ISSN (O): 2347 - 3827

RGNUL-SAM CONCLAVE ON INFORMATION TECHNOLOGY LITIGATION & DATA PROTECTION IN INDIA, 2022

Special Issue

2022

RAJIV GANDHI NATIONAL UNIVERSITY OF LAW, PUNJAB

RGNUL FINANCIAL AND MERCANTILE LAW REVIEW

RGNUL-SAM CONCLAVE

ON INFORMATION TECHNOLOGY

LITIGATION & DATA PROTECTION

IN INDIA, 2022

SPECIAL ISSUE 2022

RAJIV GANDHI NATIONAL UNIVERSITY OF LAW, PUNJAB

RGNUL FINANCIAL AND MERCANTILE LAW REVIEW

[Citation: RFMLR I.T. Sp. Ed. <Page Number> 2022]

July 2022

Visit us at: www.rfmlr.com

Printed, published and owned by the Registrar, Rajiv Gandhi National University of Law, Punjab, Bhadson-Patiala Rd, Sidhuwal, Patiala, Punjab, 147 006.

PATRONS

Prof. (Dr.) G.S. Bajpai	*Chief Patron*
Prof. (Dr.) Anand Pawar	*Patron*

EDITORIAL BOARD

Prof. (Dr.) Anand Pawar	*Faculty Editor*
Aditya Mathur **Soumya Tiwari**	*Managing Editors*
Nalinaksha Singh **Ridhima Bhardwaj** **Rohit Guru** **Talin Bhardwaj**	*Senior Editors*
Divyank Tikkha	*Citation Editor*
Dhawal Srivastava **Nishant Nagori** **Reet Kaur Virk** **Srishti Kaushal**	*Associate Editors*

Harshit Kapoor **Nandini Mishra** **Nishi Kaur** **Vansh Bhatnagar** **Vanshika Samir**	*Junior Editors*
Aryan Gupta **Jyoti Jindal** **Raghav Sehgal**	*Copy Editors*
Arun Mahapatra **Kunal Yadav** **Lakshya Sharma**	*Digital Editors*
Akshat Verma **Ananya Banerjee** **Dhruv Bhatia** **Diya Vig** **Shashwat Sharma** **Tarpan Soni**	*Assistant Editors*

FOREWORD

On behalf of Shardul Amarchand Mangaldas & Co (SAM & Co), I would like to extend my sincerest congratulations to the Editorial Board of the RGNUL Financial and Mercantile Law Review (RFMLR) for successfully conducting the 2nd RGNUL - SAM Conclave on Practical Aspects of Information Technology Litigation & Data Protection in India 2022 (2nd RGNUL - SAM Conclave, 2022). I would also like to thank the talented pool of authors, faculty members of RGNUL, and professionals at SAM whose time and efforts helped in the successful fruition 2nd RGNUL - SAM Conclave, 2022.

India is positioned as one of the largest data markets in the world. In furtherance, it is of paramount importance to have robust regulations and comprehensive laws that complement the pervasive information technology sector. India presently does not have any express legislation governing data protection or privacy, though there are some relevant laws in India dealing with data protection such as the Information Technology Act, 2000 and the Indian Contract Act, 1872. Over the years, various sectoral regulations and rules have also introduced suitable remedies and preventive mechanisms for data protection. However, a fragmented set of regulations and the constantly changing trends in technology have resulted in some loopholes in the existing laws. Thus, it is important to initiate discourse around the disputes that have emerged in the realm of information technology and data protection, and to tread upon the evolving global data governance landscape. With this spirit, SAM & Co collaborated with RFMLR for the purpose of expatiating and

stimulating research on contemporary issues regarding the practical aspects of information technology and data protection in India.

The 2nd RGNUL - SAM Conclave, 2022 was organized virtually, over two weekends: May 07, 2022 and May 14, 2022. The first event was the Paper Presentation Session which proved to be informative and insightful for both the participants and the panelists. Research papers on diverse and pertinent topics such as Online Dispute Resolution, End-to-End encryption and privacy, data localization etc. were presented by various law students.

Further, I was glad to be a speaker along with other leading experts such as - Mr. Gauhar Mirza (Partner, SAM & Co), and Dr. Subhajit Basu (Associate Professor, Leeds University) at the Expert Panel Discussion of the 2nd RGNUL - SAM Conclave, 2022. The discussion was moderated by Mr. Prakhar Deep (Senior Associate, SAM & Co), and it was attended by students and professionals from across the country.

The Special Edition, 2022 tries to capture a detailed discourse on the emerging issues faced in the Indian data governance and information technology landscape, with a particular focus on understanding the disputes that emerge in India. The cutting-edge research demonstrated by the authors through their comprehensive papers will prove to be seminal in furthering the aim of providing practical insights into the evolving field of information technology and data protection. We hope that the research papers are insightful and useful for students and professionals interested or working in this field.

Lastly, we look forward to collaborate with RFMLR again in the upcoming academic sessions and collectively move towards disseminating legal knowledge and furthering the discourse on various pertinent legal issues.

Best Wishes

Mr. Tejas Karia

Partner, Head-Arbitration

Shardul Amarchand Mangaldas & Co

TABLE OF CONTENTS

I. KEEPING IT ONLINE: DEVELOPING AN ODR MECHANISM FOR INDIA'S E-COMMERCE DISPUTES

- Pratham Arya & Lisa Sankrit*

ABSTRACT

While the COVID-19 pandemic disrupted the traditional practices that the courts used to follow, it also paved way for innovative and novel methods of alternate dispute resolution to evolve. One such method of dispute resolution called 'Online Dispute Resolution' has been dealt within this paper. Even though there is a rising number of e-consumers (India is expected to have 500 million online shoppers by 2030), India does not have any ODR regulation and the shortcomings in the current mediation framework have us lagging behind in terms of motivating litigants to initiate ODR-led complaints. Uncertainty regarding *inter alia* the enforcement of awards, low demand for mediation, and the lack of trained mediators are a few issues that plague the mediation framework and make it an unpopular choice among litigants. Considering the fact that mediation can be suitable for the adjudication of many B2C and B2B disputes, the time is just right to make amends in order to make space for a solid ODR framework. In this paper, we aim to draw inspiration from such contemporary jurisdictions so that e-consumers have an efficacious ODR platform that is not merely a digital layer on top of existing dispute resolution methods. Thus, in a structured manner, we provide how in our opinion an ideal ODR mechanism should function both in B2C and B2B disputes.

* The authors are fourth-year students of B.A. LL.B. at Symbiosis Law School, Noida. Views stated in this paper are personal.

I. INTRODUCTION: UNDERSTANDING THE WOES OF THE INDIAN CONSUMER

Consider Chitra to be a typical Indian e-commerce customer. A few years ago, Chitra like many of us, tempted by an offer on an e-commerce website ordered a Dell laptop at a discounted price of INR 27,000. However, the delivered laptop was nowhere close to the original Dell laptop leading to multiple call redirections from customer care. Each time she called customer care she was allotted a different executive who would then provide a complaint number and ask her to wait while they would get back to her. She also visited the registered office of the e-commerce website but did not find any grievance officer. After one and a half months of continual, she lost all hopes and decided to live with the duped laptop rather than subject herself to the tardiness and vicissitudes of the court proceeding.[1] Many e-consumers in India strive hard to agitate their concerns but the absence of an effective Online Dispute Resolution (**"ODR"**) mechanism makes this task cumbersome and hence they fail to pursue remedies.[2] Therefore, the plight of many such consumers makes it evident that there is a crying need for an ODR platform.

The desperate need also stems from the fact that India in the past two years has seen a surge in online shopping and as a result, e-consumer disputes have also seen a sequential rise. According to the data published by the Ministry of Consumer Affairs for April 2020 to February 2021, a total of

[1] Navya PK, 'Cheated While Shopping Online? Here's What You Can Do' (*Citizen Matters*, 9 January 2009*)* <https://citizenmatters.in/ecommerce-online-shopping-consumer-protection-law-5526> accessed 26 April 2022.
[2] Rahul Matthan, 'The need for an online dispute resolution mechanism' (*Livemint*, 5 March 2019) <https://www.livemint.com/opinion/columns/opinion-the-need-for-an-online-dispute-resolution-mechanism-1551808916274.html> accessed 26 April 2022.

1,88,262 complaints relating to e-commerce were lodged.[3] Furthermore, according to data published by the Department of Consumer Affairs (**"DCA"**), Ministry of Consumer Affairs, it has been observed that in the last four years e-commerce disputes constituted 22% of the entire corpus of consumer complaints.[4] India is also expected to have 500 million online shoppers by 2030.[5]

Despite having a multitude of online shoppers, India does not have any ODR regulations. Further, the shortcomings in the current mediation framework have us lagging in terms of motivating litigants to initiate ODR-led complaints. Uncertainty regarding *inter alia* the enforcement of awards, low demand for mediation, and the lack of trained mediators are a few issues which plague the mediation framework and make it an unpopular choice among litigants. Considering the fact that mediation can be suitable for adjudication of many business-to-consumer (**"B2C"**) and business-to-business (**"B2B"**) disputes, the time is right to make amends in order to make space for a sound ODR framework.

In this paper, we aim to draw inspiration from such contemporary jurisdictions so that e-consumers have an efficacious ODR platform that is not merely a digital layer on top of existing dispute resolution methods. Thus, in

---

[3] Zia Haq, 'As shopping goes online, e-commerce disputes rise to unprecedented levels' (*Hindustan Times*, 22 March 2021) <https://www.hindustantimes.com/business/ecommerce-disputes-on-the-rise-shows-data-101616366508503.html> accessed 26 April 2022.

[4] Samyak Pandey, 'Over 22% of consumer complaints in India in last 4 years are linked to e-commerce sector' (*The Print*, 15 March 2021) <https://theprint.in/india/over-22-of-consumer-complaints-in-india-in-last-4-years-are-linked-to-e-commerce-sector/622383/> accessed 26 April 2022.

[5] AMMP Community, 'Modern Marketeers Guide to Connected Consumer Journeys' (*The AMMP Community*, July 2022) <https://bestmediainfo.in/mailer/mma_groupm_modern_marketers_guide_to_connected_consumers_journeys.pdf> accessed 26 April 2022.

a structured manner, we provide, how in our opinion, an ideal ODR mechanism should function both in B2C and B2B disputes.

II. DEVELOPING INDIA'S ROBUST ODR FRAMEWORK

A. Establishing An ODR Platform

Before we delve into the discussion of how the ODR mechanism functions, it is of utmost importance to define this term. According to the United Nations Commission on International Trade Law, the ODR Working Group defines ODR as *"[…] a mechanism for resolving disputes facilitated through the use of electronic communications and other information and communication technology".*[6]

An ODR platform is the foremost and primary step in any online dispute resolution; it is through this platform that a consumer files a complaint and the proceedings are initiated. Organisation for Economic Co-operation and Development (**"OECD"**) published a report in the year 1999 wherein it encouraged businesses, government and consumer representatives to work together for the betterment of consumer dispute redressal through the innovative use of technology in Alternative Dispute Resolution (**"ADR"**).[7] Post these, various steps[8] were taken to include electronic media and e-dispute

[6] The United Nations Commission on International Trade Law, 'UNCITRAL Technical Notes on Online Dispute Resolution' (2017) (hereinafter "**UNICTRAL Technical Notes**").
[7] Organization for Economic Co-operation and Development, 'The Guidelines for Consumer Protection in the Context of Electronic Commerce' (1999).
[8] European 'Directive on Electronic Commerce' (98/0325 (COD)).

settlement in the existing system.[9] However, the major regulatory framework came in the year 2013[10] which is of particular relevance to India as well.

According to Article 5[11] of Regulation (EU) No 524/2013, the European Commission has established an ODR platform and the commission is itself responsible for the maintenance, data security, privacy and accessibility of this platform. The ODR platform, a neutral third party, serves a multifarious purpose. It starts with providing an electronic complaint form, then informing the respondent about the complaint that has been filed, and goes on to offer a case management tool that is free of cost so that the parties can initiate the ODR proceeding. Additionally, the Regulation also mandates all the traders in the EU to provide an easily accessible link to this ODR platform.[12]

The Brazilian Government also realized the potential use of Information and Communications Technology (**"ICT"**) in resolving B2C disputes and therefore created a subsidized website *Consumidor.gov* in the year 2014, where consumers can file a complaint against the company that then responds within a reasonable span of 10 days. After this the consumer reviews this response on a scale of 1 to 5 within 20 days, showing their satisfaction or dissatisfaction. This entire process is free of cost.[13] This

---

[9] Marc Andre Wilikens, A Vahrenwald and Philip Reginald Morris, 'Out-Of-Court Dispute Settlement Systems for E-Commerce. Report On an Exploratory Study' (JRC Publications Repository, 2022) <https://publications.jrc.ec.europa.eu/repository/handle/JRC20538> accessed 4 July 2022.

[10] Regulation (EU) No 524/2013 of the European Parliament and of the Council (2013) on online dispute resolution for consumer disputes and Amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (hereinafter "**Regulation on Consumer ODR**").

[11] ibid.

[12] ibid.

[13] 'Brazil Government's Official B2C Dispute Resolution Portal' <https://www.consumidor.gov.br/pages/principal/?1649915253885> accessed 26 April 2022.

platform seemed effective as in the year 2018, 500,000 complaints were solved online with an 80% success rate thus reducing the burden on the judiciary. However, the only drawback that exists is the lack of consumer awareness as this website is not a 'shaming' platform and the disputes are resolved between the parties without making the complaint public. Therefore, the website only received 800,000 complaints between the years 2016 to 2018. On the contrary *ReclameAquit,*[14] a website that posts complaints publicly and then resolves them had more public engagement as this platform created a 'public shaming effect' that exerted pressure on companies to change their behaviour.[15]

B. Choosing An ODR Mechanism

1. Automated Settlement System

Any ODR proceeding consists of various processes and options from which a complainant/complainant may choose. The UNCITRAL Technical Notes on Online Dispute Resolution provides various stages and options which can be used for effective dispute resolution.[16]

The first stage as envisaged in this technical note is negotiation which is conducted through this ODR platform. The process generally commences after the respondent receives a response and if a response is not received within a reasonable period, then the negotiation process commences. In cases where

[14] 'Reclame AQUI' (2022) <https://www.reclameaqui.com.br/empresa/reclameaqui/> accessed 4 July 2022.
[15] MJ Schmidt-Kessen, Rafaela Nogueira and Marta Cantero, 'Success or Failure? - Effectiveness of Consumer ODR Platforms in Brazil and in the EU' (2019) Copenhagen Business School, Law Research Paper Series No. 19-17, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3374964> accessed 4 May 2022.
[16] UNICTRAL Technical Notes.

negotiation does not settle, then the process moves to the next stage.[17] The second stage is the facilitated settlement wherein a neutral third party is appointed who then assists the parties to settle. This neutral is appointed by the ODR administrator who then notifies the party about the appointment. The neutral attempts to achieve a settlement by communication between parties and if any settlement is not reached at this stage, then the process moves to the last stage.[18] Once the neutral has failed in achieving an amicable solution then the neutral intimates the parties about how the final stage would occur and what process would be involved.[19]

2. Online Mediation

The other way in which this process can be done is through online mediation which appears to be the most effective model for small claim disputes as particularly in these cases, the dispute is not a matter of conflicting rights but customer services. While no regulation clearly provides for adopting only this method as the most effective, but a study conducted by the Centre for Information Technology and Dispute Resolution at the University of Massachusetts in 1999 demonstrated the effectiveness of online mediation through the case of eBay.[20] Online mediation is much like offline mediation, the only difference being that the entire process takes place in virtual space with the help of encrypted emails, secure chat rooms and maintaining confidentiality. The process starts with the filing of a dispute on the website,

[17] UNICTRAL Technical Notes, Section VII.
[18] UNICTRAL Technical Notes, Section VIII.
[19] UNICTRAL Technical Notes, Section IX.
[20] Ethan Katsh, Janet Rifkin and Alan Gaitenby, 'E-Commerce, E-Disputes and E-Dispute Resolution: In the Shadow of "eBay Law"' (2000) 15(3) Ohio State J Dispute Resolution <https://www.umass.edu/cyber/katsh.pdf> accessed 26 April 2022.

and then a mediator is either appointed by the website or chosen by parties wherein they are informed by the governing rules. The mediator then goes on to introduce themselves and the mediation process commences which is mostly done in text-based formats.[21] Globally, e-commerce entities have been practising this. For example- SquareTrade offers a platform for online mediation wherein people and businesses come on their site and settle a dispute.[22]

India too has embarked on this journey as the National Law School of India University (**"NLSIU"**) Bangalore in the year 2016 established its Online Consumer Mediation Centre under the aegis of the Ministry of Consumer Affairs, wherein they aim to resolve the consumer dispute through their web portal which is speedy and affordable.[23]

3. Crowdsourced Online Dispute Resolution

This kind of trial is a form of crowd justice and has a non-binding nature thus helping in settling small claim disputes effectively and timely.[24] Currently, there exist various Crowdsourced ODR services providers who

---

[21] K J Hopt and F Steffek (eds), *Mediation: Principles and Regulation in Comparative Perspective* (OUP, Oxford 2013) <https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780199653485.001.0001/acprof-9780199653485 accessed> 26 April 2022.

[22] 'Effective Dispute Resolution' (*Squaretrade.com*, 2022) <https://www.squaretrade.com/merchant/pop/fees_effective_odr.html> accessed 4 May 2022.

[23] 'NLSIU Online Consumer Mediation Centre' (*National Law School of India University* 2016) <https://www.nls.ac.in/centres/online-consumer-mediation-centre/> accessed 26 April 2022.

[24] Richard A. Posner, 'The Summary Jury Trial and Other Methods of Alternative Dispute Resolution: Some Cautionary Observations', (1986) 53 U Chicago L Rev <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2880&context=journal_articles> accessed 26 April 2022.

resolve the dispute through online opinion polls, online mock juries or decisions by private parties. An example of online opinion poll are platforms such as iCourthouse (www.icourthouse.com), SideTaker (www.sidetaker.com), AllRise (www.allrise.com), People's Court Raw, Truveli (www.truveli.org). On all these websites, the complainants post their queries and the internet users provide feedback on the same. This process usually is neither binding nor is a form of dispute resolution. However, it becomes useful in the current scenario for it acts as a deterrent to the complainant from proceeding with the case in instances where she receives negative feedback on her query.[25] Thus, it helps in reducing the number of complaints being filed and minimizing the burden on the judiciary.

4. Blind Bidding

This process has been popularized by the ODR platform 'Cybersettle' which helps resolve the monetary dispute between both B2B and B2C consumers. The contending parties submit their offers and demands that they expect from each other without disclosing what the other party has submitted. If the amount of both parties falls within the same range, then they make the payment and end the dispute else the website prompts them to submit another offer.[26]

5. Conciliation

Conciliation, as defined, is the process of persuading parties to reach an agreement and appears to be effective in settling consumer disputes.

---

[25] APC, 'Crowdsourced Online Dispute Resolution' (*APC*, 21 July 2011) <https://www.apc.org/fr/node/12693> accessed 26 April 2022.
[26] Cybersettle <http://www.cybersettle.com/> accessed 26 April 2022.

Mexico's ODR mechanism relies on the process of conciliation. The Federal Consumer Prosecutor's Office (**"PROFECO"**) of Mexico created a website, Concilianet[27] where consumers can file a complaint either against manufacturers or service providers who have agreed to resolve their disputes via this website. The consumers who register on this website provide all the necessary documents which are then analyzed by PROFECO. After analyzing the documents online, conciliation is organized between the parties and a conciliator is appointed. The manufacturer or the service provider is mandated to appear if a complaint is filed on this website failing which they will have to pay a fine.

C. Enforcement Of ODR Awards

In the current mediation framework, there exists a lack of certainty regarding the enforceability of mediation settlement agreements. To start with, they don't fall within the ambit of Section 74 of the Arbitration and Conciliation Act, 1996 (A&C Act, 1996) and therefore are not capable of being enforced under that legislation.[28] At this juncture, it is pertinent to note that conciliation differs from mediation in the sense that while the former is covered within the A&C Act, 1996, proceedings under the latter are deemed to be a Lok Adalat, thereby making settlements as enforceable as decrees.[29] While the court-referred mediation process still has recognition under Legal Services Authorities Act, 1987[30], there is no recognition for private mediation

[27] 'Concilianet' (Concilianet) <https://concilianet.profeco.gob.mx/Concilianet/inicio.jsp> accessed 26 April 2022.
[28] *Angle Infrastructure Pvt Ltd v Ashok Manchanda & Ors*, 2016(2) Arb LR 394 (Delhi).
[29] *Afcons Infrastructure and Ors v Cherian Verkay Construction and Ors*, 2010 (8) SCC 34, para 19.
[30] The Legal Services Authorities Act, 1987 (Act 39 of 1987), s 21.

initiated outside the four walls of the courtroom.[31] To effectively promote ODR as an alternative to traditional litigation, it is paramount to ensure that the awards have legal recognition and sanctity, otherwise, there would be no incentive for conflicting parties to engage in the same.

In India, there already exists a platform called SAMA which functions as an ODR platform helping persons seek resolutions to their disputes. It utilizes the correct mix of legal processes used in ADR mechanisms and ICT as it functions as an 'Online Lok Adalat'.[32] The online portal provides a concise procedure to reach an agreement on the platform. First, the parties sign up on the platform and explain their dispute after which a qualified conciliator is appointed. Second, parties make their respective offers and counter-offers and discuss settlement terms. Once the parties come to an agreement, the final settlement agreement is drafted by the qualified conciliator. Once signed, it has the legal sanctity of an arbitral award and can be enforced akin to a court decree. The portal provides detailed rules and procedures which are to be followed.[33] Other platforms such as eBay and PayPal also provide their own ODR platforms which act as a mediation platform for customers.[34]

Promotion and recognition of such platforms will surely go a long way in establishing ODR as an effective resolution method, especially in the

---

[31] *Shri Ravi Aggarwal v. Shri Anil Jagota*, (2009) SCC Online Del 1475.

