

IJLT

THE INDIAN JOURNAL OF
LAW AND TECHNOLOGY

Volume 18 | Issue 2 | 2022

[Cite as: 18 IJLT, < page no. > (2022)]

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY
BANGALORE

Price: Rs. (in 2 issues)

© The Indian Journal of Law and Technology 2022

The mode of citation for this issue of The Indian Journal of Law and Technology, 2022 is as follows:

18 IJLT, <page no.> (2022)

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission.

The articles in this issue may be reproduced and distributed, in whole or in part, by non-profit institutions for educational and research purposes provided that such use is fully acknowledged.

Published by:

Student Bar Association

National Law School of India University

Nagarbhavi, Bangalore – 560072

Website: www.ijlt.in

Email: ijltedit@gmail.com

Distributed exclusively by:

Eastern Book Company

34, Lalbagh, Lucknow - 226 001

U.P., India

Website: www.ebcwebstore.com Email: sales@ebc.co.in

The views expressed by the contributors are personal and do not in any way represent the institution.

IJLT
WWW.IJLT.IN

THE INDIAN JOURNAL OF
LAW AND TECHNOLOGY

Volume 18 | Issue 2 | 2022

BOARD OF EDITORS

Chief Editor

Devansh Kaushik

Deputy Chief Editor

Lakshmi T. Nambiar

Editors

Aarohi Chaudhuri

Ankit Kapoor

Debditya Saha

Manav Sridharan

Sushant Khalkho

Line Editors

Debmalya Biswas

G Bharat Krishna

Palak Kumar

Shivansh Bagadiya

Administrative Member

Shubh Mittal

Technical Member

Pranav Kumar

PATRON

Prof. (Dr.) Sudhir Krishnaswamy
Vice-Chancellor, National Law School of India University

IJLT

THE INDIAN JOURNAL OF
LAW AND TECHNOLOGY

Volume 18 | Issue 2 | 2022

BOARD OF ADVISORS

Justice S. Ravinder Bhat
Judge, Supreme Court of India

Justice Prathiba Singh
Judge, Delhi High Court

Dr. Graham Greenleaf
Professor of Law, University of New South Wales,
Sydney, Australia; Co-Director, Cyberspace Law
and Policy Centre, Sydney, Australia

Dr. T. Ramakrishna
Professor of Law, National Law School of India University,
Bangalore, India; Coordinator, Centre for Intellectual
Property and Research and Advocacy

Rahul Singh
Associate Professor of Law, National Law School of India
University, Bangalore; Visiting Professor, Harvard University

Rahul Matthan
Founding Partner and Head of Technology
Practise Group, Trilegal

Malavika Jayaram
Executive Director, Digital Asia Hub; Faculty Associate,
Berkman Klein Center, Harvard Law School

Chinmayi Arun
Resident fellow of the Information Society Project,
Yale Law School; Founder Director of the Centre
for Communication Governance

CONTENTS

ARTICLES

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

Luca Belli 145

Designing the Narratives of Protests: The Role of Design in
the Portrayal of Protests on Social Media Platforms in India

Saumyaa Naidu 203

Data Privacy and Elections in India:
Microtargeting The Unseen Collective:

Sayantana Chanda 272

Bringing Shadow Libraries out of Legal Shadows:
An Opportunity for the Delhi High Court

Rahul Bajaj and Anchal Bhateja 316

NEW DATA ARCHITECTURES IN BRAZIL, CHINA, AND INDIA: FROM COPYCATS TO INNOVATORS, TOWARDS A POST-WESTERN MODEL OF DATA GOVERNANCE

*Luca Belli**

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

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

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

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

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

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

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

Introduction	146		
I. Background: The Rise of Data Architectures in Brazil, China, and India	152		
A. Brazil: Towards the Harmonisation of a Fragmented System	155		
B. China: Building a New Type of Architecture, Blending Policy, Institutional, and Investment Upgrades.	159		
C. India: The Unfinished Journey towards a Data Protection Law	164		
II. New Data Architectures: Legal Transplants and Innovative Elements	171		
A. Brazil.	172		
i. The Brazilian Data Protection Authority			
		(ANPD) and the National Council for the Protection of Personal Data and Privacy	177
		B. China.	179
		i. Data Security with Chinese Characteristics.	186
		C. India	191
		i. The Personal Data Protection Bill 2021, the Digital Personal Data Protection Bill 2022, and a New Bill with Consultation in 2023.	193
		ii. The Data Empowerment and Protection Architecture.	197
		III. Conclusion: The Emergence of a Post-Western Model of Data Governance	199

INTRODUCTION

This paper explores the recent data protection evolutions in three leading emerging economies: Brazil, China, and India. Members of the BRICS grouping, projected to be amongst the largest economies in the world by 2030¹, the BIC of BRICS provide some particularly interesting examples of innovative approaches to data governance. While Brazil, China, and India

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

are not renowned for their commitment to (data) privacy², the recent innovations introduced by these countries are particularly relevant. Indeed, due to their considerable geopolitical and economic weight at both regional and international levels, their policy choices are likely to be considered as models to which national and international frameworks may adapt in the future.

