Status for China' (Speech at the Paul H. Nitze School of Advanced International Studies of the Johns Hopkins University, 8 March 2000) http://www.techlawjournal.com/cong106/pntr/20000308sp.htm accessed 22/09/2021.
Constitution of India, 1950, Part III enumerated the fundamental rights. https://legislative.gov.in/sites/default/files/COI_1.pdf accessed 24/09/2021.
Desjardins Jeff, 'How Much Data Is Generated Each Day?' (World Economic Forum, 17 April 2019)
Gan Nectar, *A Chinese Australian Woman breached coronavirus quarantine in Beijing to go for a Jog—and lost her job*, CNN (Mar. 20, 2020), https://edition.cnn.com/2020/03/20/asia/beijing-coronavirus-woman-fired-intl-hnk/index.html.
Gong Sherry and Shaw Nolan, *Chinese Appellate Court Provides Guidance for Lawful Use of Cookies*, **HOGAN LOVELLS** (Aug. 3, 2015), https://www.hldataprotection.com/2015/08/articles/international-eu-privacy/chinese-appellate-court-provides-guidance-for-lawful-use-of-cookies/ accessed 25/09/2021.
Haas Benjamin, *Man in China sentenced to five years' jail for running VPN*, **GUARDIAN** (Dec. 21, 2017) https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn accessed 25/09/2021.
https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf accessed 21/07/2021.
https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf accessed 22/09/2021.
https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/&gt accessed 19/09/2021.
Kuner Christopher, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", OECD Digital Economy Papers, No. 187, (OECD, 2011) https://www.oecd-

ilibrary.org/docserver/5kg0s2fk315f-en.pdf?expires=1632583184&id=id&accname=guest&checksum=5B68A70E599A3E4DF254649D803CFD8B accessed 25/09/2021.
Lorand Laskai, 'Chapter 6 - "Nailing Jello to a Wall' in *The China Story* https://www.thechinastory.org/yearbooks/yearbook-2016/chapter-6-nailing-jello-to-a-wall/ accessed 21/09/2021.
Mačák K, 'Is the international law of cyber security in crisis?,' *2016 8th International Conference on Cyber Conflict (CyCon)*, 127-139
McKinsey, Digital globalisation: the new era of data flows', (2016) https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows accessed 24/09/2021.
Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective, August 2020, at 28 https://www.oecd-ilibrary.org/docserver/6345995e-en.pdf?expires=1632666746&id=id&accname=guest&checksum=1E3EC06588AE601125E29ECC1472E796 accessed 25/09/2021.
Mills Nicole, *Coronavirus quarantine rules will force international arrivals into two-week quarantine in hotels and caravan parks*, ABC News (Mar. 27, 2020), https://www.abc.net.au/news/2020-03-27/coronavirus-quarantine-laws-force-international-arrivals-hotels/12097312
Mueller Milton, 'Internet Fragmentation Exists, But Not In the Way That You Think' (*Council on Foreign Relations*, 12 June 2017) https://www.cfr.org/blog/internet-fragmentation-exists-not-way-you-think accessed 23/09/2021.
Regulatory Divergence: Costs, Risks, Impacts: An International Financial Sector Study by Business at OECD and the International Federation of Accountants, (2018) 5 https://biac.org/wp-content/uploads/2018/04/IFAC-OECD_Regulatory-Divergence_V9_singles.pdf accessed 26/09/2091.
Report of the Group of Experts on Privacy, (2012) https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf accessed 10/09/2021.
Schia Niels Nagelhus and Gjesvik Lars, 'China's Cyber Sovereignty' (Norwegian Institute of International Affairs (NUPI) 2017) http://www.jstor.org.ezproxy.sau.ac.in/stable/resrep07952 accessed 22/09/2021.
Segal Adam, 'An Emerging China-Centric Order: China's Vision for a New World Order in Practice' (The National Bureau of Asian Research 2020) Special Report 87
Tallinn Manual on International Law Applicable to Cyber Warfare, prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Center of Excellence. More information available at http://csef.ru/media/articles/3990/3990.pdf
Telecom Regulatory Authority of India Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector (2018)
The Committee of Experts on a Data Protection Framework for India, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* (2018) https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf accessed 20/09/2021.
The OECD Privacy Framework, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf accessed 26/09/2021.
The Personal Data Protection Bill, 2019 Bill No. 373 of 2019,
UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, UN Doc A/68/98, [19]-[20].
UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, UN Doc A/70/174, [13].