[32] 'SAMA: Online LokAdalat' (*SAMA*) <https://www.sama.live/lokadalat.php> accessed 26 April 2022.

[33] 'SAMA Rules and Procedure' (*SAMA*, 2021) <https://www.sama.live/rules_and_procedures-2021.php#_Toc62347161> accessed 26 April 2022.

[34] PayPal, 'Resolving a dispute with your seller' <https://www.paypal.com/in/webapps/mpp/buyer-dispute-resolution> accessed 26 April 2022.

backdrop of the government's flagship initiatives such as 'Digital India', which aim to improve the use of ICT in public services ecosystem.[35]

III. ODR FRAMEWORK IN B2B: USE OF GENETIC ALGORITHM

A vast amount of research has been done on methods of resolving consumer disputes through ODR but there exists little or no data on how a dispute between traders shall be redressed via the ODR platform. However, a method called Genetic Algorithm (**"GA"**) has been proposed to resolve B2B disputes.[36] A GA as defined is an Artificial Intelligence (**"AI"**) tool used for a settlement-oriented system that helps in dealing with negotiation support.[37] How this GA functions is similar to the functioning of dispute settlement mechanisms in B2C and appears to be more effective in B2B disputes. Why this model seems to be more effective in B2B disputes is because of threefold reasons: Firstly, both the parties herein come up with an economically efficient solution. Secondly, this not only resolves the dispute but also builds confidence between the parties.[38] Thirdly, in B2B disputes, the number of disputed goods is higher and therefore this process becomes more effective as can be seen from the case of SmartSettle wherein the process of GA was proved cost-efficient in B2B disputes.[39]

---

[35] 'About Digital India' (*Government of India*) <https://www.digitalindia.gov.in/> accessed 26 April 2022.

[36] Colin Rule, *Online Dispute Resolution for Businesses. B2B, E-Commerce, Consumer, Employment, Insurance, and Other Commercial Conflicts* (San Francisco: Jossey Bass 2002).

[37] D. Ilter and A. Dikbas, 'A Review of the Artificial Intelligence applications in Construction Dispute Resolution' (26th International Conference on Managing IT in Construction, Istanbul 2009) 41-50.

[38] Ethan Katsh, 'Online Dispute Resolution: Some Implications for the Emergence of Law in Cyberspace' (2007) 27(2) Intl Rev L Computers and Technology, 97–107.

[39] Cortés P, 'Online Dispute Resolution For Consumers In The European Union' (*Econstor.eu*, 2010) <https://www.econstor.eu/bitstream/10419/181972/1/391038.pdf> accessed 4 May 2022.

The phases of GA include[40]: First, gathering information wherein each party fills a questionnaire so that they know the each other's position. Second, each party then proposes their solutions with a different variant. Third, then these solutions are rated on a scale of 0 to 10. Fourth, based on the assessment, the GA then chooses the best. Fifth, both the parties express their opinion on the option selected and then either they can succeed or fail in resolving the dispute or continue with the negotiations. Illustrating the same: if Grocer, a retail store needs a quintal of rice and approaches Z, a dealer who delivers a substandard product. Then using this GA process, Grocer and Z would first fill out a questionnaire, then provide their solutions, out of which the best solution would be picked by the GA, thus making the entire process cost-efficient and less time-consuming.

The application of this B2B dispute resolution can be seen in the framework of the Asia-Pacific Economic Cooperation (**"APEC"**) wherein any business of one economy can file an online consumer dispute against any other business in another economy. The only prerequisite is that both these businesses have consented to ODR being a dispute redressal mechanism.[41]

IV. PRINCIPLE FRAMEWORK FOR ODR PLATFORMS

ODR functions as an interplay of detail-oriented legal processes inspired by ADR legislations such as the A&C Act as well as a strong ICT infrastructure powered by artificial intelligence/machine learning (**"AI/ML"**)

[40] Nikola Simkova and Zdenek Smutny, 'Conceptual design of online dispute resolution in B2B relationships' (24th Interdisciplinary Information Management Talks, Podebrady, 2016) 303-310.
[41] APEC, 'APEC Collaborative Framework for Online Dispute Resolution of Cross-Border Business-to-Business Disputes' In: Second Economic Committee Meeting (2019).

to facilitate timely justice done in a transparent manner. It must be ensured that both these tools – ADR rules and ICT infrastructure – operate within a robust principal framework. Thus, this section, taking inspiration from the UNCITRAL Technical Notes on ODR[42], attempts to provide for a robust principal framework within which the ADR processes and ICT infrastructure must operate:

A. Legal Principles

- Principles of natural justice: It must be ensured that ODR platforms provide fair and equal opportunity of hearing to the parties as well as eliminate the possibility of incidents of malfeasance by either the parties or the neutral.

- Timely justice: The unique selling proposition (**"USP"**) of ODR is the time-bound resolution of disputes, therefore measures must be taken to ensure the same.

- Accessibility: In order to make the whole process more inclusive, ODR platforms should strive to provide user-friendly portals so that people from all regions and backgrounds can utilize the services.

- Accountability: The conduct of ODR platforms and their use of the ICT infrastructure in the resolution process must be regulated by either external regulators or internal accountability frameworks to ensure accountability.

[42] UNICTRAL Technical Notes.

B. ICT Principles

- Open source: The use of open-source software which can be freely available and widely distributed without any hindrances must be advocated for. This will have an impact on two levels – one, to aid the collective growth of the ODR ecosystem and two, greater adaptability to new features and expansion to wider territories and regions. At the nascent stage that ODR is in our country in the present, open-source software will facilitate customizing, modifying and distributing the technology in an autonomous manner.[43] Credible precedence can be found in the e-Courts project which has effectively utilized Free and Open-Source Software (**"FOSS"**) in enabling courts across various jurisdictions with the necessary tools to function in an online manner.[44]
- Privacy and security: Resolving disputes using digital infrastructure raises obvious concerns regarding the privacy of sensitive information and evidence involved. Therefore, a sound infrastructure which ensures the security of private information becomes relevant.
- Actionability: ODR platforms will be required to be dynamic in nature thereby having the ability to continuously adapt to technological advancements and function within the legal ecosystem with the skill to critically analyze and act upon the metadata being made available to them.

---

[43] 'Designing The Future of Dispute Resolution: The ODR Policy Plan For India' (*Niti.gov.in*, 2021) <https://www.niti.gov.in/sites/default/files/2021-11/odr-report-29-11-2021.pdf> accessed 4 May 2022.

[44] Goswami Y, 'Innovations Phase II Of The Ecourts Project' (*Ecourts.gov.in*, 2019) <https://ecourts.gov.in/ecourts_home/static/manuals/FINAL%20INNOVATIONS%20IN%20PHASE%20II.pdf> accessed 4 May 2022.

V. CONCLUDING REMARKS: BRINGING CHANGES IN THE STATUS QUO

Online redressal mechanisms not only provide timely and transparent justice to the parties but also alleviate the overall E-Commerce experience for consumers as well as businesses. In order to substantively and effectively inculcate a robust ODR mechanism in India, we suggest a few changes in the current legislative framework.

First, the Consumer Protection (E-Commerce) Rules, 2020 under the Consumer Protection Act, 2019 were notified recently with the intention to protect consumer interest in the e-commerce ecosystem. They apply to every good and service brought or sold over digital/electronic networks and thus have a wide scope and applicability. The increased responsibility the rules place on the e-commerce platform to ensure consumer protection is noteworthy. Still, concerns loom about whether they apply to B2B disputes as well.[45] The rules introduce the term "user" to define 'any person (individual and/or company) who accesses/avails any compute resource of an e-commerce entity'.[46] While the Consumer Protection Act, 2019 calls for full disclosure to consumers about the sellers, details of goods and services sold and payment mechanisms available on the platform,[47] the term "user" opens up a new avenue for ambiguity as there is room for confusion as to whether the scope

[45] Legacy Law Offices, 'E-Commerce Rules, 2020, A Boon or a Bane?' (*Mondaq.com,* 4 November 2021*)* <https://www.mondaq.com/india/dodd-frank-consumer-protection-act/1128900/e-commerce-rules-2020-a-boon-or-a-bane> accessed 26 April 2022.
[46] Consumer Protection (E-Commerce) Rules, 2020, s. 3(1).
[47] The Consumer Protection Act, 2019 (Act 35 of 2019), ss 5, 7.

of the rules applies to B2B transactions as well.[48] At this juncture, we propose that the rules be amended to explicitly include a provision for the establishment and use of an ODR platform as the first means of dispute resolution. Further, clarity must be given on the applicability of the rules to B2B disputes.

Second, the development of a robust ODR platform presents two requirements in terms of logistical support – technological capacity and trained professionals. It must be noted that internet users only account for about 45% of the total population in the country.[49] Limited internet penetration acts as a hindrance to ODR adoption across India, and therefore must be dealt with both by the government and private entities in partnership with each other. Furthermore, ODR requires trained professionals to act as neutrals since they act as the limited human intervention source in the process. For this purpose, the government must step forward and create a cadre of well-trained ODR professionals. The formation of a Mediation Council of India, along the lines of the Arbitration Council of India, will go a long way in aiding this process – as was recommended by MCPC in their draft mediation legislation.[50]

Third is the need to improve the digital infrastructure. Some pre-requisites to resolving disputes online are access to computers, internet

---

[48] Trilegal, 'Consumer Protection (E-Commerce) Rules, 2020' (*Mondaq.com*, 2022) <https://www.mondaq.com/india/dodd-frank-consumer-protection-act/980140/consumer-protection-e-commerce-rules-2020> accessed 4 May 2022.

[49] Tanushree Basuroy, 'Internet Penetration Rate in India 2007-21' (*Statista.com*, 15 March 2022) <https://www.statista.com/statistics/792074/india-internet-penetration-rate/> accessed 26 April 2022.

[50] Ajmer Singh, 'Supreme Court forms committee to draft mediation law, will send to Government' (*The Economics Times*, 19 January 2020) <https://economictimes.indiatimes.com/news/politics-and-nation/supreme-court-forms-committee-to-draft-mediation-law-will-send-to-government/articleshow/73394043.cms?from=mdr> accessed 26 April 2022.

connection and technical know-how. Hopes can be placed on the work done by the government under the National Digital Communication Policy, 2018 under which the resolve to provide universal broadband connectivity is undertaken.[51] Moreover, in order to improve digital literacy, the efforts made by the government under the Pradhan Mantri Gramin Digital Saksharta Abhiyaan to improve internet penetration in rural India are projected to bridge the digital gap.[52]

The future of justice delivery and dispute resolution lies in employing advanced technology for timely, transparent and reliable justice.[53] For this purpose, developing an effective ODR mechanism will require not only legal principles but also a strong ICT infrastructure. India already has the foundational structure for it in terms of e-commerce rules and a few private initiatives, but what is now required is a clear multi-pronged strategy to truly inculcate ODR mechanisms for dispute resolution in India.

[51] Department of Telecommunication, 'National Digital Communication Policy 2018' (2018) <https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf> accessed 26 April 2022.
[52] PMGDISHA, 'Objective' (*Ministry of Electronics and Information Technology, Government of India*) <https://www.pmgdisha.in/about-pmgdisha/> accessed 26 April 2022.
[53] Richard Susskind, 'The Future of Courts' (2020) 6 (5) The Practice <https://thepractice.law.harvard.edu/article/the-future-of-courts/> accessed 26 April 2022.

II. DATA LOCALISATION AND CROSS-BORDER FLOW OF DATA: BALANCING THE INCONGRUENT DIMENSION OF BARRIERS, SAFEGUARDS AND "FREE FLOW OF DATA"

- Raj Shekhar & Aman Yuvraj Choudhary[*]

ABSTRACT

The growth in today's century has been seen to go hand in hand with the globalization of society; a phenomenon of which the Internet can be seen to be a cause and a component, as well as a reflection. Data localization often refers to those policy measures which are aimed at restricting the free flow of data by limiting the physical storage and processing of data within a given jurisdiction's boundaries. The phenomenon has started to garner a plethora of international support with many countries having adopted localization policies to combat multiple concerns over the free flow of data. However, the usage of "free flow" and "data localization" seems ambiguous owing to their antagonistic nature and has been criticized by experts citing it to be against the very spirit of the internet – connectivity without barriers. The Joint Parliamentary Committee to which the Personal Data Protection Bill, 2019 was referred has once again stirred the international debate surrounding data localization by strongly supporting its implementation. In light of these issues, this paper tries to understand the plan of action, structure and objectives of data localization by the Indian Government while simultaneously carrying out a hedonistic analysis of their overall impact. It further carries out a global comparative analysis of the existing data localization practices in other mature jurisdictions and pitches forth conducive suggestions to aid in the proper implementation of such policies without hampering the crucial element of cross-border data transfer.

[*] The authors are fourth and third-year students of B.A. LL.B. (Hons.) respectively at National University of Study and Research in Law, Ranchi. Views stated in this paper are personal.

I. INTRODUCTION

The growth in today's century has been seen to be in concert with the globalization of society; a phenomenon of which the Internet is a component, a cause, and a reflection. On account of this digitalization, the concept of data privacy has assumed a position of paramount importance in the present-day digital space. This is evident from the emphasis that governments around the world, including India, have put on developing data privacy legislations. While legislations such as the General Data Protection Regulation (**"GDPR"**)[1] have proved instrumental in acting as guiding beacons, the policymakers still don't consider it sufficient. As a result, the concept of data localisation has become a significant policy issue in many countries including India. In general parlance "Data localisation" refers to the myriad policy measures that restrict the free flow of data across geographic boundaries.

The acceptance of the premise that *"data is the new oil"* has led to the origination of data protection laws worldwide, creating a variety of legal and

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

commercial challenges for global organizations.[2] Data localisation which effectively restricts the cross-border transfer of data is one such. The phenomenon has started to garner a plethora of international support with many countries having adopted localisation policies to combat multiple concerns over the free flow of data. However, the usage of phrases "free flow" and "data localisation" seems ambiguous owing to their antagonistic nature and has been criticized by experts citing it to be against the very spirit of the internet – connectivity without barriers. The Joint Parliamentary Committee to which the Personal Data Protection Bill, 2019[3] was referred has once again stirred the international debate surrounding data localisation by strongly supporting its implementation.

The Indian Government has stated four wide objectives behind introducing the data localisation requirements which are: (i) securing more convenient access to personal data for law enforcement, (ii) bolstering economic growth and employment, (iii) preventing foreign surveillance, and (iv) better enforcement of data protection laws.[4] However, there has been no elaboration on how such a stringent data localisation policy would lead to accomplishment of these objectives (without hampering the cross-border flow of data) which is essential to globalization and development. In light of these issues, this paper tries to understand the plan of action, structure, and

[2] 'Data Protection and Privacy Legislation Worldwide' (*UNCTAD*) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 28 April 2022.

[3] 'Joint Committee on the Personal Data Protection Bill, 2019' (*PRS Legislative Research*, 28 April 2022) <https://prsindia.org/parliamentary-committees/joint-committee-on-the-personal-data-protection-bill-2019> accessed 28 April 2022.

[4] Anirudh Burman and Upasana Sharma, 'How Would Data Localisation Benefit India?' (*Carnegie India*, 2021) <https://carnegieendowment.org/files/202104-Burman_Sharma_DataLocalization_final.pdf> accessed 28 April 2022.

objectives of data localisation by the Indian Government while simultaneously carrying out a hedonistic analysis of their overall impact.

II. THE EVOLUTION OF DATA LOCALISATION: ANALYSING THE DIFFERENT APPROACHES TO DATA LOCALISATION

As previously emphasized, the "data localisation" requirements have evolved and covered a majority of countries. The number of countries with data localisation legislation has almost doubled to 62 in 2021 from 35 in 2017.[5] This stands true for the total number of data localisation policies which have also more than doubled to 144 in 2021 from 67 in 2017. Another 38 data localisation policies have been proposed or considered in countries around the world in which China (29), India (12), Russia (9), and Turkey (7) are world leaders in requiring forced localisation within their respective territorial jurisdictions.[6]

On a closer analysis of the requirements and consequently the effects, data localisation measures can be classified under three major heads. To begin, several nations prohibit the transfer of certain types of data outside of their boundaries which include, but are not limited to:

- Personal data;
- health and genomic data;

[5] Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (*Information Technology and Innovative Foundation*, 19 July 2021) <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/> accessed 28 April 2022.

[6] Rajat Kathuria and Mansi Verma, 'Economic Implications of Cross Border Data Flows' (*Indian Council for Research on International Economic Relations*, November 2019) <https://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf> accessed 2 July 2022.

- mapping and geospatial data;
- government data;
- banking, credit-reporting, financial, payment, tax, insurance, and accounting data;
- publicly-traded company-internal data;
- data related to user-generated content on social media and the Internet service platforms;
- subscriber data, and communications content and metadata for traditional telecommunications and Internet-based communication services;
- and e-commerce data.

The restriction on such data transfer and a need for its localisation is based on the nature of these data being "critically sensitive" in nature.[7] For example, the USA under its Defense Federal Acquisition Regulation Supplement[8] requires an unconditional localization of critical information for operational security and national defence. Further, Russia provides for unconditional mirroring of all personal data of Russian Citizens under Federal

[7] Rishab Bailey and Smriti Parsheera, 'Data Localisation in India: Questioning the Means and Ends' (2018) National Institute of Public Finance and Policy Working Paper No. 242, 2018 <https://macrofinance.nipfp.org.in/PDF/BP2018_Data-localisation-in-India.pdf> accessed 28 April 2022.

[8] Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018).

Law.[9] Similar is the case with other prominent countries: China,[10] Indonesia,[11] Australia,[12] EU[13] *inter alia*.

Secondly, we are witnessing instances where countries are restricting data under broad umbrella categories involving data labeled as "sensitive," "important," "core," or related to national security, which often impacts a wide range of commercial data.[14] While this development in itself is alarming, in India, a broad framework targeting non-personal data is also proposed to be introduced which shall further extend the ambit of these vague data brackets. For example, the proposed framework in India is based on a similar model. While extensive data localization plans are being chalked out, hardly any heed is being paid to define the categories of data on which such measures would be implemented.[15]

Thirdly, the emergence of de facto localisation seems to have gained pace. This type of data localisation requirement makes the transfer of data extremely complicated and cost-extensive, as a result of which firms are

[9] Federal Law Number 242 – FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation.

[10] Yuxi Wei, 'Chinese Data Localization Law: Comprehensive but Ambiguous' (*University of Washington Henry M. Jackson School of International Studies*, 7 February 2018) <https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/> accessed 28 April 2022.

[11] Regulation of the Government of the Republic of Indonesia Number 82 of 2012 Concerning Electronic System and Transaction Operation.

[12] 'My Health Records Amendment (Strengthening Privacy) Bill, 2018' *Australian Parliament* (2018) <https://www.aph.gov.au/Parliamentary_Business/bills_LEGislation/bills_Search_Results/Result?bId=r6169> accessed 2 July 2022.

[13] 'EU Data Protection Rules' (*European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en> accessed 2 July 2022.

[14] cf Burman (n 4).

[15] Vikram Jeet Singh and Kalindhi Bhatia, 'What's Driving Data Localisation in India?' (*Mondaq*, 6 May 2020) <https://www.mondaq.com/india/data-protection/928916/what39s-driving-data-localisation-in-india-> accessed 4 May 2022.

spared no option other than storing the data locally. For example, the European Union's removal of data transfer mechanisms, failure to add new certifications and other new legal tools for data transfers, and ever-ratcheting up of restrictions and conditions for the remaining mechanisms (such as standard contractual clauses) have the potential to make GDPR the world's largest de facto localisation framework.[16] Other examples include explicit consent requirements for personal data transfers and the need to submit data transfers for opaque and ad hoc authorization.

III. INDIA'S TAKE ON DATA LOCALISATION: WHY A SUDDEN PUSH?

It is believed that the regulatory interest in data localisation has gained impetus recently, however, there existed laws almost a decade back which indirectly had the essence of data localisation. In the year 2007, when the terms of the unified telecom license agreement requirements were released, the telecom service providers of India were mandated to not transfer certain information on subscribers outside India.[17] Further, as per the Companies Act, 2013,[18] companies registered in India are to maintain their books of accounts for audit and inspection in India only. The Insurance Regulatory and

[16] Nigel Cory, Ellysse Dick, and Daniel Castro, 'The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade' (*Information Technology and Innovative Foundation*, 17 December 2020) <https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade> accessed 2 July 2022.
[17] 'Licensing Framework for Telecom: A Historical Overview' (*Centre for Internet & Society*) <https://cis-india.org/telecom/resources/licensing-framework-for-telecom> accessed 28 April 2022.
[18] The Companies Act, 2013 (Act 18 of 2013).

Development Authority of India mandates all original policyholder records to be maintained in India.[19]

These requirements that existed much before the ongoing push are a clear indicator that data localisation had existed before and all we are witnessing today is an aggravated plan of its implementation on an expanded plane. The most recent push in this direction has been the data localisation restrictions placed on payment data by the Reserve Bank of India (**"RBI"**) which on April 6, 2018, issued a circular mandating all payment system providers to store payment data locally, exclusively in India.[20]

These developments would surely make us question the rationale behind such data localisation rules. While no straight jacket idea is provided, several rationales are given for data localisation. In certain policies where such requirements are implemented the reasons are included in the document or rule itself. For example, in the above example where RBI mandated payment data localisation, the rationale provided was to ensure an "unfettered supervisory access" to "ensure better monitoring", and protect consumer interests. However, broadly the below-mentioned subheads constitute the rationale behind data localisation requirements:

[19] Insurance Regulatory and Development Authority of India (Minimum Information Required for Investigation and Inspection) Regulations, 2020 (F. No. IRDAI/Reg/3/169/2020).

[20] Guidelines on Storage of Payment Data, (*RBI*, 2018), <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244> accessed 2 July 2022.