On the one hand, Brazil, China, and India are becoming increasingly relevant technological players whose software applications, hardware, and artificial intelligence (AI) systems are gradually adopted well beyond their national borders. On the other hand, having some of the largest populations and economies in the world, these countries can afford the luxury of foreseeing an extraterritorial scope for their regulations in their data protection frameworks. Until recently, only the European Union had dared to include the “privilege” of extraterritorial reach in its data protection framework. Indeed, extraterritorial scope seems to be a path chosen primarily³ by last-generation data regulations of large countries or regional blocks, such as the European Union, which have the bargaining power and institutional capacity necessary to afford imposing such extraterritorial reach.

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

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

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

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

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

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

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

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

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

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

Furthermore, it is important to note that the normative regimes and approaches to digital governance of the countries present an interesting degree of convergence. The similarities seem to be facilitated both by their willingness to transplant into their national frameworks some key elements of foreign systems which act as common sources of inspiration, and by their shared membership of the BRICS grouping, which increasingly acts as a “pentilateral” digital governance forum.⁶ Curiously, despite the existence of relevant scholarship exploring the economic and geopolitical relevance of the BRICS countries⁷ and the BIC part of BRICS, their digital policies and particularly their data architectures, are remarkably underexplored. Hence, this paper should be seen as part of a broader effort aimed at providing further insight and visibility to non-Western approaches to digital policies driven by leading emerging countries, especially the members of the BRICS grouping.⁸

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

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

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

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

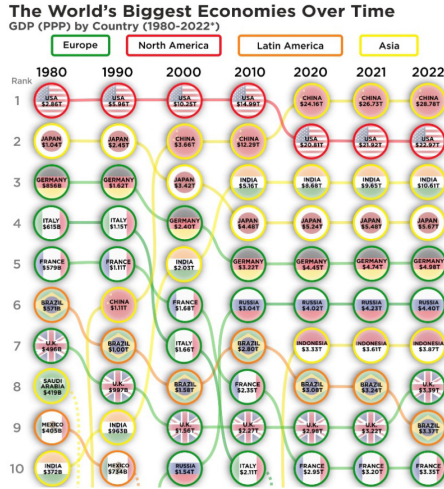


Table 1: Largest Economies in The World Over the Last 40 Years. Source *Howmuch.net*⁹, estimates by International Monetary Fund.

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

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

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

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

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

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

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

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

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

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

I. BACKGROUND: THE RISE OF DATA ARCHITECTURES IN BRAZIL, CHINA, AND INDIA

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

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

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

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

¹³ See (n 5).

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

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

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

¹⁴ Since 2014, the countries have discussed the creation of the Working Group of Experts of the BRICS States on security in the use of ICTs and the BRICS Working Group on ICT Cooperation, which were formalised with the 2015 BRICS Declaration. See ‘BRICS (VII BRICS Summit) “Ufa Declaration” (9 July 2015)’ (BRICS) <www.brics2015.gov.in/BRICSDocuments/2015/Ufa-Declaration-2015.pdf> accessed 8 October 2021. The empirical research conducted by the CyberBRICS project provides a useful comparison of an ample range of elements of the BRICS national data protection frameworks. A detailed comparative analysis of such elements is available in “BRICS Data Protection Map” updated by the CyberBRICS Project in December 2021. “Data Protection across BRICS Countries” (*CyberBRICS* March 28, 2022) <<https://cyberbrics.info/data-protection-across-brics-countries/>> accessed 1 January 2023.

¹⁵ ‘BRICS (IX BRICS Summit) “Xiamen Declaration” (4 September 2017)’ (MEA) <www.mea.gov.in/uploads/publicationdocs/28912_xiamendeclaratoin.pdf>

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

The Snowden disclosures had a particularly dire effect on the countries, confirming with evidence the long-held suspicions of US global espionage via home grown digital technologies. Such evidence included the illegal wiretapping of the Brazilian President's personal phone¹⁷ and the communications of numerous members of the Brazilian government.¹⁸ The reaction of the then President Dilma Rousseff, eloquently illustrated in her opening statement of the 68th UN General Assembly, is a potent reminder of the NSA scandal consequences:

As many other Latin Americans, I fought against authoritarianism and censorship, and I cannot but defend, in an uncompromising fashion, the right to privacy of individuals and the sovereignty of my country.