A. Protection of Individual Rights

Post the Supreme Court's verdict in *Justice K.S. Puttaswamy v. Union of India*,[21] a special emphasis has been supplied on the protection of an individual's privacy. As a result, attempts are being made to build a robust data protection regime that balances legitimate concerns of the state and individual interests. The Personal Data Protection Bill was accompanied with an expert committee report which justified the need for data localisation[22] on the pretext that with the changing dynamics of cyberspace, the data of Indian citizens is being exposed to foreign surveillance and attacks. Therefore, if data is hosted abroad, an effective remedy against foreign-service providers will not be available for Indians which they may have had if the data was hosted locally.[23]

B. National Security Concerns and a Better Access for Investigatory Authorities

National Security stands as the major contention put forward time and again to justify the rigorous data localisation requirements. The justification being certain critical information (such as telephone numbers) might jeopardize state security, while other data can be vital to a country's financial well-being (like payment data). The Indian Information Technology Act of 2000[24] (**"IT Act"**) has an extraterritorial application; however, it has proven

---

[21] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[22] Padmini Ray Murray and Paul Anthony, 'Designing for Democracy: Does The Personal Data Protection Bill 2019 Champion Citizen Rights?' (*Economic and Political Weekly*, 2 June 2020) <https://www.epw.in/engage/article/designing-democracy-does-personal-data-protection> accessed 28 April 2022.
[23] Ministry of Electronics and Information Technology, 'White Paper Of The Committee Of Experts On A Data Protection Framework For India' (2017).
[24] Information Technology Act, 2000 (Act 21 of 2000).

to be ineffective. For example, there have been instances where the investigation agencies have to face a dead-end owing to the foreign nations, where the required data is stored, declining to co-operate even though letters rogatory (that are issued by courts) under mutual legal assistance treaties (**"MLAT"**) to access evidence in other jurisdictions have been presented.[25] As a result, it is believed that data localisation could help in overcoming these barriers.

C. Economic Protectionism and Promotion of Indigenous Players

The requirements of data localisation which lead to the on-soil presence of data provide an economic advantage to local firms. While it cannot be denied that there are unintentional side effects, however, the local players are usually much better equipped to tackle those. For India, this is not an unusual regulatory position. Foreign investment and exchange control restrictions in India continue to limit the use of foreign currency in specific industries and activities. Foreign engagement in certain sectors, such as multi-brand retail, is still limited. In the last two decades, there has been a movement in India to open up to more international investment and engagement. [26]

A bare perusal of the above pointers is enough to substantiate the point that data localisation could indeed be a great tool of redemption. However, a critical analysis would also uncover the fact that almost every proposal for data localisation has a combination of motives. When their primary (hidden)

---

[25] Amber Sinha, 'MLAT Report' (*Centre for Internet & Society*, 20 May 2018) <https://cis-india.org/internet-governance/files/mlat-report/view> accessed 28 April 2022.

[26] 'FDI in India: Foreign Direct Investment Opportunities Policy' (*India Brand Equity Foundation*, 1 March 2022) <https://www.ibef.org/economy/foreign-direct-investment> accessed 28 April 2022.

purpose is protectionism, national security, more control over the Internet, or any mix of these, policymakers frequently employ a "dual-use" strategy with an official and ostensibly legitimate goals, such as data privacy or cybersecurity. In certain circumstances, such as India, all of them are used. A lack of proof, openness, discussion, and involvement surrounding a data localisation plan is a clear indicator of hidden objectives.[27]

IV. DATA LOCALISATION AND BALKANIZATION OF INTERNET: INTERNET NO LONGER "FREE AND AFFORDABLE"?

Internet was envisioned to be free, unrestricted, and interoperable. The entire idea behind a global network was to create an essentially free channel for the flow of data without regard for national borders. Under such a system, the data was supposed to move from location to location quickly in the most efficient manner with or without the consent and knowledge of the user. Such a free cross-border data flow has led to the development of previously unheard technical efficiencies in storing and processing data that was previously thought to be non-existent. One of the major outcomes of this borderless data transfer can be seen in technical innovations such as cloud computing, which distributes data across multiple data centers to provide cost-effective and efficient ways where users have on-demand access to a shared pool of

[27] Usman Ahmed and Anupam Chander, 'Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows' (2015) *UC Davis Legal Studies Research Paper Series*, Research Paper No. 480 <http://ssrn.com/abstract=2731888> accessed 02 July 2022); Jonah Force Hill, 'A Balkanized Internet? The Uncertain Future of Global Internet Standards' (2012) Georgetown J Intl Affairs 49, 49.

processing and storage resources, while the data's real physical location(s) is mainly hidden from view.[28]

The emphasis being provided on data localisation is bound to balkanize the Internet as we know it today and lead to the fragmentation of the global network into "various distinct, idiosyncratic '(I)nternets,'" resulting in delays, inefficiencies, and higher costs.[29] The data localisation requirements imposing stringent conditions have led to a situation where the existing internet would need a significant redesign of its technical architecture to adapt to the rigorous requirements.

Data localisation requirements would further force the global service providers to develop physical infrastructure in each jurisdiction separately leading to a drastic rise in the associated costs and administrative burdens. This would significantly impact the accessibility of services to the customers who would not be in a state to bear the hiked price. Moreover, this would lead to service providers operating in a "complex array of different jurisdictions imposing conflicting mandates and conferring conflicting rights."[30] Consequently, the data localisation requirements would jeopardize the benefits individual users and businesses enjoy owing to the integration of existing globalization and the economy.

---

[28] Judith Rauhofer and Casper Bowden, 'Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud' (2013) U of Edinburgh School of L, Research Paper Series No 2013/28 1, 25 <https://ssrn.com/abstract=2283175> accessed 28 April 2022.
[29] Sascha Meinrath, 'We Can't Let the Internet Become Balkanized' (*Slate*, 2013) <https://archive.ph/jSwgF> accessed 28 April 2022.
[30] ibid.

V. DRAWBACKS OF DATA LOCALISATION: THE UNSEEN CORRIDORS OF PLACEBIC SAFETY AND DEVELOPMENT

The major thrust of arguments supporting data localisation has derived legitimacy from the supposed "safety, integrity, and security" factors that such a practice promises. However, the claims fall flat on a deeper analysis of the existing and the promised future post-data localisation. To have a better understanding, a brief analysis of the same becomes imperative.

A. Data Security

Data localisation is touted as a means to promote and enhance data security by implementing a framework to ensure the privacy and security of individual data from non-state actors.[31] However, the fact that existing data is protected through best practices and state-of-the-art technology, and local storage would have no better access to such practices and technologies than leading global companies, leads to a belief that there will be instances when such local storage would not apply the same rigor due to fewer financial resources and less available expertise. As a result of these flaws, firms may face legal responsibility and poorer customer confidence as a result of being restricted to data processing and/or storage within the boundaries of nations with inferior data security standards. This clearly reflects the fact that data localisation requirements could lead to increased risks of a breach.

[31] Patrick Ryan, Sarah Falvey and Ronak Merchant, 'When the Cloud Goes Local: The Global Problem with Data Localisation' (2013) 46 Computer 54, 54, 56.

B. Preventing Foreign Surveillance

Preventing foreign surveillance is another justification for data localisation laws, which are grounded in the belief that placing data abroad jeopardizes security and privacy. This argument has gained momentum in recent days with the world witnessing increased cyber warfare from Russia and China.[32] There exists no cogent rationale behind claiming that data localisation can effectively tackle foreign surveillance activities. For example, the Russian data localisation law provides for copies of data relating to Russian citizens to be transferred internationally and stored on servers outside Russia.[33] Further, localisation in no way prevents surveillance, as physical access to the data storage or processing facilities is not technically necessary to conduct surveillance activities.[34] In contrast, such a measure could lead to an even increased ease owing to foreign players getting an edge by recognizing and concentrating their efforts in a particular direction. Thus, the entire argument about foreign surveillance falls flat too.

C. Promotion of Domestic Economic Development

Data localisation regulations are frequently touted as a way to encourage domestic economic growth; yet, there are strong grounds to assume

---

[32] Audrey Conklin, 'Chinese Cyberattacks on NATO Countries Increase 116% since Russia's Invasion of Ukraine: Study' (*Fox Business*, March 26, 2022) <https://www.foxbusiness.com/technology/chinese-cyberattacks-nato-increase-ukraine> accessed 28 April 2022.

[33] Christopher Millard, 'Forced Localisation of Cloud Services: Is Privacy the Real Driver?' (2015) 2 IEEE Cloud Computing <http://ssrn.com/abstract=2605926> accessed 2 July 2022.

[34] Advaya Legal, 'Data Localisation – Protection or Protectionism?' (*The Hindu Business Line*, 8 August 2021) <https://www.thehindubusinessline.com/business-laws/data-localisation-protection-or-protectionism/article35801546.ece> accessed 28 April 2022.

that they may have negative economic consequences.[35] Any improvements in the economy would most certainly be restricted to a few local firms, data centers, and related industries, with a limited scale of new employment. Data localisation could lead to incurring of significant infrastructure, data migration, and service-related costs without benefiting from the same efficiencies or economies of scale as global businesses. There is no denying that the introduction of data localisation requirements inevitably results in increased initial and ongoing costs for users, including domestic businesses. Furthermore, services may be unavailable if the related expenses are too high and the market is too small to make them economically viable. This might make it difficult for local enterprises to grow and participate in the global digital economy, especially in emerging markets that lack the technological infrastructure that is already available online.

Due analysis of the above-stated tri-fold argument clearly points to the fact that there exist no substantial grounds on which data localisation can be pushed as a necessity. The arguments generally put forth in support of data localisation hardly stand the test of logic and are backed by nothing more than flimsy claims as demonstrated above.

VI. UNDERSTANDING PROPORTIONALITY PRINCIPLE: TAKING A CUE FROM EU AND WTO JURISPRUDENCE

When referring to proportionality in data localisation measures, under international law such as EU law, WTO jurisprudence, academic literature,

[35] Ashish Aggarwal, 'Can Data Localisation Help Protect National, Economic Interests?' (*Mint*, 7 August 2018) <https://www.livemint.com/Opinion/P9bGTw36JUx8YTK0RxKGhN/The-economic-impact-of-a-strict-data-localisation-regime.html> accessed 28 April 2022.

and various trade agreements, weightage is given to considerations such as (1) whether the measures to be enacted are likely to fulfil the objectives pursued, (2) whether there is any less restrictive measure that could be enacted, and (3) whether the measure in question stands in a reasonable relation to the intrusion it will cause.[36]

In addition to this test of proportionality, the OECD Digital Economy Paper titled, 'Data Localisation Trends and Challenges: Considerations for The Review of the Privacy Guidelines' recommends (Recommendation 6) a list of comprehensive factors to be taken into account while determining proportionality. They are:

- data sensitivity;
- the object of the processing;
- whether, and the extent to which, data localisation measure effectively achieves the goals for which it was introduced;
- availability of any less restrictive measures;
- implications of the measures: international, national, direct, indirect etc.;
- evidence of intent (wherever possible to establish);
- and the implications likely to arise if also other countries adopt the same measure ('scalability' as a consideration in the assessment of proportionality).

With regards to data sensitivity, paragraph 18 of the OECD Privacy Guidelines lays down that there must be proportionality between the

[36] Dan Svantesson, 'Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines' No. 301 OECD Digital Economy Papers OECD Publishing, Paris <https://doi.org/10.1787/7fbaed62-en> accessed 28 April 2022.

restrictions (on cross-border flow of personal data) and the risk that flow of data represents. Such proportionality must be achieved by factoring in data sensitivity and purpose. Same idea shall find resonance in the Indian legislative landscape.

As regards to the object of the processing, evidence must be garnered to come to a conclusion as to whether the measures so opted for fulfilling the objects required to be fulfilled. Evidence is of key importance here.

In assessing proportionality and if there are any less restrictive measures that could be enacted, the assessor may fruitfully venture beyond domestic considerations and also take into account international consequences and implications, direct and indirect. There would be unwarranted friction where domestic data policy decisions are made without due considerations to the international policy trends. Path of minimal resistance may be preferred while making such legislative decisions so there is in turn minimal friction with the international community while keeping the national interests at high priority.

Another factor that should be considered is the scalability of the measure. That is to say that it must be considered that what would be the effect if multiple countries adopt the same mechanisms.[37] In assessing proportionality, it would be consequential to know that whether many countries already have or would adopt similar measures. If so, such large-scale adoption may point towards legitimacy of such measure. Adding factor of

[37] D Svantesson, 'Internet & Jurisdiction Global Status Report 2019' (*Internet & Jurisdiction Policy Network*, 2019) <https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Global-Status-Report-2019-Key-Findings_web.pdf> accessed April 28 2022.

scalability into proportionality assessment would level the playing field between developed and developing countries.

Significant weightage is given to state practice in international law[38] which gives an impetus to countries to engage in universal and scalable measures. Large scale adoption, for one, points to legitimacy. The OECD digital economy paper, further goes to recommend that the proportionality test must, as an additional factor, be equipped to evaluate justifications attached to localisation measures.[39] It must be able to consider what is behind the benign label of data security and localisation.

It is pertinent to note Dr Christopher Kuner's (A law professor and a leading lawyer in Brussels, Belgium, specializing in EU and global data protection and privacy laws) arguments on data nationalism which deem it synonymous with data localisation.[40] According to him, in proportionality, both objective and subjective standards should be applied. While conceding that subjective standards are difficult to work with, the paper recommends a subjective test to look at the relevant actor's interest, whether it is a legitimate interest towards localisation and protection or intended towards privacy and human rights violations. A method of making such distinction is also suggested: to look at whether the country has definite structure of data privacy that is running parallel at both international and national levels. If there is a measure restricting foreign policy violation, then there should be a

[38] Statute of the International Court of Justice (adopted on 17 December 1963, entered into force on 31 August 1965) 33 UNTS 993 art 38(1)(b).
[39] Alpha Partners, 'Update on Data Protection Law - Privacy Protection – India' (*Mondaq*, January 3 2022) <https://www.mondaq.com/india/privacy-protection/1146570/update-on-data-protection-law> accessed April 29 2022.
[40] Christopher Kuner, 'Data Nationalism and Its Discontents' (2014) 64 Emory L J, 2089.

concomitant domestic restriction. If not so, it can be assumed that such a restriction is favouring the government in power rather than the citizens.

The above-mentioned seven-pronged test clearly highlights the fact that proportionality in terms of the application of measures is given due weightage in mature jurisdictions. However, it is striking to note that even Indian jurisprudence has a similar test which shall be elaborated on in detail in the paragraphs that follow.

VII. THE INDIGENOUS "PROPORTIONALITY TEST": A PROBABLE SOLUTION?

The Doctrine of Proportionality is a constitutional doctrine that courts use to resolve conflicts and achieve balance when competing rights exist. There have been several decisions around the world in which courts have invoked this doctrine and resolved the conflict by holding that rights and limitations must be interpreted harmoniously to facilitate coexistence.[41] It is critical to ensure that any proposed framework for cross-border transfer prioritizes the interests of effective law enforcement and economic benefits to Indians.

There are three prominent arguments posited in favour of imposing stringent data localisation rules: sovereignty and government functions, which refer to the need to recognise Indian data as a resource to advance national interest (economic and strategic), and, further, to enable the enforcement of Indian law and state functions. The second argument is that local industry will profit economically from the development of local infrastructure, job creation,

[41] *Modern Dental College & Research Centre v. State of M.P.*, (2016) 7 SCC 353.

and contributions to the AI ecosystem. Finally, in terms of civil rights, hosting locally improves security and privacy by guaranteeing the application of Indian law to the data and users' access to local remedies.

Without a question, data localisation is a representation of the state's public power. The principle of proportionality is the "paramount clause" that must be followed when exercising public power; its requirements on the necessity, appropriateness, and balance of purpose and means are of immense directional relevance for governing data localisation according to law and setting reasonable limits for it.[42] There must be a rationale behind any manner of restriction in the name of localisation. The rationale must justify the extent of the requirement of localisation putting it at a reasonable nexus with the object sought to be achieved. The test, adopted by countries globally, is a shield protecting the civil liberties of individuals and against transgressions committed by the state authorities.

Holding privacy to be a fundamental right, the Supreme Court in *K.S. Puttaswamy Case* reiterated the four-pronged proportionality test:

- ‘A measure restricting a right must have a legitimate goal (legitimate goal stage).
- It must be a suitable means of furthering this goal (suitability or rationale connection stage).
- There must not be any less restrictive but equally effective alternative (necessity stage).

[42] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, 221.

- The measure must not have a disproportionate impact on the right holder (balancing stage).'

Furthermore, Chandrachud J. drawing on the concept of proportionality, which is also used in EU law to balance competing interests, notes that any invasion of life or personal liberty must meet the three requisites of (a) legality, i.e., there must be a law in existence; (b) legitimate aim, which he illustrates as goals such as national security, proper deployment of national resources, and revenue protection; and (c) proportionality of the legitimate aim and measure adopted.[43]

The probable purpose of such a policy designed to impose limits must be defined in the first step. It should be mentioned that such a purpose must be legal. However, before deciding on the aforementioned approach, the authorities must consider the presence of any other mechanism that would advance the aforementioned purpose. The appropriateness of such a policy is determined by its implications for basic rights as well as its need. The aforementioned ruling makes it clear that the State can only use the least restrictive measure possible in light of the facts and circumstances. Finally, because the order has important implications for the basic rights of affected parties, it should be backed by appropriate evidence and be subject to judicial scrutiny. The application of this test has been witnessed in leading cases such

[43] Vrinda Bhandari and others, 'An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict' (2017) 11 IndraStra Global <https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1#:~:text=Proportionality%3A%20There%20should%20be%20a,State%20interference%20(Kaul%20J.> accessed 2 July 2022.

as in *RBI Cryptocurrency Ban Case*[44] and *Internet Ban Case*[45] where the regulations surrounding the impugned matters were dealt with in a way to maintain proportionality without infringing on the rights of individuals.[46]

VIII. BALANCING "PROPORTIONALITY" WITH DATA LOCALISATION: TOWARDS AN AMIABLE IMPLEMENTATION

The entire idea behind nations advocating for data privacy legislation and within them for data localisation standards is based on the placebic belief that the same would cater to their needs of creating a safe haven for data. However, on a deeper analysis of the subject, it is evident that the approach being undertaken is neither enough nor balanced. The proportionality test which seems like a beacon for leading us towards a digital utopia is still underdeveloped. The brief understanding of EU and Indian jurisprudence on the concept of proportionality indicates that both the jurisdictions have their own understanding and mode of implementation of the same. But what is striking is the fact that even though the ideas are not congruent they are still largely intersecting. However, the question that arises is – "How do we ensure that the implementation of data localisation stays within the four walls of proportionality without losing its essence and effectiveness?"

---

[44] *Internet and Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC274.
[45] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
[46] Prithviraj Senthil Nathan, 'MHA Order Dated March 29, 2020: Proportionality and Necessity Arguments' (*Mondaq*, 11 May 2020) <https://www.mondaq.com/india/constitutional-administrative-law/932272/mha-order-dated-march-29-2020-proportionality-and-necessity-arguments#:~:text=A%20measure%20restricting%20a%20right,effective%20alternative%20(necessity%20stage)> accessed 29 April 2022.

The analysis clearly shows that there exist four major grounds of consideration for introducing data localization measures:[47]

- the scope of access,
- the speed of access,
- the risk of foreign retaliation against Indian firms abroad, and
- the risk of data loss due to foreign firms exiting India amid heightened regulations.

At the same time there exist four major considerations as well for promotion of economic growth which have to be taken into consideration seriously:

- demand for goods and services,
- competitive advantages for domestic producers and competitors,
- the risk of data loss due to foreign firms exiting India amid heightened regulations, and
- the risk of foreign retaliation against Indian firms abroad.

The above facts are indicative of and can act as beacons for shaping the policy. However, the key to unfolding this conundrum lies in the existing approaches implemented by the EU and India. While the need for implementing a better data localisation regime cannot be denied, at the same time it needs to be ensured that the measures undertaken are proportional and equitable to the perks they offer.

[47] cf Burman (n 4).

The major takeaway from the doctrinal as well as practical analysis of the existing jurisprudence is that any data localisation measure should be implemented within the circumscribing limits of legitimate, necessary, suitable, and balanced needs. While the strict EU grounds could be a beacon for laying down the foundation for such measures, the Indian court developed proportionality doctrine would act as the pillar for the entire structure. While it may be too early to lay down comprehensive guidelines for amalgamating data localisation and proportionality, it is however the right time to take action for ensuring the continuation of free cross-border transfer of data to fuel the ongoing globalization and development.

III. DATA LOCALIZATION: AN ISSUE BEYOND BORDERS

- Gargi Whorra[*]

ABSTRACT

In modern day, technology driven life, data has acquired a critical position, resulting in an increased assertion for greater control in order to achieve greater digital sovereignty. Therefore, data localization has emerged as a significant policy decision by various nations. However, the data localization approach poses severe limitations and regulatory complexities and at the same time proves ineffective in providing data security, data access and innovation. Therefore, blanket data localization policies might in turn become detrimental depending on the ground realities of each nation. The fact of the matter remains that whether localization of data in general would have any net benefit for the nation is the most pertinent consideration to be assessed.

The primary focus of this paper is to identify a balanced approach for data governance taking into consideration national sovereignty and broader global concerns. This research paper will examine the prevalent forms of data localization while highlighting the various policy considerations underlying the rising data localization surge. Thereafter, it shall evaluate the privacy, security and economic implications and costs to be born in case of such data localization. The paper provides special focus on the prevalent data regulations and data localization policies in India while assessing its potential impact and an insight into the ongoing global interplay with data localization. Lastly, the paper summarises the analysis with policy recommendations premised on the understanding that like-minded nations would work together to arrive at an arrangement that focuses on identifying a workable balance in the coming future.

[*] The author is a Ph.D. scholar at Ram Manohar Lohiya National Law University, Lucknow. Views stated in this paper are personal.

I. INTRODUCTION

Modern-day technology and innovation dictate most aspects of modern life from healthcare to energy, financial transactions to election processes to state a few. These technologies and innovations are heavily data reliant and therefore data has emerged as a global currency. As a result, there is an increased assertion by various countries to harness and exercise greater control over the data of their citizens. This task is particularly important to create greater digital independence, digital sovereignty, and infuse public trust. Thus, data localization has emerged as a significant policy decision by various nations, in response to pressing concerns and to exercise control over data being stored beyond their national jurisdiction.

The attempt to define the term 'data localization' poses a difficulty since its meaning would defer depending on the context in which it is used. However, for general understanding, it may be understood as a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.[1] Data localization generally connotes some form of requirement for the physical storage of data within the borders of a country, limiting the cross-border flow of such data. Therefore, such localization has also been termed as an encumbrance preventing the flow of data beyond national

[1] D Svantesson, 'Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines' (2020) OECD Digital Economy Papers, No. 301 <https://www.oecd-ilibrary.org/science-and-technology/data-localisation-trends-and-challenges_7fbaed62-en> accessed 24 March 2022.

borders.[2] It poses itself more in terms of an obligation thereby effectively restricting data within a particular place.

The nature of such restriction is identified under two broad categories i.e., strict or conditional.[3] In terms of strict data localization, the mandate can range from local storage and data processing requirements to even complete restrictions on any form of cross-border data flow. Whereas, the conditional data localization mandate provides for cross-border transfer of data only upon fulfilment of certain conditions. Therefore, the focus is to create a legal limitation on the movement of data by imposing requirements that restrict it to remain locally.[4]

A. The Prevalent Forms of Data Localization

Since globally, data localization has acquired different shapes and forms, it is difficult to categorize it in a straight-jacketed manner. As of now, the most stringent form of data localization can be identified where the obligation of hard localization is imposed. This requirement focuses on local storage, local processing, and the local transmission of data. Therefore, the data is restricted within the boundaries of such a nation, and cross-border data

---

[2] A. Chander, U. P. Le, 'Data Nationalism' (2015) 64 Emory LJ 679 <https://ssrn.com/abstract=2577947> accessed 3 May 2022.

[3] M F Ferracane, 'Restrictions on Cross-Border Data Flows: A Taxonomy' (2017) European Centre for International Political Economy Working Paper 1/2017 <https://deliverypdf.ssrn.com/delivery.php?ID=142095081069090008107127093075126113014042095000089091121086085094072015121024010092119034022008009024050127005078105008116025006007037073081010101123094116031123104037082049074084105081126019114000027079089067> accessed 3 May 2022.

[4] J Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' (2013) 22 Issues in Technology Innovation <https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf> accessed 3 May 2022.

transfer is either prohibited or strictly regulated.[5] The prime example of such data localization is China which requires personal data from critical information infrastructure (**"CII"**) to be stored within China by a CII operator.[6] Similarly, Russia requires that the personal data of citizens be accumulated, recorded, stored, retrieved, updated, and altered by operators through the database servers located within Russia.[7]

A limited data localization approach that focuses on cross-border data transfer, with conditional requirements to be fulfilled by the transferee entity is also widely prevalent. European Union's General Data Protection Regulation (**"GDPR"**) is the prime example of such localization. Under the GDPR, the European Commission needs to be satisfied that the transferee is located in a territory that meets the adequate level of protection standards. There are certain exceptions to the said rule i.e., where the public interest of the EU or a member state of the EU is involved or to fulfil a contract or where explicit consent is given by the data subject.[8]

B. Determining the Indian Approach

A comparatively less stringent, nevertheless, cumbersome approach is to require companies to maintain a local copy of data within the territory of such nation. India is primarily moving in this direction under the Personal Data

---

[5] Pablo Urbiola and others, 'Data Flows across Borders: Overcoming Data Localization Restrictions' (*Institute of International Finance,* March 2019) <https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf> accessed 27 March 2022.

[6] Cybersecurity Law of People's Republic of China 2017, art 37.

[7] Russian Federal Law No. 242-FZ.

[8] Kurt Wimmer, Gabe Maldoff and Diana Lee, 'Indian Personal Data Protection Bill 2019 vs. GDPR' (*International Association of Privacy Professionals*, March 2020) <https://iapp.org/media/pdf/resource_center/india_pdpb2019_vs_gdpr_iapp_chart.pdf> accessed 27 March 2022.

Protection Bill 2019 which requires Sensitive Personal Data to be stored in India.[9] Cross-border transfer of such data would be permissible only when a copy of such data is stored within India and certain mandatory conditions are fulfilled which are:[10]

- Explicit consent from the data principal
- Transfer of such data should be through a contract/intra-group scheme approved by the Data Protection Authority (**"DPA"**) [Or]
    - The transferee country/entity should be included in the list drawn by the Central Government which deems that such a country provides the necessary adequate protection [Or]
    - Where the DPA, in consultation with the Central Government, authorizes such transfer of sensitive personal information for a specific purpose.

There are even stricter restrictions on cross-border transfer of Critical Personal Data barring limited exceptions such as:

- Health emergency
- Request made by a country/entity that the Central Government has deemed the transfer as permissible.[11]

Irrespective of its form, data localization as a tool of "data nationalization" bears its own cost especially when it acts like a non-tariff

[9] The Personal Data Protection Bill 2019 (373 of 2019), cl 33.
[10] ibid, cl 34.
[11] ibid.

barrier to trade.[12] Therefore, concern associated with increasing data localization is not limited to only economic factors but has far-reaching effects on almost every aspect of modern, technology-driven life.

The rising data protectionism as evident in the case of Russia and China and data restrictiveness as in the case of the EU GDPR are both two ends of the spectrum. China has enforced blanket unconditional localization across all sectors including CII, important personal information of a natural person, financial, energy, transport information, etc. Similarly, Russia provides for unconditional localization by mirroring all personal data of their citizens. Whereas EU supports data transfer, provided personal information is transferred only upon the fulfilment of certain prerequisites. However, the focus of the present discourse lies in between the spectrum, towards countries such as India that are still to determine their policy in terms of data governance and localization. In the long run, the development of policies by such countries will prove vital in determining the future of the global digital economy and the nature of the internet as either open and regulated or as closed and controlled.

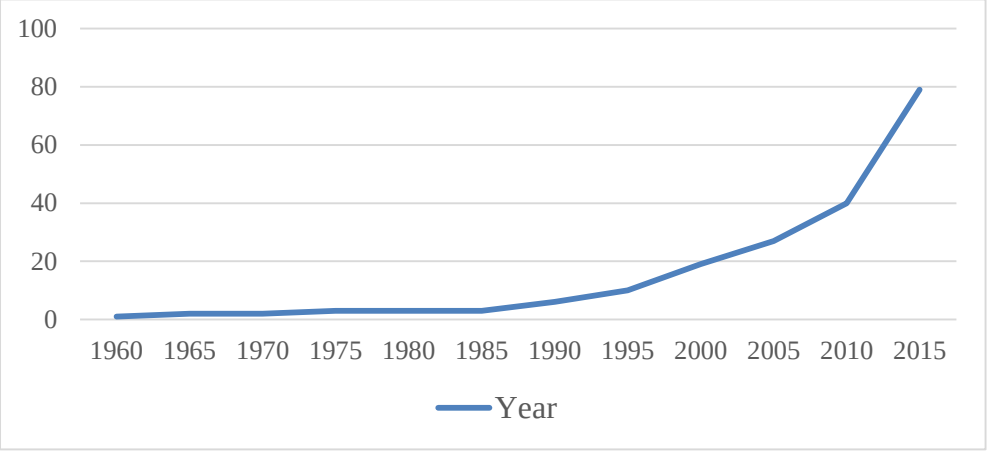
II. POLICY CONSIDERATIONS UNDERLYING DATA LOCALIZATION SURGE

Most governments are devising policies to exercise greater control over data as a response to myriad concerns associated with data being stored beyond their national jurisdiction. Most of the reasons stem from an apprehension that such states would be unable to exercise sovereignty over the

[12] A. Chander, U. P. Le, 'Breaking the Web: Data Localization vs. the Global Internet' (2014) UC Davis Legal Studies Research Paper Series 1 <http://ssrn.com/abstract=2407858> accessed 30 March 2022.

data of their citizens. Furthermore, considering the prevalent data dominance exercised by developed nations in the digital environment, particularly the USA and China, these fears are not without reason. Thus, data localization has emerged as a significant policy consideration by various nations, especially those lacking sufficient geopolitical influence, in response to such pressing concerns.[13]

Illustration I: Increase in data localization measures globally (1960 - 2015)[14]



It can be noted that a significant increase in data localization regulations has been made with the development and growth of information technology.[15] In the past few years, development in big data technologies has been a driving force resulting in increased demand for data, data control, and

[13] Emily Wu, 'Sovereignty and Data Localization' (*Harvard Kennedy School Belfer Center for Science and International Affairs*, July 2021) <https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf> accessed 1 April 2022.

[14] United States International Trade Commission, 'Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions' (*United States International Trade Commission*, August 2017) <https://www.usitc.gov/publications/332/pub4716_0.pdf> accessed 1 April 2022.

[15] ibid.

subsequent data localization.[16]

Reliance on widening data localization policies is primarily on technical concerns associated with the free flow of data. Such factors vary from (a) Data safety, and national security including foreign surveillance; (b) Restricted access to data stored beyond national jurisdiction; (c) Concerns regarding the overuse of personal data including breach of privacy rights; (d) Inability to access data necessary for prevention and investigation of crimes by national law enforcement and security agencies; and (e) Inability to reap economic benefits from data of their nationals on account of its control and exploitation by foreign companies.[17]

At the same time, geopolitical realities and the wide global divide in terms of dominance by developed nations in the technological environment, infrastructure, and control over access is of grave concern. Value concerns associated with such data dominance by a select few have given rise to pertinent fear of a form of "neo-colonialism" in the present times.[18] Furthermore, failure in establishing privacy and data protection norms and past incidents such as the expose by Edward Snowden keeps the distrust

[16] Yanqing Hong, 'Data Localisation: Deconstructing Myths and Suggesting a Workable Model for the Future - The Cases of China and the EU' (2019) 5(17) Brussels Privacy Hub Working Paper <https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOL5-N17.pdf> accessed 2 April 2022.

[17] Anirudh Burman and Upasana Sharma, 'How Would Data Localisation Benefit India?' (2021) Carnegie Endowment for International Peace Working Paper <https://carnegieendowment.org/files/202104-Burman_Sharma_DataLocalization_final.pdf> accessed 2 April 2022.

[18] Carla Hobbs and others, 'Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry' (*European Council on Foreign Relations*, 30 July 2020) <https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/> accessed 2 April 2022.

alive.[19] Therefore, the immediate focus has shifted to controlling presently unregulated data flow by putting in place even more expansive data localization requirements. It is for these technical, value, and practical concerns that data localization as a response has been resorted to by various policymakers to strengthen data control.[20]

III. IMPLICATIONS UNDERLYING DATA LOCALIZATION POLICIES

Time and again, data localization measures are referred to by regulators and policymakers as a possible approach to ensure better privacy, data security, and infrastructural and economic development.[21] However, even if intended towards securing such ends, it is relevant to evaluate the probable impact and implications of data localization on them.

A. Privacy Concerns

The issue of privacy concerns over cross-border data transfer per se does not arise in the case of transferee nations that have established adequate privacy protection safeguards but rather with transferees which fall below such thresholds. This threshold of adequate protection is both subjective and in a

[19] Jonah Force Hill, 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders' (2014) 2(3) The Lawfare Research Paper Series <https://www.researchgate.net/publication/272306764_The_Growth_of_Data_Localization_Post-Snowden_Analysis_and_Recommendations_for_US_Policymakers_and_Business_Leaders > accessed 3 April 2022.

[20] Yue Wang, 'Analysis on the Justification of Cyber Data Localization Legislation' (2016) 36 J of Xi'an Jiaotong U (Social Sciences).

[21] Shamel Azmeh and Christopher Foster, 'The TIPP and The Digital Trade Agenda: Digital Industry Policy and Silicon Valley's Influence on New Trade Agreements' (2016) London School of Economics Working Paper No. 16-175, 26-27 <https://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf> accessed 3 April 2022.

constant state of change. Therefore, the focus is on establishing effective frameworks to secure privacy within the nation as well as globally through technical measures such as design mechanisms in networks and digital systems and encrypting user data.[22] Therefore, data localization has a limited impact on addressing the actual problems associated with data privacy itself.[23]

The prevalent frameworks engaging bilateral mutual data transfer systems are cumbersome and impractical in the long run as noted in the case of the invalidation of the EU-US Privacy Shield.[24] Therefore, the discourse towards greater privacy protection lies in establishing a working multilateral discourse that prioritizes privacy along with responsible data transfer in the future. For instance, the Asia-Pacific Economic Cooperation (**"APEC"**) has worked towards such a solution in the form of the Cross-Border Privacy Rules (**"CBPR"**). The CBPR provides a certification framework that globally provides for the exchange of data between entities that meet the necessary accountability requirements.[25] Such frameworks provide more holistic data privacy mechanisms which are aligned with global requirements without creating excessive cost and offer the possibility of greater adoption. Similarly, the ongoing Data Free Flow with Trust (**"DFFT"**) initiative by Japan proposes a possible solution that offers an interoperable system, which targets

[22] Bret Cohen, Britanie Hall and Charlie Wood, 'Data Localisation Laws and Their Impact on Privacy, Data Security and the Global Economy' (2017) 32(1) Antitrust 107.
[23] Helena U Vrabec and others, 'Data Localisation Measures and Their Impacts on Data Science' in Roland Vogl (ed), *Research Handbook on Big Data Law* (Edward Elgar 2021).
[24] Ryan Browne, 'EU and US agree to new data-sharing pact, offering some respite for Big Tech' (*CNBC,* 25 March 2022) <https://www.cnbc.com/2022/03/25/eu-and-us-agree-new-data-transfer-pact-to-replace-privacy-shield.html#:~:text=Privacy%20Shield%2C%20an%20arrangement%20allowing,was%20invalidated%20in%20July%202020> accessed 4 April 2022.
[25] Asia Pacific Economic Cooperation, 'What is The Cross-Border Privacy Rules System' (*Asia Pacific Economic Cooperation,* October 2021) <https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system> accessed 5 April 2022.

developing trade rules for cross-border data transfer while considering the actual differing circumstances existing.[26]

India has raised concerns about the sweeping provisions of the DFFT and calls out for policy space to develop its own domestic legal framework first.[27] However, the two cardinal principles of the DFFT i.e. careful protection to be guaranteed to sensitive and personal data, and free flow of data such as industrial or medical for economic purposes, help in the establishment of a useful baseline balancing data privacy and data transfer.[28] India should take into consideration such a model which can help it develop a more symmetrical framework of data protection and data transfer, inconsonance with global economic realities.

B. Access to Data by State

Another aspect for which emphasis is cast on data localization is expeditious access of data by law enforcement agencies by doing away with the 'request' framework established under the present Mutual Legal Agreement Treaty (**"MLAT"**) regime. The fact of the matter remains that the

[26] Nigel Cory, Robert D. Atkinson and Daniel Castro, 'Principles and Policies for "Data Free Flow Trust" (*Information Technology and Innovation Foundation*, 27 May 2019) <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust> accessed 5 April 2022.

[27] Asit Ranjan Mishra, 'India Says No to Free Flow of Digital Data at G20 Meeting' (*LiveMint*, 22 Sep 2020) <https://www.livemint.com/news/india/india-says-no-to-free-flow-of-digital-data-at-g20-meeting-11600787726265.html> accessed 4 May 2022.

[28] Karthik Nachiappan, '579: The Battle Over India's Data Policy Framework: What Gives?' (*ISAS NUS*, 4 Sep 2019) <https://www.isas.nus.edu.sg/papers/579-the-battle-over-indias-data-policy-framework-what-gives/> accessed 4 May 2022.

MLAT framework is a time-consuming process[29] that lacks transparency,[30] is afflicted by differing ineffective privacy standards,[31] and tends to dilute the due process element in trials.[32] Therefore, the solution lies in introducing a new framework that addresses the lacunas posed by the MLAT regime.

Thus, emphasis should be on devising multilateral arrangements which overcome the lacunas in the present-day MLAT regime. For instance, the US Clarifying Lawful Overseas Use of Data Act (**"CLOUD Act"**) requires certification from the competent authority based on the privacy and civil liberties standards and safeguards maintained by the transferee nation.[33] It further requires an assessment of the overall terms of the agreement to evaluate if it meets the standards under the CLOUD Act.

C. Safety of Data

Safety and security of data is a factor no longer dependent on the physical location of data but rather on the policy framework and security measures of the entities dealing with it. This becomes even more relevant considering the use of data by large global corporations across multiple jurisdictions. Storing large volumes of data at one physical location or with a

---

[29] Bedavyasa Mohanty and Madhulika Srikumar, *Hitting Refresh: Making India-US Data Sharing Work* (Observer Research Foundation Special Report No 39, 2017).

[30] Amber Sinha and others, 'Cross-Border Data Sharing and India' (*The Centre for Internet and Society,* September 2018) <https://cis-india.org/internet-governance/files/mlat-report> accessed 5 April 2022.

[31] Sarah Cortes, 'MLAT Jiu-Jitsu and Tor: Mutual Legal Assistance Treaties in Surveillance' (2015) 22(1) Rich JL & Tech 1.

[32] Robert J. Currie, 'Human Rights and International Mutual Legal Assistance: Resolving the Tension' (2000) 11(2) CLF15.

[33] Emily Wu, 'Sovereignty and Data Localization' (*Harvard Kennedy School Belfer Center for Science and International Affairs*, July 2021) <https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf> accessed 5 April 2022.

centralized data storage center would enable the possibility of a catastrophic breach.[34] Therefore, this issue of safety and security of data is not based on the location of data per se but on technical safeguards and cyber security measures.[35]

On the other hand, certain sectors are heavily reliant on the free flow of data to ensure better security. One such instance is the payment systems being used globally which require data not only to improve and update the payment networks but also to detect fraud, notify it, and prevent it in the future. Therefore, in such cases where the flow of data is disrupted and restricted within territories, the ability of the system to detect instances of fraudulent activity would be limited and would expose such payment systems to risk.[36]

D. Economic Considerations

Considering the interconnected nature of the global economy, ill-conceived data localization policies can lead to creating substantial data storage and processing costs. These actual costs can severely impact the economy in general and certain digitally reliant sectors in particular. Similarly, sectors such as e-commerce, manufacturing, exports, finance, logistics, and service providers, which require secure, continuous access to cross-border data would be unable to function efficiently. Such data localization not only disrupts economic growth and the flow of business but also acts as a deterrent to further innovation which is based on the borderless nature of the internet

[34] cf Vrabec (n 23).
[35] ibid.
[36] Rajat Kathuria and others, 'Economic Implications of Cross-Border Data Flows' (*Indian Council for Research on International Economic Relations*, November 2019) <https://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf> accessed 6 April 2022.

and reliant on the free flow of data. The Leviathan Security Group estimated the burden of data localization could result in the rise of costs for such entities by 30-60%.[37] Such policies create tendencies of raising barriers and limiting possibilities, especially for small-scale entities and new players in a sector.

IV. DATA LOCALIZATION FRAMEWORK IN INDIA

In the past few years, India has taken significant steps by amending and introducing laws toward a wider data localization policy. Most significant developments in this regard have been made in the case of the corporate, finance, insurance, banking, and electric sector. In 2018, the Reserve Bank of India required certain organizations to store and maintain payment data in India.[38] Similarly, the IRDAI (Maintenance of Insurance Records) Regulation, 2015[39] requires insurers to store and maintain data within India.[40] Furthermore, Section 94 read with Section 88 and 92 of the Companies Act, 2013[41] requires financial information to be maintained at the registered office of the company by such specified companies.

The Personal Data Protection Bill 2019 (**"PDP Bill"**)[42] has laid down further requirements for data localization of sensitive personal data and critical personal data. In December 2021, after two years of deliberation, the Joint Parliamentary Committee (**"JPC"**) laid down its report on the PDP Bill. The

---

[37] Brendan O'Connor, 'Quantifying the cost of forced localization' (*Leviathan Security Group*, 24 June 2015) <https://www.leviathansecurity.com/media/quantifying-the-cost-of-forced-localization> accessed 6 April 2022.
[38] Reserve Bank of India Dir 2017-18/153, para 2(i).
[39] Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulation 2015.
[40] ibid para 3(9).
[41] The Companies Act 2013, ss 88 and 92.
[42] The Personal Data Protection Bill 2019 (373 of 2019).

JPC has emphasized the importance of storing data within India and mirroring copies stored outside India in light of growing national and security concerns. The report has stressed developing policy to eventually localize all forms of data within India. Therefore, it has focused the attention on the need for developing greater data storage infrastructure, while supporting and assisting businesses within India and ensuring ease of doing business with India.[43]

V. IMPACTS OF WIDENING DATA LOCALIZATION

The impact and practical implications of data localization measures in India can be assessed from three perspectives.

A. Economic Impact

Ultimately, it is critical to evaluate the cost-benefit and overall effect of data localization on the economic growth of India. In 2014, European Centre for International Political Economy provided that a mandatory localization policy could negatively impact India's GDP by 0.8%.[44] In terms of the welfare cost, India would be losing 11% of the monthly salary per worker.[45] Another study estimates investment losses in India to amount to US $18bn and the welfare losses to US $2.4bn by 2025.[46]

---

[43] Joint Parliamentary Committee, *Report of the Joint Committee on The Personal Data Protection Bill, 2019* (16 December 2021) 8-10.

[44] M Bauer and others, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (*European Centre for International Political Economy*, May 2014) <https://ecipe.org/publications/dataloc/> accessed 7 April 2022.

[45] ibid.

[46] CUTS International, 'Data Localisation: India's Double Edged Sword?' (*CUTS International*, Jaipur 2020) <https://cuts-ccier.org/pdf/data-localisation-indias-double-edged-sword.pdf> accessed 7 April 2022.