In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy. In the absence of the respect for sovereignty, there is no basis for the relationship among Nations.

*We face, Mr. President, a situation of grave violation of human rights and of civil liberties; of invasion and capture of confidential information concerning corporate activities, and especially of disrespect to national sovereignty.*¹⁹

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

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

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

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

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

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

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

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

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

A. Brazil: Towards the Harmonisation of a Fragmented System

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

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

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

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

²³ Belli ‘BRICS Countries to Build Digital Sovereignty’ (n 16).

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

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

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

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

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

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

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

Importantly the process leading to the elaboration of LGPD took almost a decade since the proposal of the first official Draft Bill on the Protection of Personal Data and Privacy.²⁸ This was based on a proposed model law debated within the Mercosur (the international economic organisation composed of Argentina, Brazil, Paraguay, and Uruguay) working group on electronic commerce.²⁹ The Brazilian Ministry of Justice opened the first public consultation on a data protection bill in 2010.³⁰ The Draft Bill was largely moulded on Council of Europe Convention 108 and the EU Directive 95/46/CE, which were the main legal reference at the time and already included some typical Brazilian law features that were maintained until the final text of the LGPD, such as the explicit reference to core elements of consumer law.

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

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

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

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

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

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

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

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

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

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

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

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

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

Brazilian Constitution, which was enacted in February 2022.³⁵ By granting personal data protection the rank of a fundamental right, the Brazilian Congress took a landmark step towards the recognition of the importance of personal data and its protection for the Brazilian people, especially considering recent technological developments. However, it is important to stress that the Brazilian Congress failed to seize the opportunity to define what are the essential elements of such a right – e.g., the principle of consent, legality, fairness, transparency, independent overview, etc. – which have been included in other experiences of the fundamental right to data protection, such as in Article 8 of the EU Charter of Fundamental Rights or Article 6 of the Mexican Constitution. Moreover, while the country has made considerable advancements, data protection compliance and a data protection culture are still very far from being achieved.

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

Chinese efforts to start regulating personal data processing started in the mid-2000 and were substantially upgraded in 2012, when the National People's Congress decided to initiate the elaboration of sectorial regulations, with the aim to strengthen the data protection rights of consumers³⁶ while establishing define a new cybersecurity and informatisation framework.³⁷ The Standing Committee of the National People's Congress updated the Consumer Protection Law (CPL) in 2013, conferring the right of data protection on consumers under Article 14. Since then, data protection principles such as confidentiality, purpose specification and consent, began having fundamental importance through reference in regulations.³⁸ In this perspective, the CPL was amended to include guidelines for regulating online consumer

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

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

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

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

transactions, stipulated in Articles 25, 28 and 29³⁹, demanding that businesses preserve consumer information confidentiality. Thus, it prohibited the illegal disclosure, sale or provision to third parties without the consent of consumers.

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

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

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

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

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

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

⁴² *ibid.*

⁴³ Pernot-Leplay (n 36) 72.

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

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

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

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

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

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

⁴⁷ Pernot-Leplay (n 36) 74-75.

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

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

⁵⁰ Jiang (n 38) 190.

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

⁵² *ibid.*

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

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

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

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

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

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

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

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

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

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

⁵⁶ Yu-Jie Chen, Ching-Fu Lin and Han-Wei Liu, “‘Rule of Trust’: The Power and Perils of China’s Social Credit Megaproject” (2018) 32 *Columbia Journal of Asian Law* 1.

⁵⁷ Ling Li, “‘Rule of Law’ in a Party-State: A Conceptual Interpretive Framework of the Constitutional Reality of China” (2015) 2 *Asian Journal of Law and Society* 93.

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

⁵⁹ For a detailed analysis of China’s “Cyber Power Strategy”, see Rogier Creemers, “How China Intends to Become a ‘Cyber Power’” (2020) N° 177-178 *Hérodote* 297.

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

⁶¹ See Matthew Steven Erie and Thomas Streinz, ‘The Beijing Effect: China’s “Digital Silk Road” as Transnational Data Governance’ (2021) 54 *NYU J Int’l L & Pol* 1.

infrastructures⁶² that enable data governance in DSR countries, according to Chinese technical standards. To these initiatives, one must add the considerable influence exercised by the extraterritorial scope of its recently adopted data-related regulations, notably by PIPL.