The lack of infrastructure to support sweeping data localization policies would force additional costs towards hardware investments either by improving existing data centers or by investing in cloud service providers. In terms of data center infrastructure, India accounts only for 1.2 percent globally and 5.23 percent in the Asia-Pacific region.[47] The Asia Cloud Computing Association in its Cloud Readiness Index has ranked India at 10 out of the 14 Asian countries it studied and a score of 56.7 out of 100.[48] It will also have a critical impact on investment which is essential for any digital development, particularly digital infrastructure which is presently targeting to attract significant FDI. Presently, on account of the high cloud service cost,[49] lack of data centers, and associated infrastructure, the possibility of India hosting such significant quantities of data would prove uneconomical.[50]

B. Privacy and Civil Liberties

The issue of privacy concerns over citizens' data is dependent on developing an effective data protection framework not only against foreign nations and entities but also the state and domestic entities. India has been lagging behind its global counterparts on this front despite the landmark pronouncement of the Hon'ble Supreme Court in *Puttaswamy v. Union of*

---

[47] Internet and Mobile Association of India, 'Conducive Policy and Regulatory Environment to Incentivize Data Center Infrastructure' (*IAMAI*, May 2016) <https://www.medianama.com/wp-content/uploads/iamai-make-in-india-data-center-report-india.pdf> accessed 8 April 2022.

[48] Asia Cloud Computing Association, 'Cloud Readiness Index' (*Asia Cloud Computing Association*, 2020) <https://www.digitalcentre.technology/wp-content/uploads/2020/06/CRI2020_ACCA_Final.pdf> accessed 8 April 2022.

[49] Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla, 'The Localisation Gambit-Unpacking Policy Measures for Sovereign Control of Data in India' (*The Centre for Internet and Society*, March 2019) <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf> accessed 8 April 2022.

[50] ibid.

India,[51] recognizing privacy as a fundamental right. Therefore, the need of the hour is not sweeping data localization but rather a strong workable privacy framework in harmony with global standards and safeguards.

Furthermore, sweeping measures of mandatory data localization would have to stand the test of being proportionate, reasonable, just, and fair as laid down by the Puttaswamy judgment.[52] It is on these thresholds that mandatory data localization will not hold ground in the face of more proportionate alternatives. At the same time, it can be reasonably apprehended that such measures could be counter-intuitive and premature in guaranteeing any form of privacy, especially against the state. Such data localization can encourage wide-scale surveillance and intrusive measures by local governments which in many ways can cause irreparable damage to civil liberties.[53]

C. Access to Data by the State

Accessing information stored beyond the jurisdiction of the state is a compelling challenge for the state. Therefore, it appears that localization would aid law enforcement agencies to access data and implement local laws more effectively. However, this too has its fair challenges. Modern technologies such as encryption techniques would require state agencies to invoke more comprehensive legal processes to overcome such issues. Under such localization requirements, smaller entities might exit the market but

[51] *Justice K.S. Puttaswamy and Anr. v. Union of India and Others*, (2017) 10 SCC 1.
[52] ibid.
[53] Gautam Bhatia, 'Making the Internet Disappear' (*The Hindu*, 18 October 2017) <https://www.thehindu.com/opinion/lead/making-the-internet-disappear/article19877770.ece> accessed 10 April 2022.

larger corporations such as Whatsapp, Twitter, Google, and Facebook, are more likely to continue and are harder to negotiate with.[54] A viable solution for the present situation, particularly concerning US-based entities, would be to enter into an agreement under the CLOUD Act that would help India mitigate the MLAT issues and still gain access to Indian data held by US firms. In the longer run, limited localization mandates which are targeted for specific purposes might prove more conducive for India.

VI. THE GLOBAL INTERPLAY WITH DATA LOCALIZATION

The current global dialogue on data localization is strongly impacted by the prevalent North-South geopolitical divide. The present data framework is focused on harvesting data from the South to be processed, stored, and utilized by the North. This pattern has led to a surge in interventions by the developing countries calling out the hegemony of the North over digital intelligence and reclaiming control over their data by supporting indigenous platforms.[55] India has been developing its stance along these lines in recent years with payment data local storage mandate, digital taxation on foreign businesses and platforms, stricter regulations, and supervision of significant social media companies.[56]

---

[54] Justice BN Srikrishna, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (*Ministry of Electronics and Information Technology*, 27 July 2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 10 April 2022.

[55] cf CUTS International (n 46).

[56] Mark Linscott and Anand Raghuraman, 'Atlantic Council India's Digital Policies are Putting US Tech in a Bind' (*Atlantic Council*, 10 August 2021) <https://www.atlanticcouncil.org/blogs/new-atlanticist/indias-digital-policies-are-putting-us-tech-in-a-bind/> accessed 11 April 2022.

Therefore, global data localization is taking up two patterns, firstly, hard data localization is enforced by China, Russia, Indonesia, and Nigeria, through which such countries prohibit/restrict the cross-border flow of data outside the national territory.[57] Secondly, countries allow the regulated and conditional flow of data which may or may not include local storage of data. These conditions vary depending on legal, regulatory, certification requirements, etc.[58] Most nations have taken steps anywhere between these two approaches with varying degrees of control over data transfer, nature of the data, applicability, and enforcement measures. In this regard, most data localization steps have been with regards to specific sectors targeting critical and sensitive data such as health records in Australia, cloud service providers working for the department of defense in the United States, and data to ensure accountability in the government system in Canada, etc.[59]

On the other hand, several regions/countries have identified more frameworks focused on developing robust cross-border data transfer while utilizing data localization policies where necessary. The European Union's GDPR has been one of the most significant data protection frameworks. It provides for the free flow of personal data to regions/entities that meet the 'adequate level of protection' requirement.[60] In terms of non-personal data, the EU Regulation (EU) 2018/1807 facilitates the free flow of data by

---

[57] A Segal, 'Year in Review: Chinese Cyber Sovereignty in Action' (*Council on Foreign Relations*, 4 December 2017) <https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action> accessed 11 April 2022.

[58] cf Kathuria (n 36).

[59] cf Basu (n 49).

[60] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Dir 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, art 45.

prohibiting member states from localizing such data which is not under the scope of the GDPR.[61] It limits the conditions for local storage on the ground public security and after communicating such localization to the European Commission.[62] Therefore, the focus is on demanding and maintaining adequate data protection standards to ensure a safe and accountable free flow of data.

Similarly, Singapore under the Personal Data Protection Act, 2012 (**"PDPA"**) provides for cross-border transfer of personal data only if the prescribed standards and requirements under the PDPA are ensured by the organization.[63] The PDPA creates a dual obligation on the organization to comply with the legally enforceable data protection mandates while it is in possession of such personal data and at the same time to ensure that the recipient maintains standards similar to the PDPA in safeguarding such data.[64]

To overcome the differences in domestic privacy legislation, APEC has developed the CBPR. The CBPR works as an enforceable certification system in which companies can join voluntarily to comply with globally recognized standards to ensure data privacy and protection.[65] Furthermore, both the EU under the Binding Corporate Rules System and APEC CBPR mandate such companies to establish processes for independent review to ensure necessary protection in case of data transfer.[66] The EU scrutinizes

[61] Regulation (EU) 2018/1807 of the European Parliament and of Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59.
[62] ibid.
[63] Personal Data Protection Act 2012, s 26(1).
[64] Personal Data Protection Regulations 2021, reg 10.
[65] Asia Pacific Economic Cooperation (n 25).
[66] United Nations Conference on Trade and Development, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (*United Nations*

contracts under which data is primarily transferred to assess whether the wording of the contract ensures sufficient data protection. The EU also provides individuals the opportunity to consent to the transfer of their data to a foreign country/entity as a mandatory condition.[67] However, this form of consent might prove ineffective, illusionary, and impractical under various circumstances. Therefore, best practices evolving to facilitate data transfer focus on combining elements of different approaches to mitigate many of the concerns driving data localization practices.

VII. CONCLUSION AND RECOMMENDATIONS

The most pertinent issue at present surrounding data localization is the lack of a global consensus in terms of the future of data sharing, privacy, and protection. Therefore, in a global arena greater initiative needs to be undertaken to facilitate key policy options. These policy considerations involve:

- Constant dialogue on different aspects of data control and protection, while targeting greater transparency and involvement of developing nations and stakeholders. Such engagement is critical in identifying a workable balance between data protection, innovation, and digital economic growth.
- Move away from piecemeal sector-specific legislation and develop broad, comprehensive data privacy and regulatory frameworks. For instance, cybercrime and data protection should be discussed under broader legal frameworks such as the Budapest Convention on

Conference on Trade and Development, April 2016) <https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf> accessed 12 April 2022.

[67] Regulation (EU) 2016/679 (n 60), art 6.

Cybercrime which requires revision and improvement and a possible protocol, to become truly effective.

- Efforts have to be made to imbibe common principles and best practices to move towards an interoperable system. Such interoperability signifies developing legal frameworks addressing concerns such as data transfer, privacy, cybersecurity, and other issues through a similar framework guaranteeing an adequate level of protection. Digital interoperability should introduce greater regulatory interoperability which can be attained through consensus, agreement, and, recognition of global principles and certification standards for instance under the APEC CBPR framework.
- On the domestic front, the focus has to be directed towards establishing functioning regulatory bodies and robust enforcement mechanisms to address appropriately data breaches and privacy violations.
- To actively deliberate on data transfer and localization issues in light of:
    - Data transfer exceptions such as law enforcement requests, emergencies, in furtherance of contractual obligations, etc. The initiative should be taken by major developed countries to improve existing frameworks such as the MLATs and to facilitate greater assistance under existing domestic laws such as the United States CLOUD Act.
    - Establish a working model of a comprehensive evaluation to identify jurisdictions that provide an adequate level of data protection standards.

  - Procedure to evaluate the corporate policy and rules within corporate entities engaging in different capacities with data and data transfer.
  - Lay down necessary accountability standards for foreign entities in case of any breach.
- To facilitate developing nations in their capacity-building efforts towards establishing data protection frameworks and also their effective implementation.

Since India stands at the cusp of developing its data policy, in addition to the above-stated aspects, it is pertinent for it to engage with the following considerations to identify a workable balance in the coming future:

- Data localization measures do not provide India the access to data stored beyond the national jurisdiction and therefore they do not resolve jurisdictional conflicts or further jurisdictional claims. Thus, India would have to initiate opening up channels of negotiation under key instruments such as the European Union's e-Evidence Directive, US CLOUD Act, etc. This is particularly important in dealing with foreign entities bound by such instruments. India should leverage its present stance to exercise greater pressure on countries that rely on such data and resolve deadlocks in the present data-sharing framework. It will also enable India to stress for more workable bilateral/multilateral agreements that ensure time-bound sharing of data with Indian law enforcement agencies in light of Indian laws.

- To evaluate and identify the most critical and beneficial data categories for local data storage instead of applying sweeping data storage mandates.
- To research and identify structured, systematic, and phased localization mandates through transparent engagement with important stakeholders.
- India should also work towards developing its framework for data sharing and conditional mandates to maintain the privacy and security of data. This will ensure that data of Indian citizens are treated with the necessary precaution and safety standards and also uplift India's position globally.
- In light of possible threats to fiber optic cables and cyberattacks, India needs to align strong defense, and initiate dialogue and alliances with countries holding strategic positions.
- To strategically plan and develop robust internet infrastructure to meet requirements of future data localization policies, as and when necessary.

Strategically, it would be extremely onerous to the digital economy for India to introduce sweeping data localization mandates at this point. Therefore, the global patterns also encourage India to redirect its effort towards the development of a legal framework that facilitates certainty and stability in cross-border data transfer. However, this provides only an important starting point for the Indian government to evaluate data localization as a policy consideration in light of the present circumstances and to assess its viability to achieve broader future objectives.

IV. ONLINE DISPUTE RESOLUTION PLATFORM FOR B2C AND B2B E-COMMERCE IN INDIA: A CRITICAL APPRAISAL

- Abhay Raj & Ajay Raj[*]

ABSTRACT

Online Dispute Resolution (ODR) in India is a relatively modern subfield of dispute resolution that is slowly gaining traction. While legislators and academicians have struggled to develop legal rules and policy frameworks governing cyberspace (particularly ODR), there have been a number of effective initiatives in the subfield, for instance, the UNCITRAL law proposal, and the European Union ODR proposal. Even with the effective initiatives, more study, particularly from an interdisciplinary and jurisdictional viewpoint, is needed that combines legal pluralism and cosmopolitanism, in an attempt to develop the platform while avoiding its drawbacks. Through the present paper, the author advocates for the promotion of the ODR scheme, specifically for B2C and B2B e-commerce in India. The paper heavily relies on the involvement of current dispute resolution scholarships and takes into account the seismic development in major jurisdictions. With that, the author uses a rather novel approach in the present paper and comments based on the online survey conducted amongst peers and experts. Following the data analysis, this paper identifies three main issues in the ODR scheme, in specific regard to e-commerce disputes in India: structural challenges, organisational challenges, and behavioural challenges in the scheme. The implications of the paper will be both methodological and practical.

[*] The authors are fourth and fifth-year students of BA/BBA LL.B. and BBA. LL.B. (Hons.) at Jindal Global Law School and Symbiosis Law School, Pune respectively. Views stated in this paper are personal.

I. INTRODUCTION

"*I have a dream, that one-day international arbitration will rise up and feel out the true meaning of its creed: to live out as a truly transnational system of justice*".[1]

In his 2007 article entitled, 'Online Dispute Resolution: Some Implications for the Emergence of Law in Cyberspace', Professor Ethan Katsh, widely recognised as the founder of Online Dispute Resolution ("**ODR**"), while critiquing David Johnson and David Post's article,[2] articulated and perhaps started a rather controversial but important debate around the States' driving force for interacting with the cyberspace. Katsh

[1] Maxime Chevalier, 'From Smart Contract Litigation to Blockchain Arbitration, a New Decentralized Approach Leading Towards the Blockchain Arbitral Order' (2021) 12 J of Intl Dispute Settlement 558.

[2] David R Johnson and David Post, 'Law and Borders – the rise of law in cyberspace' (1996) 48 Stanford L Rev <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535> accessed 8 April 2022.

noted that one side of the argument affirms that territorial nations may and should prescribe authoritative cyberspace norms, while the alternative argument states that cyberspace, in itself, is a different place/identity having authority for its own set of norms. With that, Katsh pointed out, at a more basic level, what is the real impact of technologies on the State's power to prescribe and enforce legislation. At a further basic level, the focus should be on the issues of what the law is, how it emerged, how it is evolving, and the issues that have a long history and still, remain unanswered in cyberspace.

The previous few decades have seen an evolving process for ODR, and the current ODR regime is the result of such advances. Started as a movement, ODR has evolved to handle millions of disputes through cyberspace.[3] The authors, in an attempt to answer the above-mentioned questions, have divided this movement into four different phases, including, phase one (1970 - the 1980s), phase two (1980 - late 1990s), phase three (early 2000 - 2010), and phase four (2010 - 2022).[4]

A. The First Phase: A Phase of Reluctance, A Phase of Promotion

The first phase could be simply understood as the phase for the growth of the alternative dispute resolution (**"ADR"**) movement. This was a direct

[3] Del Duca, Colin Rule and Zbynek Loebl, 'Facilitating Expansion of Cross-Border E-Commerce- Developing a Global Online Dispute Resolution System (Lessons derived from existing ODR systems- work of the United Nations Commission on International trade law)' (2012) 1 Penn State J of L & Intl Affairs 59.

[4] Ethan Katsh, 'ODR: A Look at History, A Few Thoughts About the present and Some Speculation About the Future' Mediate: Online Dispute Resolution Theory and Practice <https://www.mediate.com/odr-theory-and-practice-table-of-contents-forward-introduction-first-chapter-odr-past-present-future/> accessed 8 April 2022.

result of the Pound Conference[5] and a phase for an attempt to promote ADR.[6] In the Indian-specific context, the phase was not pro-arbitration, with even the Hon'ble Apex Court observing, "[*e*]*xperience shows and law reports bear ample testimony that the proceedings under the* [Indian Arbitration] *act have become highly technical and accompanied by unending prolixity, at every stage providing a legal trap to the unwary*" (emphasis authors').[7]

B. The Second Phase: Development of Internet and ODR

Universally, the second phase could be understood as the phase for the development of the internet, and the evolution of ideas for ODR.[8] The development of ideas for ODR could be seen in the works of McCarty's Harvard Law Review article[9] and Susskind and Capper's work.[10] Again, in the Indian-specific context, this time could be considered as a developing period for dispute resolution. In 1985, the UNCITRAL Model Law was signed and adopted by India;[11] which was subsequently followed by the adoption of the Arbitration and Conciliation Act, 1996.[12] While this period, for India, was a novel one, India did not specifically lean in favour of the ODR.

---

[5] Rex E Lee, 'The Profession Looks at Itself–The Pound Conference of 1976' (1981) Brigham Young Univ L Rev 737.
[6] Roger Fisher, L William Ury and Bruce Patton, *Getting to YES: Negotiating Agreement Without Giving In* (185 Penguin 2011).
[7] *M/s Guru Nanak Foundation v Rattan Singh & Sons*, 1982 SCR (1) 842.
[8] Fahimeh Abedi, John Zeleznikow and Emilia Bellucci, 'Universal standards for the concept of trust in online dispute resolution systems in e-commerce disputes' (2019) 27 Int'l J of L and Information Technology 209.
[9] L. Thorne McCarty, 'Reflections on Taxman: An Experiment in Artificial Intelligence and Legal Reasoning' (1976) 90 Harvard L Rev 837.
[10] Phillip Capper and Richard E Susskind, *Latent Damage Law: The Expert System* (Butterworths1988).
[11] UNCITRAL Model Law.
[12] Arbitration and Conciliation Act, 1996 (Act 26 of 1996).

C. The Third Phase: Evolution of ODR space into E-Commerce

The third phase from the early 2000s to 2010 could be understood as the period for the growth of ODR-specific space, especially its usage in e-commerce. For instance, the usage of ODR by PayPal and eBay is one such example.[13] This was further catalysed by wide research by scholars building trust towards ODR, such as, works by Chang,[14] Pecnard,[15] and Ebner.[16] These scholars addressed important concerns to create confidence with both human and cyberspace platforms. Moreover, it is interesting to note that with the growth of ODR, there was a growth in the use of ODR to protect users' data, as observed by scholars.[17] For India, this period was the growth and trust for the traditional dispute resolution mechanisms, for instance, offline mediation, and offline arbitration.[18]

D. The Fourth Phase: The Important Phase

For ODR, the fourth phase can be attributed as a phase for understanding "*ODR* [as] *the only method to conflict resolution and prevention that can play a role not just in a highly complicated future, but also*

[13] Colin Rule and Chittu Nagarajan, 'Leveraging the Wisdom of the Crowds: The Ebay Community Court and the Future of Online Dispute Resolution' (2010) 2(2) ACResolution 7; E Katsh, J Rifkin and A Gaitenby, 'E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of eBay Law' (2000) 15 Ohio St J on Disp. Resol (2000) 705.
[14] Elizabeth Chang, Farookh Hussain and Tharam Dillon, *Trust and Reputation for Service-Oriented Environments: Technologies for Building Business Intelligence and Consumer Confidence* (John Wiley & Sons 2006).
[15] Camile Pecnard, 'The Issue of Security in ODR' (2004) 7(1) ADR Bulletin 1.
[16] Noam Ebner, '*ODR and Interpersonal Trust*' in Mohamed S Abdel Wahab, Ethan Katsh and Daniel Rainey (eds), ODR: Theory and Practice (Eleven International Publishing 2012).
[17] Suzanne Van Arsdale, 'User Protections in Online Dispute Resolution' (2015) 21 Harvard Negotiation L Rev 107.
[18] Stephen York, 'India as an Arbitration Destination: The Road Ahead' (2009) 21(2) National L School of India Rev 77.

in a fast-changing one".[19] This can be attributed to the failure of offline dispute resolution in many commercial endeavours and the fault (of traditional methods), which is exacerbated by the fact that courts are irrelevant to many, if not all, disputants.[20] ODR, in lieu of traditional methods, has evolved as a transnational system of justice.[21] It has proved that justice, under any circumstance, is not a mere imagination; but rather an attempt in providing prompt resolution of disputes through cyberspace.[22] As such, this phase was an attempt to provide justice and protect users' data in cyberspace.[23] This was further witnessed by the development of usable systems in ODR, for instance, the Civil Resolution Tribunal by the British Columbia and Rechtwijzer by the Dutch.[24] Particularly, these platforms became the artificial intelligent third-party resolvers in disputes.[25]

In specific regard to the theme of the conclave, "*Practical Aspects in Information Technology Litigation and Data Protection in India*", the fourth

---

[19] cf Katsh (n 4).

[20] Dave Orr and Colin Rule, 'Artificial Intelligence and the Future of Online Dispute Resolution' (New Handshake) <http://www.newhandshake.org/SCU/ai.pdf> accessed 6 April 2022.

[21] Emmanuel Gaillard, *The Present–Commercial Arbitration as a Transnational System of Justice: International Arbitration as a Transnational System of Justice* in Albert Jan van den Berg (ed), Arbitration: The Next Fifty Years (ICCA Congress Series No 16 of 2012).

[22] Aranya Chatterjee and Sharique Uddin, 'Online Dispute Resolution: An Effective Mechanism and an Alternative Tool for Justice at a Reasonable Time' (2021) 87(4) The Intl J of Arbitration, Mediation and Dispute Management 529; Raymond H Brescia, Alexandria Decatur and Julia Kosineski, 'Civil Society and Civil Justice: Teaching with Technology to Help Close the Justice Gap for Non-Profit Organizations' (2019) 29 Albany LJ of Science and Technology 29.

[23] Robin V. Cupido, 'The Growth of E-Commerce and Online Dispute Resolution in Developing Nations: An Analysis' (2016) 10(10) Intl J of Economics and Management Engineering 3371.

[24] cf Arsdale (n 17).

[25] Scott Shackelford and Anjanette Raymond, 'Building the Virtual Courthouse: Ethical Considerations for Design, Implementation, and Regulation in the World of ODR' (2014) Wisconsin L Rev 615.

phase universally observed that with the ever-increasing rise in online transactions,[26] the issue of data protection played a major challenge. It is believed, and as has been highlighted below in the last part of the article containing empirical research, there have been confidence/trust issues in regards to the protection of consumer data and security in the ODR mechanism. The data protection issue that the disputants may desire protection from is twofold: (a) unanticipated, and unauthorized 'data usage' by e-commerce platforms;[27] (b) any 'data access' in the form of technical security.[28] This shall be explained in greater detail in the last part of the article.

While the scholars were writing jurisdictional specific work,[29] it is enthralling to observe how not much has been written on ODR and e-commerce in Indian-specific disputes, let alone work on data protection through ODR. Nonetheless, there were instances of Indian e-commerce platforms using ODR; for instance, Snapdeal, an Indian e-commerce company, in 2020 used ODR as a mechanism to resolve its disputes.[30] That said, more study, particularly from an interdisciplinary and jurisdictional

[26] Daniela Coppola, 'E-commerce worldwide' (*Statista*, 23 February 2022) <https://www.statista.com/topics/871/online-shopping/> accessed 17 April 2022.
[27] cf Arsdale (n 17).
[28] Karim Benyekhlef and Fabien Gelinas, 'Online Dispute Resolution' (2005) 10(2) Lex Electronica <https://ssrn.com/abstract=1336379> accessed 5 April 2022.
[29] Julia Hornle, 'Encouraging Online Dispute Resolution in the EU and Beyond-Keeping Costs Low or Standards High?' (2012) 122 Legal Studies Research Paper 1; Trish O'Sullivan, 'Developing an Online Dispute Resolution scheme for New Zealand consumers who shop online—are automated negotiation tools the key to improving access to justice?' (2015) 24 Int J of L and Information Technology 22; Pablo Cortes, 'Developing Online Dispute Resolution for Consumers in the EU: A Proposal for the Regulation of Accredited Providers' (2010) 19(1) Int J of L and Information Technology.
[30] Neha Alawadhi, 'Snapdeal partners with Sama for online dispute resolution, sees success' (*Business Standard India*, 17 June 2021) <https://www.business-standard.com/article/companies/e-commerce-marketplace-snapdeal-sees-success-in-online-dispute-resolution-121061701499_1.html> accessed 17 April 2022.

viewpoint, is clearly needed to expand India's interest in cyberspace to resolve disputes, particularly, through ODR.

With that prelude, the authors proceed ahead with the article in the following manner. In **Part 1**, the authors rely on the involvement of current dispute resolution scholarships and take into account the seismic development in major jurisdictions. We use the theoretical understanding from ODR scholarships to review and provide suggestions in regard to the protection of personal data in e-commerce and the ODR space. Then, in **Part 2**, the authors use a rather novel and sequential explanatory approach by relying on the survey conducted amongst peers and experts. The survey findings include a survey of 68 individuals about their experience related to the protection of data in the e-commerce space of Indian specific jurisdiction and the limitations associated with it. This is followed by the conclusion and final remarks in **Part 3** of the article.

II. REVISITING E-COMMERCE, DATA PROTECTION AND ODR IN INDIA

As previously noted, the fourth phase brought with it, both, an inundation of e-commerce transactions and a sense of responsibility to use information and communication technology (**"ICT"**) properly. E-commerce has made it possible to execute transactions that were previously unusual and complex, not only for high-value purchases but also for low-value purchases.[31] Currently, business-to-business (**"B2B"**), business-to-consumer (**"B2C"**), and consumer-to-consumer (**"C2C"**) transactions are increasingly taking place

[31] Julio César Betancourt and Elina Zlatanska, 'Online Dispute Resolution (ODR): What Is It, and Is It the Way Forward?' 2013 79(3) Int J of Arbitration, Mediation and Dispute Management.

through cyberspace.[32] Due to the research restraints, the articles focus on the study of only B2B and B2C e-commerce disputes, which are respectively defined as the "*business activities serving other businesses as the end consumers*", and "*business activities serving end consumers directly with services and/or products*".[33]

Many scholars have raised issues and concerns regarding e-commerce transactions,[34] which are catalyzed by data of issues experienced by consumers when purchasing online, such as the delivery of damaged goods, non-delivery of items, or failure of goods to match their actual description.[35] Since many of these disputes/issues are not raised through a proper forum, it is quite challenging to determine the degree of incidence of difficulties that the consumer faces.[36] Nonetheless, the Indian Consumer Affairs Ministry's press release reported that a total of 1,88,262 claims and disputes related to e-commerce space were lodged.[37]

---

[32] Tony Jewels and Gregory Timbrell, *Towards a Definition of B2C & B2B E-Commerce* in Proceedings of the Twelfth Australasian Conference on Information Systems (Southern Cross University (2001).

[33] K Alboukrek, 'Note: Adapting to a new world of e-commerce: The need for uniform consumer protection in the international electronic marketplace' (2003) 35 George Washington Intl L Rev 425; Huong Ha and Sue LT McGregor, 'Role of Consumer Associations in the Governance of E-commerce Consumer Protection' (2013) 12(1) J of Internet Commerce.

[34] Temitayo Bello, 'Online Dispute Resolution Algorithm: The Artificial Intelligence Model as a Pinnacle', in Stavros Brekoulakis (ed), (2018) 84(2) Arbitration: The Int J of Arbitration, Mediation and Dispute Management 159.

[35] Neelam Chawla, Basanta Kumar, 'E-Commerce and Consumer Protection in India: The Emerging Trend' (2021) J of Business Ethics.

[36] NITI Aayog, 'Catalyzing Online Dispute Resolution in India' (12 June 2020) <https://niti.gov.in/catalyzing-online-dispute-resolution-india> accessed 13 April 2022.

[37] Zia Haq, 'As shopping goes online, e-commerce disputes rise to unprecedented levels' (*Hindustan Times India*, 22 March 2021) <https://www.hindustantimes.com/business/ecommerce-disputes-on-the-rise-shows-data-101616366508503.html> accessed 17 April 2022.

In India, the practice and concept of ODR, while being at its nascent stage, is predicted to become popular, in near future, thought-out the 'tech-savvy' disputants.[38] Traditional dispute resolution mechanisms, such as 'offline arbitration', are seemed to be frequently ineffective since they are expensive,[39] time-consuming,[40] and raise severe issues regarding enforceability and jurisdiction.[41] As a result, the "*conflicts that emerge online, should be resolved online*",[42] is the beginning point of the evolution of the ODR platform in Indian jurisdiction. This is one response to the stressed-out litigation system in India.[43]

Alternatively, however, the process of addressing difficulties that arise in the absence of rules may serve as a beginning point. This beginning point leads to the formation of new rules or, in certain cases, new ways of thinking about how to shape conduct, settle disputes, and safeguard rights. Are these both beginning points important for the evolution of ODR in the e-commerce space in India? Is ODR, going to be a framework that, with time, becomes the

[38] Aditya Ranjan, 'Creating a Safer E-Commerce Market for Online Customers in India' (*Vidhi Legal*, 30 Oct 2020) <https://vidhilegalpolicy.in/blog/creating-a-safer-e-commerce-market-for-online-customers-in-india/> accessed 8 April 2022.
[39] Raphael Ng'etich, 'The Current Trend of Costs in Arbitration: Implications on Access to Justice and the Attractiveness of Arbitration' (2017) 5(2) Alternative Dispute Resolution 111.
[40] Aditya Sondhi, 'Arbitration in India- Some Myths Dispelled' (2007) 19(2) Student Bar Rev 48.
[41] Sal Ramani Garimella, 'Issues of Jurisdiction, Choice of Law and Enforcement in International Commercial Arbitration: An Indian Perspective' (2007) Private International Law: South Asian States' Practice 323.
[42] Mansi Bhatt, 'Get ready for online dispute settlement' *Economics Times* (India, 31 July 2006); Smarika Singh, Abhijeet Swaroop, 'Online Dispute Resolution and Consumer Disputes' (2007) 9(1) Asian Dispute Review 38.
[43] Pendency and Vacancies in the Judiciary <https://prsindia.org/policy/vital-stats/pendency-and-vacancies-in-the-judiciary> accessed 8 April 2022.

engine of bringing a change to the legal regime in India? In the authors' view, the answer remains "yes", and will be expanded upon below.

III. LEGAL FRAMEWORK AND INITIATIVE GOVERNING CONSUMER PROTECTION AND DISPUTE SETTLEMENT PROCESS IN INDIA

A. Indian Legal Framework

The disputes arising through the e-commerce space in India are currently governed by the Consumer Protection Act, 2019[44] and Consumer Protection (E-Commerce) Rules, 2020.[45] Earlier they were governed by the Consumer Protection Act, 1986,[46] which had severe limitations concerning the adjudication and applicability processes.[47] The Consumer Protection Act, 2019, makes significant modifications to the extent of governance, penalties, and applicability. It establishes the Central Consumer Protection Authority ("**CCPA**") and provides them with regulatory and controlling powers in e-commerce disputes.[48]

The 2019 Act is indeed pro-arbitration/mediation since it focuses on the establishment of Consumer Mediation Cells in all Indian districts and encourages the consumers to undergo dispute resolution through mediation.[49] Furthermore, the Consumer Protection Act (E-commerce) Rules 2020, provide a step further in the promotion of the ODR by laying down the

[44] The Consumer Protection Act, 1986 (Act 68 of 1986).
[45] The Consumer Protection (E-Commerce) Rules, 2020.
[46] The Consumer Protection Act, 1986 (Act 68 of 1986).
[47] cf Chawla (n 35).
[48] The Consumer Protection Act 1986 s 10.
[49] The Consumer Protection Act 2019 s 74; The Consumer Protection Act 2019 s 37.

foundation of requiring the entities involved in the e-commerce space to advance ODR by using it for internal dispute redressal mechanisms.[50]

Illustration 1: Understanding the Consumer Protection Act, 1986 and Consumer Protection Act, 2019

Particulars	**The Consumer Protection Act, 1986**	**The Consumer Protection Act, 2019**
The mechanism for Alternative Dispute Resolution	No specific provision	Section 37:[51] Resolution of Disputes through ADR Section 74(1):[52] For the purpose of mediation, the State Government shall establish a consumer mediation cell for each District Commission and State Commission

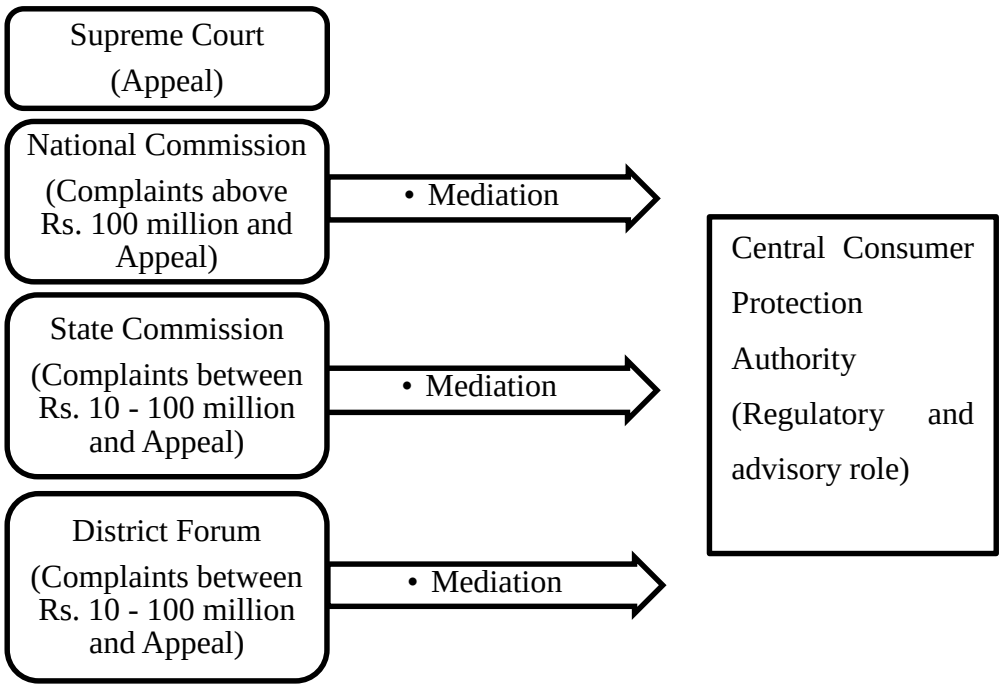
[50] Consumer Protection (E-Commerce) Rules, 2020 <https://consumeraffairs.nic.in/sites/default/files/E%20commerce%20rules.pdf> accessed 10 April 2022.
[51] The Consumer Protection Act 2019 s 37.
[52] The Consumer Protection Act 2019 s 74 (1).

E-commerce	No specific provision	Section 2(16):[53] The Act, 2019 applies to buying or selling goods or services over the digital or electronic network, including digital products, and to a person who provides technologies enabling a product seller to engage in advertising/selling goods/services to a consumer.

The 2019 Act divides the jurisdiction (for instance, between District Forum, State Commission, National Commission, and Supreme Court) based on the amount of the consideration paid, and not on the compensation sought or good and services value. Further, it extends support towards mediation, which the below-mentioned figure explains in much greater detail.

[53] The Consumer Protection Act 2019 s 2(16).

Illustration 2: Grievance Redress Mechanism in India [54]



While it is interesting to note that such reforms in the field of Indian e-commerce are an attempt to provide justice to the parties, it has not been able to cater to the needs of consumers effectively, because of the inherent limitations (discussed below). Indian legislation, per se, does not advance the usage of ODR heavily.

B. Indian Government Initiatives and the Judiciary's Understanding

The Indian government has promulgated, in 2020, the rules on e-commerce protection (Consumer Protection (E-Commerce) Rules, 2020) which provide for the following two requirements to be met by the

[54] cf Chawla (n 35).

government: (i) every e-commerce entity incorporating a proper mechanism for grievance redressal; and (ii) every e-commerce entity, voluntarily, participating in the government's Helpline of Consumer initiative. This indeed brings the usage of ICT in e-commerce to provide leverage to consumer protection. However, it does not specifically mention the usage of ODR, which could have been considered as a recourse for grievance redressal by the e-commerce entities.

With that, the Indian Supreme Court has also recognised the legality of using technology in the arbitration process in the case of *Trimex International*,[55] and *Shakti Bhog*.[56] Herein the Court affirmed the legitimacy of online arbitration agreements, and this includes agreements made through telegraph, emails, or ICT.

Further, to improve its ADR mechanism, the government has opted to be regulated by international standards and obligations in addition to its internal efforts. For instance, recently India brought into effect the United Nations Convention on International Settlement Agreements from Mediation (**"Singapore Convention"**).[57] The convention provides for expedited and direct enforcement of the mediated settlement agreements.

[55] *Trimex International v Vedanta Aluminum Ltd*, 2010 (1) SCALE 574.
[56] *Shakti Bhog v Kola Shipping*, (2009) 2 SCC 134.
[57] United Nations Convention on International Settlement Agreements Resulting from Mediation (adopted on 20 December 2018 UNGA Res 73/198) (the Singapore Convention on Mediation).

IV. LEGAL FRAMEWORK AND INITIATIVES GOVERNING CONSUMER PROTECTION AND DISPUTE SETTLEMENT PROCESS AROUND THE WORLD

A. European Union: ODR Proposal and Data Protection Framework

With the advancement of technology, the European Union ("**EU**") has become more interested in promoting ODR to stimulate and accelerate the expansion of e-commerce throughout the European market.[58] EU has made significant progress in the creation of an ODR platform that allows the European cyberspace market to start dispute resolution proceedings and track claims online.[59] This is further catalysed by the legislation promoting this idea. In accordance with Article 17 of the Directive 2000/31/EC, Member States must encourage entities responsible for the out-of-court resolution of, in particular, consumer disputes to function in a way that offers appropriate procedural protections for the parties involved.[60]

Further, the EU's effort on creating the Regulation on ODR for Consumer Dispute (**"the ODR Regulation"**)[61] and Consumer Alternative Dispute Resolution Directive (**"the ADR Directive"**),[62] became effective. The ODR Regulation and the ADR Directive directly aid in the promotion of ODR by providing consumers with access to national ADR platforms.[63] To be

[58] Green Paper of the European Commission of 19 April 2002 of Access to Consumer Justice and Alternative Dispute Resolution in Civil and Commercial Law (COM (2002) 196 final).
[59] cf Cortes (n 29).
[60] European Commission, Directive 2000/31/EC art 17.
[61] Regulation EU No 524/2013 of 21 May 2013 on Online Dispute Resolution for Consumer Disputes [2013] OJ L 165/1.
[62] Directive 2013/11/EU of 21 May 2013 on Alternative Dispute Resolution for Consumer Disputes [2013] OJ L 165/63.
[63] cf O'Sullivan (n 29); S Wrbka, *European Consumer Access to Justice Revisited* (OUP 2015); N Reich, *European Consumer Law* (2nd edn, Intersentia 2014).

specific, for instance, each EU member state is required under the ADR Directive to implement a system that makes ADR procedures available to consumers in their own country for resolving contractual disputes in the e-commerce space.[64]

Specific attention has been paid to data protection, which under Article 8 of the EU Charter,[65] is recognised as a fundamental right. In accordance with Directive 95/46/EC's Article 24,[66] appropriate measures must be put in place to ensure proper data protection, including the imposition of consequences in the event of a breach of such protection. Before going to the courts in the event of a possible disagreement, data subjects must first contact the data controller, which may in turn rely on other dispute resolution mechanisms, including ODR. This is in accordance with the EU General Data Protection Regulation's Article 38(1)(h).[67]

B. The Mexico case: ODR and the E-Government

Profeco/Concilianet, a consumer e-government service that offers online mediation, was founded in 2008 by the Mexican Protection for Consumer Agency.[68] In Mexico, the Concilianet is regarded as one of the greatest e-government systems accessible to the parties in dispute over e-

[64] ADR Directive art 2.
[65] The EU Charter art 8.
[66] European Commission, Directive 95/46 art 24.
[67] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, art 38(1)(h).
[68] Gabriela R Szlak, *Online Dispute Resolution in Latin America: Challenges and Opportunities* in Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution (Mohamed S Abdel Wahab et al eds 2012).

commerce.[69] Concilianet does not only specialize in the disputes that arise in an online setting but also provides services to resolve disputes resulting from both offline and online transactions.[70]

Concilianet in the Latin American region is the first totally-online ODR mechanism provided by the government,[71] with the entire process taking place online from start to finish, including, the submission of a case, uploading of evidence, hearing, and the determination of the decision.[72] A total of 171 cases have been handled online in the year 2008 by Concilianet, with an agreement rate of 97%.[73] With that, it mediated a total of 1134 cases, with an agreement rate of 96% from around 2008-to 2010.[74]

C. UNCITRAL ODR

The UNCITRAL's Working Group III has proposed its recommendations to the ODR regime universally. Majorly it recommends an ODR platform for filing claims and has also taken on the more ambitious mission of defining clear procedural guidelines with strict time constraints for resolving B2C and B2B low-value disputes involving e-commerce

---

[69] ibid Szlak (n 68).
[70] Mexcian Federal Law for Consumer Protection; Welcome to the New Mexico Courts Online Dispute Resolution Center' (*New Mexico Courts*) <https://newmexicocourtsdmd.modria.com/#home> accessed 11 April 2022.
[71] Consumer Protection Agency in Mexico, <www.profeco.gob.mx/>.
[72] Robert M Kossick Jr, 'Mexico's Emerging E-Government Program: The Role of the Internet in Promoting Economic Development' (2002) 8(1) *Democratic Governance, and the Rule of Law*, Law and Business Review of the Americas 141 <https://scholar.smu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1856&context=lbra accessed> 20 April 2022.
[73] Baoqing Han, *ODR in E-Government and Obstacles to Developing Countries* (Conference: The International Conference on E-Business and E-Government, ICEE 2010, 7 May 2010) Guangzhou, China.
[74] cf Szlak (n 68).

transactions. The UNCITRAL rules have suggested certain procedural stages in the resolution of disputes. The procedure of resolution of e-commerce disputes through ODR has been discussed below, in specific relation to the proposal for the Indian ODR framework (Part C.1).

D. Australia: Creation of ODR

Australian academicians and practitioners have advocated for the creation of an ODR system for e-commerce consumers.[75] Martin Dorris, himself suggested the creation of an ODR programme similar to what has been developed by the European Union in Australia.[76] In consonance with Sourdin and Liyanage, "a proper strategic framework" might help in flourishing the ODR in Australia.[77] In Australia, the consumers are protected by the Australian Consumer Law[78] and this is accompanied by its focus on fair trading and prohibition on deceptive conduct.[79] Furthermore, the government, in itself, has taken steps toward the promotion of the ODR scheme.[80]

V. MAKING INDIA A GLOBAL HUB THROUGH COMPARISON OF THE LEGAL PROPOSALS

Given the expanding amount of data indicating the benefits of a holistic and methodical approach to ODR,[81] utilising a jurisdictional approach

[75] L Griggs, 'e-Commerce' in J Malbon and L Nottage (eds), Consumer Law and Policy in Australia and NZ (Federation Press 2013) 405.
[76] M Doris, 'Developing Consumer ODR in the European Union—A Model to Imitate?' (2012) Aus Prod Liability Rep 280, 283.
[77] cf Griggs (n 75).
[78] T Sourdin and C Liyanage, 'The Promise and Reality of Online Dispute Resolution in Australia' in Wahab 497.
[79] The Australian Consumer Law in Sch 2 of the Competition and Consumer Act 2010 (AU) ss 54–59.
[80] cf Doris (n 76).
[81] cf Cortes (n 29).

for the Indian framework would seem to be a reasonable course of action for the e-commerce companies that litigate frequently. Nevertheless, India has not been able to accommodate itself with the ODR framework, and there are little to no studies of Indian specific origin, as has been stated above. As such, implementing some version of ODR in India, for many corporations looks like proverbial lemmings, and, in turn, unwilling to modify their litigation strategy.

Now one may wonder, how India will be able to be at the forefront in resolving disputes through ODR. As mentioned in Part 2.B, India needs to take a systemic strategy from jurisdiction analysis to systematically promote ODR and protect users' data. These choices are not only stand-alone, rather they can be mixed and matched to create unique hybrids.

A. Hybrid Framework in India

Aspiration may be taken from the EU proposal on ODR, specifically the ODR Regulation and ADR Directive, since its policies are quite extensive, and consumers are provided with certain rights when they interact with the e-commerce space.[82] The consumers are directly provided with access to national entities on ODR for dispute resolution.[83] The entities are required to meet certain criteria, including but not limited to, effective, independent, transparent, and fair procedure.[84] This when combined with the Mexican Concilianet, offering online dispute resolution through e-government, can serve as a catalyzer for the Indian legal framework to excel in the ODR

[82] cf Cortes (n 29).
[83] cf O'Sullivan (n 29).
[84] Eugene Clark, George Cho and Arthur Hoyle, 'Online Dispute Resolution: Present Realities, Pressing Problems and Future Prospects' (2010) 17(1) Int Rev of L, Computers & Technology.

scheme. As such, India could expand upon creating an e-government that serves in resolving high-to-low value e-commerce B2B and B2C disputes. Online traders in India, must inform the consumers about the resolution of disputes through ODR.

Other initiatives include taking a cue from the UNCITRAL ODR, which particularly focuses on e-commerce dispute resolution through ODR. This has been properly summarised in O'Sullivan's article,[85] which states, that the following can be considered an ideal procedure –

- Lodging Complaint (Article 4) – via the ODR platform website, where the communications processing mechanism is overseen by an ODR administrator.
- Negotiation (Article 5) – negotiations between the parties through the website, in order to amicably resolve disputes.
- Neutral Appointment and Settlement (Article 9) – the ODR administrator, shall select a 'neutral', that is the independent third party. Neutral also attempts to help parties reach a conclusion (Article 5/6).
- Final Conclusion – in cases where the dispute is not resolved within 10 days from point 2, then the dispute may be submitted to arbitration.
- Settlement Stage (Article 8) – if the parties reached a settlement, the ODR platform records the agreement terms, and the case is deemed to be closed.

This Part sets experience, wherein, India can adopt an e-government platform and can promote ODR, as has been promoted by the UNCITRAL

[85] cf O'Sullivan (n 29).

ODR, and this in turn also facilitates in taking the EU's ODR proposal of having a national entity on ADR.

B. ODR regime promoting Data Protection, Confidentiality, and Trust in India

E-commerce dispute resolution through ODR appears to be challenging in the Indian context, primarily because, there have been a large number of breaches of data security and confidentially,[86] which is also proved in Part 3 (empirical research). In turn, ODR comes with the inherent distrust challenge through the online environment.

It is indeed true that the consumers are most inclined to trust governments in providing them with information regarding the resolution of e-commerce disputes through ODR.[87] Primarily this is because of their legal standing and obligation to maintain society working under socially accepted standards, including trust and data protection. Indian regime has seen steps in favour of data protection and security, for instance, the recent Data Protection Bill 2021 provides for the protection of data, and data fiduciaries and prevents any misuse, unauthorised usage, and access.[88]

A well-designed ODR platform gives consumers a sense of justice and confidence in cyberspace, which in turn promotes trust in the protection of data. This well-designed ODR platform can be built upon the concept of the e-government platform of Latin America and the EU proposal and Directive

---

[86] NITI Aayog, 'Catalyzing Online Dispute Resolution in India' (12 June 2020) <https://niti.gov.in/catalyzing-online-dispute-resolution-india> accessed 12 April 2022.
[87] cf Bellucci (n 8).
[88] Ministry of Parliamentary Affairs, Joint Committee on the Personal Data Protection Bill, 2019 seeks views and suggestions (Press Information Bureau, 3 February 2020).

95/46/EC which in turn promotes data protection and resolution of disputes through ODR. ODR mechanisms have, time and again, been regarded as an effective means for enforcing data protection rights and compensating the victims of improper use of personal data in the e-commerce space.[89]

C. Enforcement and Governing Law

Another proposal for the Indian ODR regime is the framework for the enforcement of ODR awards. Since, the concerns, per se, the concern for enforcement of ODR terms, both for the customers and the awards, can only be dealt with by proper legislation, India might ensure the interoperability between ODR providers and the Courts. To do so, proper procedural standards must be brought in place by the government. Several critics have urged for the ODR to be accredited and regulated at a national level.[90]

Focusing both on legal empiricism and the existing scholarships in Indian and international jurisdictions, the authors now embark upon the inherent challenges and assess its impact on the ODR movement in India. The research further tries to capture these challenges using a range of scientific methodologies, including, interviews, and surveys. This has been discussed in the subsequent section of the article.

[89] cf O'Sullivan (n 29).
[90] Charlotte Austin, 'Online dispute resolution – An introduction to online dispute resolution (ODR), and its benefits and drawbacks' (Government Centre for Dispute Resolution, Ministry of Business, Innovation and employment, New Zealand Government, 2017).

VI. REVISITING ASSOCIATED CHALLENGES TO THE INDIAN ODR MOVEMENT

This Part seeks to identify the challenges associated with the ODR and its usage in the e-commerce space in India. For this, the starting point is the fact that there have been semantic limitations and confusion concerning the development of the ODR movement in India.[91] A recent report by Niti Aayog, a public policy think tank of the Government of India, "*Designing the Future of Dispute Resolution: The ODR Policy Plan for India*",[92] identified three main limitations of the growth of the ODR movement in India. Typically, the limitations were divided into the following three emergent themes/challenges: *first*, structural; *second*, behavioural; *third*, operational.

As such, in lieu of determining the extent empirically and forming a preliminary understanding amongst the Indian practitioners and legal experts, the authors designed an extensive survey that ran from April 3 to April 10, 2022, and collected data from around 68 respondents.

However, to narrow the research survey, and focus on the main theme of the conclave "*Practical Aspects in Information Technology Litigation and Data Protection in India*", the author has identified a major limitation, which is the concern for the protection of data.[93] The author expands upon the three mentioned emergent themes for data protection concerns in the survey.

---

[91] cf Aayog (n 86).
[92] Niti Aayog (Government of India), *Designing the Future of Dispute Resolution: The ODR Policy Plan for India* (60-65).
[93] cf Alboukrek (n 33); cf Arsdale (n 17); cf McGregor (n 38); cf Chawla (n 35).

Thus, the research question for the survey conducted was, "*What are the inherent limitations in the way for the Indian ODR regime to be at the forefront of resolving e-commerce disputes?"*

Further, the narrower question that the author has focused on is, "*Does the concern of data protection play a major role in being a limitation? Are the other emergent and sub-emergent themes (including, structural challenges, behavioural challenges, and operational challenges*) *interrelated to the major theme of data protection?"*

A. Quantitative Data Analysis

Before proceeding ahead with the survey's conclusion, it is imperative to discuss how the survey was conducted. The research analysis uses Qualtrics,[94] as has been used earlier in similar studies (by Fahimeh Abedi, John Zeleznikow, and Emilia Bellucci[95]), because of the design and efficiency of the online survey software system. With the huge amount of quantities collected through this survey, the data analysis tries to gradually reduce it into small information, which was in compliance with Clark Moustakas's method of a phenomenological research study[96] – with properly identified themes and as such, a model is tried to be finalized through the survey.

Throughout the survey, the authors have maintained a balance between academicians and practitioners, to ensure maximum scope and heterogeneity insight into the survey's questions. The respondents' demographic includes 48 practitioners and 20 academicians (that is 70.58 percent and 29.41 percent

[94] Jonathan Hill, Cross-border Consumer Contracts (*OUP 2008*).
[95] cf Abedi (n 8).
[96] Clark Moustakas, Phenomenological Research Methods (*Sage Publications 1994*).

respectively). Around 58.33 percent of respondents had the experience of 5 to 10 years as practitioners. Most of the respondents (67 respondents) indicated to be associated with the field of 'Law', more precisely, 'Arbitration'; with 64 respondents belonging to India, and 3 belonging to the United Kingdom.

The survey was organised to define, apply, and measure security and data protection concerns in the ODR systems from arbitration experts. The rest of this Part of the article details upon the research conducted and the themes, and answers identified.

B. Overview of the Findings

The four research questions addressed in this paper are only concerned with the factors contributing to the problem presented in Part 3 (research questions and narrower questions):

- Is the ODR system compatible to privacy?
- How likely it is for the ODR regime to flourish in India if it works on all the associated challenges?
- Is there a need for a legislative framework governing data protection and ODR in India?
- Is there a need for robust management of data and ODR in India?

1. Theme 1: Structural Challenges:

Though the survey conducted, structural challenges were indeed agreed upon as a major challenge concerning trust and compatibility with the ODR system. We noted that users and practitioners have been facing a majority of issues due to structural challenges, which include, sub-issues like lack of proper knowledge, lack of proper infrastructure, lack of literacy, and a

divide in the access to information and technology. One of the participants suggested, "that there needs to be a proper knowledge about the ODR scheme in dispute resolution, primarily, because of it being a relatively new field". With this, as was expanded upon by one of the respondents: "ODR in India faces the inherent limitations of the Indian society, and there appears to be a gap because of no-proper digital infrastructure coupled with the lack of digital literacy". Another respondent observed, "'ODR' and 'trust for ODR' goes hand in hand, even if one of these is disrupted, the ODR regime would not flourish in Indian regime".

In specific regards to data protection, one of the respondents observed, "data protection is a major concern in the field of ODR, because of both, (a) concerns – primarily, confidentially, security and privacy, in the Indian regime of e-commerce space; (b) trust issues for ODR in Indian specific space, because of consumer's experience in e-commerce space". As such, it must be noted, this appears because of the general issue of structural challenges.

2. Theme 2: Behavioural Challenges:

The survey also noted behavioural challenges, for instance,[97] the lack of awareness, the lack of proper governing legal culture, and lack of interaction, to also be a concern in the promotion of ODR. The behavioral challenge in the promotion of proper data protection in ODR is intertwined with the sub-emergent themes. For instance, it was noted by one of the respondents, "data protection is not a singular issue, rather a combined issue emanating from other issues of behavioral challenges, including, but not limited to, trust, transparency, relationship, anonymity. For instance,

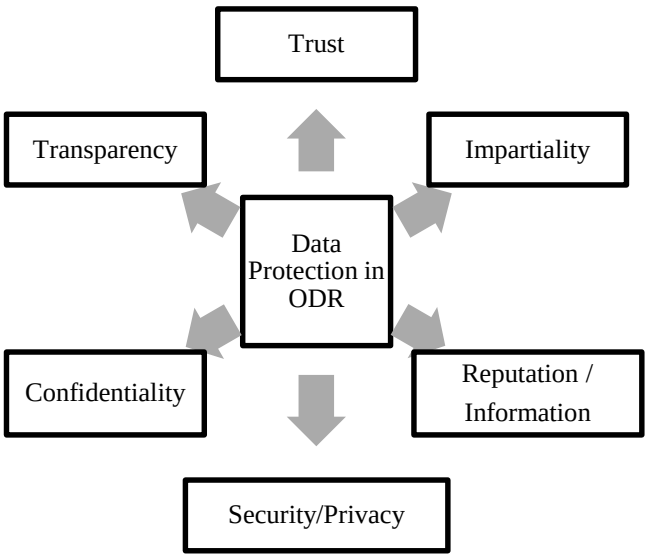
[97] cf Aayog (n 86).

transparency is an important concern, which if not properly explained to users, may cause an issue. However, the 'transparency' concern ultimately affects the major 'privacy and data confidentiality' concern because users/consumers do not tend to believe that their data is protected if not processed transparently".

3. Theme 3: Operational Challenges:

Operational challenges, as was also observed by Niti Aayog's report include – privacy and confidentiality concerns, archaic legal processes, and ODR-related specific issues, such as its enforcement issues. This operational challenge is interlinked with the other two emergent themes (structural and behavioural challenge). For instance, one respondent interestingly observed that "the lack of interaction, specifically, in-person, combined with the no proper legal process, demolishes the users' trust for protected data and security".

Illustration 3: ***Model for Consumer's Data Protection in ODR***



C. Recommendations from the Findings

1. Recommendation 1: Legislative Framework:

The data collection showed that 94.56% of respondents agreed upon having a legislative framework in India that governs both ODR and data protection concerns. The respondents concluded and have also been observed in the Niti Aayog's report, that in India, a strong ODR framework can only be possible, with comprehensive legislation on data protection that handles both security and confidentiality issues that emerges during the ODR procedures.[98] In this respect, the recent Personal Data Protection Bill, 2019,[99] can indeed serve towards being the legal framework that protects users/consumers. As

[98] cf Aayog (n 86).
[99] The Personal Data Bill 2019 (373 of 2019).

such, the data produced online will be secured and trust in the ODR regime will be advocated. Other than that, the legislation should interact with the ODR, for instance, provisions may be added in the Commercial Courts Act, 2015, and the Consumer Protection Act, ultimately recognising ODR in India.

2. Recommendation 2: Building Robust ODR Framework:

Again, the respondents (83.7%) agreed upon that the ODR framework, should itself be robust to promote ODR processes, that do not ultimately tamper with the data produced online. The other respondents (16.3%) interesting said 'no' to the question. They stated that "ODR in itself has a robust framework and the concern is primarily around robust legislative framework".

The authors believe, that online impersonation, violation of confidentiality and data given through ODR procedures, and the tamper with digitally transmitted awards/agreements or tampering with digital evidence are just a few of the issues.[100] To overcome these problems and follow the recommendation of the respondents, ODR providers, which also include government, should focus on developing strong data management and storage systems. In line with the Niti Aayog report, some of the procedures that need to be made to stably incorporate ODR for large-scale conflicts include digital signatures,[101] and document encryption to assure confidentiality[102].

---

[100] Esther van der Heuvel, 'Online Dispute Resolution as a Solution to Cross Border e-Disputes' (2000) OECD <https://www.oecd.org/internet/consumer/1878940.pdf> accessed 13 April 2022.
[101] Graham Ross, 'Challenges and Opportunities in Implementing ODR' in Proceedings of the UNECE Forum on ODR (2003) <https://www.mediate.com/Integrating/docs/ross.pdf> accessed 15 April 2022.
[102] cf Heuvel (n 100).

Illustration 4: ***Themes, Clusters, and Codes identified***[103]

Emergent Themes	Sub-Themes	Recommendations Identified
• Structural Challenges	• Digital Infrastructure • Digital Literacy • Divide in Access to Information and Technology	• Recognition of ODR under Consumer Protection Act, 2005 • Law specifically on ODR and governing data protection
• Behavioural Challenges	• Lack of Awareness • Lack of Trust • Legal Culture / Lack of Interaction • Role of the Government and PSU's • Lack of Transparency	• Building upon reputation • Building upon trust, transparency • Hosting workshops and increasing awareness/ knowledge
• Operational Challenges	• Privacy and Confidentiality Concerns • Archaic Legal Processes • Enforcement of the ODR outcome	• Building upon the Personal Data Protection Bill, 2019 and specifically including the ODR framework

[103] cf Aayog (n 86).

VII. CONCLUSION

This article has established an institutional approach and has drawn heavily on a jurisdictional analysis in an attempt to propose a legal reform, that helps in "*India* [being] *at the forefront of global online dispute resolution movement*".[104] The democratic, varied, and pluralistic potential of ODR[105] can be used to bolster e-commerce dispute resolution in India. When comparing the legal framework and initiatives in national and international jurisdictions, the article aims to reach a focal point for the Indian ODR movement.

However, reaching such a focal point comes with inherent challenges. Through this article, we investigate the major inherent challenge of "data protection", which is embedded and intertwined with the other major challenges, including, trust, transparency, reputation, confidence, security, and privacy. As such, the empirical research, interestingly identified various clusters and limitations posited in the Online Dispute Resolution field, including but not limited to, lack of infrastructure, literacy, knowledge regarding information and technology, awareness, trust, interaction, and alike. For answering and proposing recommendations, the empirical research at last also provides for the same, which mainly includes building and working upon the challenges, including, structural, behavioural, and operational.

[104] cf Aayog (n 86).
[105] cf Heuvel (n 100).

V. ANALYSING THE INTERPLAY BETWEEN END-TO-END ENCRYPTION & PRIVACY: SYMBIOTIC ASSOCIATION OR A MERE FACILITATION?

- Ayush Raj[*]

ABSTRACT

"Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect."- Bruce Schneier

Encryption is a safety wall that protects the confidentiality of data from outside snooping. End-to-end encryption is an integral feature of digital privacy that empowers users to hold their private conversations with themselves without any external interference. Though end-to-end encryptions are not fool-proof, yet they provide the safest structure for data security. With the Central government mandating social media intermediaries to reveal private conversations and their originators for curbing hate speeches, and cyber frauds, and to accelerate cyber patrolling and surveillance, privacy concerns in India have burgeoned. An argument to justify the need for a fragile nature of encryption stems from the restriction posed to enforcement and investigation agencies in conquering digital frauds, piracy, online hate speeches, terror activities, etc. Therefore, it is pertinent to re-evaluate the data protection regime in the country that resonates with the need for individual privacy and balances itself with the obligations of national security and a safe online environment. In this article, at the very outset, the author discusses the history of encryption in India and the landmark Puttaswamy judgment that revitalized the encryption debate in the country. The author, further, deals with the question that whether there is any legally enforceable right of encryption in light of different sector-specific guidelines and the new Data Protection Bill. The paper also delves into the privacy concerns ensuing from weakening encryption and excessive governmental regulation in this regard. In a nutshell, the paper holistically deals with the pros and cons of evading encryption and the author is of the view that personal privacy must not be compromised in any manner and suggests exploring alternative ways to deal with online crimes and ensure online safety rather than breaching encryption arbitrarily.

[*] The author is a third-year student of B.A. LL.B. (Hons.) at Maharashtra National Law University, Nagpur. Views stated in this paper are personal.

I. INTRODUCTION

Encryption is a process of converting plain data into a code, i.e, an unintelligible form that cannot be recovered, and if recovered, would require special arrangements.[1] End-to-end encryption ensures that any third party is restricted to access personal data, thereby ensuring strict confidentiality and privacy in online conversations and transactions. End-to-end encrypted messages can be accessed only by the sender and the receiver and it is coded in the form of a cipher text in transit.[2] The debate surrounding encryption status is of paramount significance because enabling encryption is enabling data privacy while controlling encryption is controlling data flow. What we need is a balance between these extremes that can happen through pre-determined cautious regulation of encryption. It is because there is an imminent need to protect an individual's privacy and at the same time be cognizant of the necessities of law enforcement. The motive should be to safeguard personal interests as well as national interests and therefore, a defined regulation of data and a concrete framework for sharing of personal data becomes quintessential. Pertinently, this regulation must not swing on the docks of executive discretion. Regulating the extent of encryption in a digital ecosystem lands us on the critical question of determining the extent of

[1] Schedule V, Information Technology (Certifying Authorities) Rules, 2000.
[2] Abdalbasit Mohammed & Nurhayat Firal, 'A Review Paper on Cryptography' (7th International Symposium on Digital Forensics and Security, Barcelos, June 2019).

government surveillance on digital service providers. Another intriguing factor, as the supporters of strong encryption claim, is the categorization of activities that would permit enforcement agencies to snoop on someone's private affairs under the pretext of national security.[3]

Encryption, as the proponents of regulating encryption, argue, acts as a digital shield to a host of illicit activities on the web ranging from data breaches and cyber frauds to child pornography and inciting violence.[4] On the other hand, it is also important to note that encryption is not a universal go-to measure for ensuring privacy and confidentiality because many cloud storage firms such as Google need access to unencrypted data, therefore, end-to-end encryption is currently impracticable since it might significantly degrade the present user experience.[5]

In light of the aforesaid and due to the recent policy altercations with respect to governing privacy, in India and worldwide, it is imminent to engage in discussions regarding personal privacy the data protection. This paper seeks to serve such a purpose and present a multi-dimensional analysis of this bone of contention. The author has adopted a streamlined approach to discuss the status quo of the Indian data protection regime and suggest measures for strengthening privacy as well as aiding state authorities. He has also attempted to predict the fate of encryption based on recent developments. The paper at the very beginning provides an overview of the Indian encryption regulations

[3] Trisha Ray, 'The Encryption Debate In India: 2021 Update' (*Carnegie Endowment for International Peace*, 31 March 2021) <https://carnegieendowment.org/2021/03/31/encryption-debate-in-india-2021-update-pub-84215> accessed 1 June 2022.
[4] ibid.
[5] Google Cloud, *How Google Workspace Uses Encryption To Protect Your Data* (Google Cloud Whitepaper, August 2020).

and based on judicial precedents, explores the right to encryption and traceability. In this context, the author has examined the current data protection laws, identified their loopholes, and presented potential solutions to bridge the gap between the need for fair privacy legislation and the exigency of law enforcement agencies to create a better digital environment. Lastly, the paper highlights some key concerns and tries to come up with some significant considerations that can be looked up to while framing a modern data protection law.

II. INDIAN ENCRYPTION LAW: INTERMEDIARY'S POSITION

The scope of information and decryption requests is limited by Rule 13(3) of the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009,[6] to the extent that the intermediary has control over the instruments for decryption and information. As a result, the clause, when read in conjunction with the regulations, does not hold intermediaries liable for information that they were unable to get in the first place. Rule 2(g) of the Decryption Rules supports this view, defining "decryption assistance" as enabling access "to the extent practicable, to encrypted information." As a result, the intermediary's responsibilities regarding decryption requests are constrained. This stipulation is especially important in the case of end-to-end encrypted messaging service providers because intermediates do not have access to messages or decryption keys. It is pertinent to highlight these revisions, in the form of Rules and Notifications, in privacy policies as they evidently clarify that the government has increased its regulation, in a phased manner, to curb hate speeches and

[6] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009.

promote a healthy discourse on digital platforms, and hold the intermediaries liable for the content posted on their platforms and mandate taking down any content, as and when requested by the government in a prescribed time.

A. Puttaswamy Case & Traceability

When we discuss encryption and the legal implications surrounding encryption, we must look toward the decision in *Justice Puttaswamy (Retd.) v. Union of India* (**"Puttaswamy case"**)[7] as a parameter to define the contours of privacy. It is pertinent to analyse and examine the tests put forward by the Apex Court in that case, i.e., any action having any effect on individual privacy must be tested on the grounds of legality, legitimacy, suitability, and necessity. Moreover, the data principal must have adequate safeguards against its exploitation and unwanted decryption.[8]

Coming to legality, it is a settled principle that any executive order must comply with the ingredients of a valid law otherwise it is deemed to be a type of delegated legislation.[9] In this regard, we must first examine whether the government has the lawful authority to intrude into the privacy of an individual by enabling traceability, as privacy has been declared a fundamental and an inalienable natural right under Article 21.[10] The government can only issue content removal orders to intermediaries under Section 69A of the IT Act,[11] and it has no regulatory jurisdiction to authorize any breach of privacy. Section 7 of the Act provides for procedural

[7] *Justice K.S. Puttaswamy and Anr. v Union of India (UOI) and Ors.*, (2017) 10 SCC 1.
[8] ibid.
[9] *E.P Royappa v State of Tamil Nadu and Anr.*, (1974) 4 SCC 3.
[10] *Justice K.S. Puttaswamy and Anr. v Union of India (UOI) and Ors.*, (2017) 10 SCC 1.
[11] The Information Technology Act, 2000 (Act 21 of 2000), s 69.

requirements that are required to be followed by the intermediaries with proper due diligence. Third-party actions are excluded from the ambit of this Section, thus, exempting intermediaries' liability.[12] What is noteworthy, in these Sections is that they impose restrictions on freedom of speech; whether these restrictions possess reasonability or not, can be a matter of discussion, however, they don't allow the government to decode personal conversations in any manner. Therefore, if tested from this parameter, traceability and decryption have a strong case against legality.

That said, one may argue that Section 69[13] provides for government surveillance in certain conditions and they themselves prove the presence of a legitimate state aim and national interest. As discussed, the conditions specified in the Rules are sufficient enough for a legitimate state aim; however, the expansive nature of the Rules and the discretionary power of the executive must be guided by a set of legal principles.

The third test mandated under the Puttaswamy case is that of suitability and necessity and it must be a matter of genuine concern to evaluate whether these measures of decryption could help the government in securing national security, digital safety, and crime control or not.

The criterion for traceability and breaking encryption indicates a state's intent in penalizing creators (originators) while disregarding distributors. It is pertinent to refer to Madras High Court's observation in the case of *S Ve Shekhar v. Inspector of Police*: "the act of forwarding a message amount to accepting and endorsing a message. However, the traceability

[12] Gurshabad Grover, Tanaya Rajwade & Divyank Katira, 'The Ministry And The Trace: Subverting End-ToEnd Encryption' (2002) 14 NUJS L Rev 2.
[13] ibid.

requirement seemingly ignores the culpability of forwarding parties."[14] Thus, the traceability obligation can play a part in developing a culture of impunity in message recipients, who may share the content without critically evaluating it, and still be shielded from the actions of law enforcement agencies as there is an evident loophole in the law. Information recipients play a vital in countering the spread of disinformation and rumours and are able to do the contrary as well, there is a need to balance the position of law that places an equal burden of responsibility on everyone and helps achieve the intended goal. Moreover, when we say that decryption is essential to effectuate actions against cyber frauds or child pornography, there is a lacuna in our approach. This is because, while traceability and decryption might help to find out the originator but they may not help in preventing the propagation of these crimes. The gist of the above argument is to create clarity over the need for traceability to facilitate law enforcement as it does not create any barrier to the crime, but rather only touches a part of surveillance in those cases. Therefore, traceability may not be mandatory in this regard as any common approach cannot be applied to every sort of illegal activity.

III. RIGHT TO ENCRYPTION

Pursuant to the above discussions and descriptions of digital and online privacy, the most important question that pops up is whether there exists any right to encryption in the Indian legal system. In this regard, another parameter that is required to be examined is the scope of the Puttaswamy case on encryption debates. We can reasonably infer, both from the Puttaswamy case,

[14] *S Ve Shekhar v Inspector of Police*, 2018 SCC OnLine Mad 13583.

as well as, by looking at data breaches on various online service providers,[15] that both state and non-state interference can be a potent threat to one's privacy. The Pegasus controversy has interlinked national security and privacy in a novel manner and it also raises serious concerns regarding our privacy legislation.[16]

The terms 'Right to Encryption' and 'Right to Privacy' arise out of the same concept. The state's legal authority to undertake surveillance only goes as far as one's right to privacy. Any governmental action weakening public encryption would be a violation of the right to privacy and would have to pass the Puttaswamy test in order to comply with the Supreme Court's interpretation of the right to privacy.

One may argue that a strong encryption policy protects the right to freedom of speech and expression of an individual and that the power to trace the first originator, as argued, creates conflicts with Article 19. Additionally, one may claim that traceability hinders the independent authority to express on digital platforms as the sender can be subject to unreasonable and biased action against him. It is because one can claim to be in the constant threat of surveillance if it goes against the set norms. However, it is pertinent to note that this connection is flawed because encryption is concerned with privacy and confidentiality rather than free speech. Hence, breaking or weakening

---

[15] Aditi Agrawal, 'Traceability and end-to-end encryption cannot co-exist on digital messaging platforms: Experts' (*Forbes India*, 15 March 2021) <https://www.forbesindia.com/article/take-one-big-story-of-theday/traceability-and-endtoend-encryption-cannot-coexist-on-digital-messaging-platforms-experts/66969/1 accessed> 24 April 2022.

[16] Ankita Shethy, 'Pegasus and the Law' (*Mondaq*, 1 September 2021) <https://www.mondaq.com/india/privacy-protection/1107548/pegasus-and-the-law> accessed 4 May 2022.

encryption cannot be essentially termed an attack on free speech. At this juncture, it is pertinent to mention the Puttaswamy case at the center, as the Apex Court held privacy to be a part of personal liberty under Article 21 instead of making it a subordinate of Article 19. Another striking indicator of a clear distinction between freedom of speech and the 'right to encryption' is the close resemblance of exceptions to free speech under Article 19(1) to exceptions for state surveillance under the Personal Data Protection Bill (**"PDP Bill"**).[17] Therefore, it goes both ways; freedom of speech must not be absolute but the state must also ensure that the privacy of an individual is not infringed which tackles the extended application of 'freedom' of speech.

The Srikrishna Committee[18]on data protection was constituted by the central government to examine the issues of privacy, data protection, and artificial intelligence. The PDP Bill was based on the report of this Committee, which was constituted in response to the Supreme Court's ruling in the Puttaswamy case, in August 2017 and submitted its report in July 2018. The Committee acknowledged the need for de-identification and encryption for data fiduciaries. It explicitly mentioned encryption as a digital safeguard but it didn't lay any proper procedural framework for decryption. While the Committee strongly recommended that the Puttaswamy test must be applied in cases of government surveillance and there must be a proper judicial or legislative supervision over the same; however, it failed to define what valid and lawful decryption is. Moreover, currently, the data protection regime of

[17] The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019).
[18] Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians*, (July 2018) 55.

the country lacks the necessary safeguards and shields against any possible exploitation of decryption by the government.

The Committee, however, did not attempt to rectify this flaw in the Personal Data Protection Bill, instead advocated that the Central Government enact new legislation to oversee intelligence collection. According to the committee, any non-consensual access to personal data should be subject to both legislative monitoring and judicial clearance to guarantee both ex-ante and ex post facto responsibility. This advice has yet to be implemented by the executive.

IV. THE PERSONAL DATA PROTECTION BILL: A ROLLER COASTER RIDE

Prior to discussing the PDP Bill, it is important to take cognizance of the formulation of the National Encryption Policy, 2015.[19] This policy was redacted due to massive opposition; however, it is pertinent to mention that the Policy consisted of regulations and protocols for encryption, digital signatures, etc. It stipulated that the encryption service providers should retain the data for a prescribed period of time to facilitate law enforcement. Additionally, it also required that those service providers enter into an agreement with the government for sharing the data.[20] The above two requirements sufficiently clarify the reasons for its withdrawal.

The 2018 version of the Data Protection Bill sought to acknowledge the role of encryption and decryption and attempted to carve their boundaries. The Bill, under Section 42 stipulated that lawful decryption by enforcement

[19] The Draft National Encryption Policy, 2015.
[20] The Draft National Encryption Policy, 2015.

agencies is permitted on account of the 'security of the state' and that decryption must be proportionally just and approved by law.[21] Furthermore, decrypting personal data also came under the ambit of Section 4 which mandated fair and reasonable use of personal data. Sections 29, 30, and 31 deal with maintaining proper transparency and providing adequate security safeguards in cases of processing of personal data by data fiduciary.[22]

A. The 2019 Version

In 2019, a new version of the Bill was submitted, with Section 35 expanding the extent of the immunity granted to government entities for data processing. It gave the government the authority to exclude any or all of its agencies from Bill's restrictions. It removed the words 'necessity' and 'proportionality,' and expanded the grounds to include the "interest of India's sovereignty and integrity, the security of the State, friendly relations with foreign States, and public order; or for preventing incitement to the commission of any cognizable offense pertaining to India's sovereignty and integrity, the security of the State, friendly relations with foreign States, and public order",[23] i.e., aligning with the exemptions under Article 19 and thereby giving more discretionary powers to the government to act upon data protection and privacy.

---

[21] 'Some Points On Lawful Interception Or Monitoring Or Decryption Of Information Through Computer Resource' (*Press Information Bureau, Government of India*, 21 December 2018) <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1556945>.
[22] The Personal Data Protection Bill, 2019 (Bill No 373 of 2019).
[23] ibid.

V. INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE), RULES, 2021: VIOLATING ARTICLE 21

The latest addition to this data protection debate is the Intermediary Guidelines, 2021 which further gave a free hand to the government. It holds the intermediaries liable for the content posted on their platforms and mandate taking down any content, as and when requested by the government in a prescribed time.[24] Permitting the originator of messages exchanged on digital platforms such as WhatsApp and Telegram to be traced and tracked is a violation of the right to privacy, which the Supreme Court declared a fundamental right under Article 21 in the Puttaswamy case. This argument essentially bases itself on the concept that exposing the first originator of a message is tantamount to exposing the privacy of that individual and infringing his right to speech. Tracing the original source in response to an executive or court order might jeopardize the basic right to privacy by interfering with end-to-end encryption of private communication. A comprehensive reading of the Rules also signals the overturning of the *Shreya Singhal* decision, in which the Supreme Court invalidated Section 66-A of the Information Technology Act, 2000, which penalized "offensive" information on the basis of arbitrariness.[25] It is because these guidelines are meant to keep a strict eye on the content being published on social media intermediaries and while Shreya Singhal's judgment sought to create a free online atmosphere, the former tends to bring a multi-layered regulation on online content. It is also important to analyse the judicial trend and the progress of privacy

[24] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[25] *Shreya Singhal v Union of India*, (2013) 12 S.C.C. 73.

jurisprudence in the country. While some High Courts have partially invalidated these Rules[26] but overall judicial inclination in privacy-related matters tends to be pro-state as the data protection scheme is quite nascent and national interest and integrity are prioritized.

VI. CONCERNS REGARDING WEAK ENCRYPTION

A comprehensive and holistic analysis of the Data Protection when read in consonance with the Intermediary Guidelines, 2021 will lead us to infer that the law wants data protection to be stern and effective but the same law excludes government agencies from its domain. Therefore, there is a clear dichotomy in the government's approach regarding this. Furthermore, the Rules snatch the discretion and flexibility of the intermediaries to allow or disallow a specific content and now the government can mandatorily ask the intermediary to take down any content if the same is interfering with the peace and security of the country.

In light of the above-stated contradiction, there is an imminent need to balance the need for surveillance and to guard the privacy of the citizens. Encryption, in particular, is of paramount significance as the digital economy constantly needs strong vigilance over transactions and communications. So, strong encryption is not only required to protect private conversations on social platforms such as WhatsApp but is equally necessitated for facilitating a hassle-free digital transaction. Master Direction on Digital Payments Security Controls released by the Reserve Bank of India (**"RBI"**) also

[26] *Agij Promotion of Nineteenonea Media Pvt. Ltd. v Union of India, W.P. (L) No 14172 of 2021*; *Nikhil Mangesg Wagle v Union of India,* P.I.L. (L) No 14204 of 2021.

provides for multiple layers of protection such as encryption, authentication, digital certificates, etc.[27]

Another troubling aspect of interfering with the mechanism of encryption is that it is quite complex and any change in this mechanism to lower its standard might attract fraudulent cyber-attacks on it. This concern is specifically problematic as India still lags way behind in ensuring global cyber security protocols.[28] Prior channels that were modified to meet similar government needs ended up being risky and prone to cyber malice, to the point that flaws were exploited for years before they were discovered.[29] By breaching the nondisclosure assurance and making the ingredients of all users' messages perceptible to messaging providers, employees and contractors of the service provider garner unauthorized access to individuals' personal conversations, and a large central cache of extremely sensitive information is created, which might be a tempting target for threat actors. No technology created to enable special access for surveillance and law enforcement has been sufficient to evade generating significant faults so far. There are several other reasons why this selective exemption should not be given effect to. Exemption of every government agency from the scope of the data protection law also strengthens the possibility of political opponents being placed under the

[27] 'Internet Banking In India – Guidelines', (*RBI*, 2001) <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0> accessed 04 May 2022.

[28] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (*UNHRC* 2015) <https://www.undocs.org/A/HRC/29/32> accessed 04 May 2022.

[29] Bedavyasa Mohanty, 'The Encryption Debate in India' (*Carnegie Endowment for International Peace*, 30 May 2019) <https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213> accessed 04 May 2022.

scanner and can aid the government in pursuing its illegitimate political motives.

The government should not compel the service providers to execute traceability rather the focus should be to enact laws that are, in principle, aligned to the concept of data minimalization i.e. states should create laws that force companies to collect the least amount of user information that they need to operate and provide their service.[30] The problem with traceability and decryption is that it contradicts the above principle and therefore, facilitates not just state surveillance, but encourages more private surveillance i.e bad actors with ulterior motives. Hence, the traceability obligation interferes with the security and privacy of the majority sans good cause, ostensibly to apprehend a few malicious activities who can easily cheat these technologies and sustain their activities.

VII. THE WAY FORWARD

Keeping in view the need for a balanced data protection law, an overreaching encryption guideline can be issued that will serve dual objectives. Firstly, it will clear the conundrum regarding encryption and decryption and lay down a procedural framework, and secondly, it will curb the jurisdictional conflict between different regulatory bodies and enforcement agencies that arise due to sector-specific overlapping guidelines. In this regard, introducing a local key for accessing personal data and unlocking encryption can be a useful measure. The main element behind this 'key' is that it should be kept in the device only and therefore, agencies can access the key only

[30] Andrew Grosso, 'Mandatory Key Escrow Encryption – What's Wrong with the Governments Argument in Favor of It' (1999) 14 Crim Just 34.

when they are in possession of the device.[31] This can be implemented to curtail the unlawful decryption of personal data on arbitrary and vague grounds. Moreover, if the Rules intend to curb and restrict hate speeches from spreading through online platforms, it can be interesting to explore and carve out possibilities to trace the first originator of the message without breaking the encryption. In this respect, metadata collected by online platforms can be taken into consideration for surveillance and investigative purposes without breeching encryption. This method is already utilized by several platforms.[32] However, this large-scale use of this metadata is subject to technological and economic viability.

If we compare the data protection laws of India with that of the United States of America (**"USA"**), the European Union (**"EU"**), and Australia, we can easily figure out some similarities as well as differences. The USA doesn't have a nationalized data protection guideline rather it has federal laws and sector-specific guidelines for different industries. Likewise, Australia also has different state privacy legislations. Notably, Australia has a National Protection Authority that is currently lacking in India. Furthermore, it is recommended that India should also have a specific online privacy regulation with respect to cookies, location data, and advertising.[33] Lastly, a comparison of the EU's General Data Protection Regulation with India's proposed privacy law shows that the ambit of Indian law is wider in terms of its applicability. However, the most significant distinction between both laws lies in the way

[31] Chinmayi Arun, 'Paper-Thin Safeguards and Mass Surveillance in India' (2014) 26 National L School of India Rev 105.
[32] ibid.
[33] Harmanpreet Singh, 'Data Protection and Privacy Legal-Policy Framework in India: A Comparative Study vis-à-vis China and Australia', (2018) 2 Amity J of Computational Sciences 22.

they treat anonymous data. While GDPR does not govern anonymous data, the Indian law empowers the central government to direct organizations to disclose anonymized personal data and even non-personal data.[34] Therefore, access to non-personal data is a cause of concern that needs to be addressed and the government should consider removing this provision as it is subject to abuse on the grounds of political, social, and economic interests. Moreover, data portability is also a feature on which these two legislations differ. The Indian deviation in this respect is that the right to data portability is independent of any legal basis while as per the GDPR data portability is only allowed when it arises out of a legal contract.[35]

Moreover, reliance on sector-specific encryption policies, particularly in the finance sector can be of utmost utility in formulating a national encryption guideline. In this regard, SEBI and RBI have their own guideline to secure digital transactions, for example, the former follows 64/128-bit encryption[36] and the latter follows 128-bit SSL encryption[37] in their respective digital operations.

It should be evidently clear from the above discussion that encryption cannot be interfered with by inserting vague and arbitrary clauses. All

---

[34] Poulomi Sen, 'EU GDPR and Indian Data Protection Bill: A Comparative Study' (*SSRN*, 26 April 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834112> accessed 04 May 2022.

[35] Kurt Wimmer, CIPP/E, CIPP/US, Gabe Maldoff & Diana Lee, 'Indian Personal Data Protection Bill vs. GDPR' (*International Association of Privacy Professionals*, March 2020) <https://iapp.org/resources/article/comparison-indian-personal-data-protection-bill-2019-vs-gdpr/> accessed 04 May 2022.

[36] 'Committee on internet based securities trading and services – first report' (*SEBI*, 2001 <https://www.sebi.gov.in/sebi_data/commondocs/99290report_p.pdf> accessed 20 April 2022.

[37] 'Internet Banking in India – Guidelines', (*Reserve Bank of India*, 14 June 2001) <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=414&Mode=0> accessed 04 May 2022.

programs that assist online communications should be permitted to use an end-to-end encryption scheme. India needs unique legislation that addresses individual privacy and, therefore, a clear law that establishes clear guidelines for companies, law enforcement agencies, and people on how to manage user data is needed. Existing rules and regulations must be updated immediately to address the rise of secure communication services.[38] This would be accompanied by an increase in the general level of internet security to promote free expression and e-commerce. India should also focus on finding and implementing worldwide best practices in information security and data protection, which it may learn from the EU Data Protection Directives.[39]

VIII. CONCLUSION

In the new digital world order, it is pertinent to stress upon the fact that anonymity seldom acts as a pre-condition for free speech as it prevents unwanted and biased personal responses. At the same time, it is equally paramount to take care of a nation's security and integrity from technological weapons because advancement in technology has been a boon, both, for pursuing one's legitimate as well as illegitimate interests. In this respect, it is imminent upon the parliament to extensively discuss the issue of privacy and come up with a clear and concise law that leaves no space for ambiguous interpretation and misuse by any of the stakeholders. The parliament can

[38] 'Srikrishna Committee Data Protection Bill and Artificial Intelligence in India', (*The Centre for Internet & Society*, 03 September 2018) <https://cis-india.org/internet-governance/blog/the-srikrishna-committee-data-protection-bill-and-artificial-intelligence-in-india> accessed 04 May 2022.

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

reorganize the joint parliamentary committee and open the draft Bill for public review and comments. Another interpretation of end-to-end encryption is to further security interests. The partial deterioration of law enforcement instruments should not be used to undermine other critical national security concerns.

The author is of the stern opinion that law enforcement and individual privacy can complement each other and go hand-in-hand without causing any hindrance. The author reiterates that overreaching legislation is required to tackle the issue of data protection to generate uniformity in privacy jurisprudence. The use of technological equipment such as encryption in certain pre-defined circumstances coupled with the use of metadata can possibly serve the purpose. It is also worth noting that end-to-end encryption allows for safe network connection anywhere in the globe, regardless of data storage location or service provider. Several data breaches in the recent past have also re-ignited the need to have a strong encryption policy.[40] Advancement in technology has led to people oversharing their information digitally, for example, sharing live locations and keeping their personal documents on social platforms, all of this is empowered and enabled by encryption only. Therefore, the need of the hour is to devise a harmonious way to deal with the privacy of individuals, albeit, ensuring strict vigilance against cyber frauds and other online crimes i.e., a data protection law that guards individual privacy and empowers institutional grip against new-age digital crimes.

[40] Devansh Kaushik, 'Deciphering Encryption Rights In India: The Road Ahead' (2021) Global Privacy L Rev (Wolters Kluwer).

Keeping It Online: Developing an ODR Mechanism for India's E-Commerce Disputes - by Pratham Arya & Lisa Sankrit

Data Localisation and Cross-Border Flow Of Data: Balancing the Incongruent Dimension of Barriers, Safeguards and "Free Flow Of Data" - by Raj Shekhar & Aman Yuvraj Choudhary

Data Localization: An Issue Beyond Borders - by Gargi Whorra

Online Dispute Resolution Platform for B2C and B2B E-Commerce in India: A Critical Appraisal - by Abhay Raj & Ajay Raj

Analysing the Interplay between End-to-End Encryption & Privacy: Symbiotic Association or a Mere Facilitation? - by Ayush Raj