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

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

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

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

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

⁶⁴ *ibid.*

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

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

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

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

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

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

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

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

The second objective has been facilitated largely by the implementation of Aadhaar. Indeed, the word “Aadhaar” which literally means “foundation” is apt since the digitalisation of identity has been deemed as the cornerstone of digital transformation since the early stages of the Digital India implementation. However, the growing ubiquity of Aadhaar came under sustained criticism from various quarters. The debate on the privacy concerns over Aadhaar resulted in a clutch of petitions before the Supreme Court that challenged the validity of the legislation that enabled the system: the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. The five-judge bench of the Supreme Court that heard the petitions stated that, since the petitions claimed infringement of the right to privacy, it was of utmost importance to determine whether this right existed under the Indian Constitution. It referred this issue to a bench of nine judges of the Supreme Court, which held in August 2017 that a right to privacy did exist under Article 21.⁶⁹

In a long line of past cases, privacy was used to protect specific interests, such as privacy from night-time police visits in the Kharak Singh case or privacy from telephone tapping in PUCL v Union of India. The narrative around data protection in India reached a crescendo during the hearings in the *K.S. Puttaswamy v Union of India* (2017) “right to privacy” case.⁷⁰ In a landmark verdict, crafted by a rare nine-judge bench, the Supreme Court of India affirmed the right to privacy⁷¹ as a fundamental right. The ruling proclaimed that “the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution”.

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

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

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

⁷⁰ *ibid.*

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

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

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

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

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

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

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

⁷³ See Matthan (n 67).

⁷⁴ *ibid* 112.

⁷⁵ *ibid*.

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

Bill⁷⁷ and an accompanying report interestingly entitled ‘A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians’.⁷⁸ Ultimately, the Personal Data Protection Bill was introduced into Parliament in December 2019, after more than two years of fierce debate on the bill’s provisions.

Importantly, rather than pushing to fast-track this hugely significant bill, India’s minister of information technology, Ravi Shankar Prasad, referred it for scrutiny to a Joint Parliamentary Committee (‘JPC’) on the Personal Data Protection Bill, 2019.⁷⁹ The JPC conducted numerous meetings with Government ministries, industry bodies and various stakeholders. It also held meetings for clause-by-clause considerations of the PDP Bill. After two years of deliberation, the JPC tabled its report in December 2021, appending its recommendations to a substantially revised version of the law, named the ‘Data Protection Bill, 2021’.

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

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

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

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

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

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

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

Table 2: Personal Data Protection Bill timeline

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

⁸⁰ See s 2.3.1 of this paper.

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

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

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

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

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

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

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

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

II. NEW DATA ARCHITECTURES: LEGAL TRANSPLANTS AND INNOVATIVE ELEMENTS

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

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

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

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

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

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

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

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

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

A. Brazil

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

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

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

⁸⁸ “Data Protection across BRICS Countries” (n 81) Policy Question 9.

⁸⁹ *ibid* Policy Question 13.

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

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

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

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

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

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

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

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

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

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

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

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

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

- I. *support and promotion of activities of the controller; and*
- II. *protection, in relation to the data subjects, of the regular exercise of their rights or provision of services that benefit them, observing their legitimate expectations and the fundamental rights and liberties, pursuant to the provisions of this Law.*

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

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

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

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

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

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

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

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

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

Since 2014, Article 4 of the Civil Rights Framework for Use of the Internet in Brazil has enshrined interoperability into legislation, considering the promotion of “open technology standards that enable communication, accessibility and interoperability between applications and databases” as one of “the objectives of the regulation of Internet use in Brazil”.⁹⁶ While the Brazilian data protection authority, ANPD, should take the lead⁹⁷ as regards the definition of interoperability standards for personal data, in accordance with article 40 of the LGPD,⁹⁸ the ANPD has not even clarified when this all-important issue will be regulated. Interoperability, and the right to data portability, whose effective implementation depends on the existence of interoperability standards, exist only on paper so far in Brazil. This is because the ANPD has not even included the definition of interoperability standards in its first regulatory agenda, published in January 2021.⁹⁹

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

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

⁹⁶ The Civil Rights Framework for the Internet, better known as *Marco Civil da Internet* (MCI), Federal Law n. 12.965 of 2014. Available at: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.html> accessed 1 January 2023.

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

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

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

3. The execution of agreements, contracts, or legal provisions in an instrument which explicitly allows the sharing of such data, as long as the agreements, contracts are communicated to the ANPD.
4. The protection of the integrity and security of the data subject and to prevent fraud or other financial irregularities.

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

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

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

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

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

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

The involvement of a variety of stakeholders into policy elaboration and implementation, in the context of a participatory multistakeholder governance¹⁰² is, indeed, deeply rooted in the DNA of Brazilian digital policymaking¹⁰³, and has been baked into the new Brazilian data architecture, shaped by the LGPD. The multistakeholder council advising the ANPD board has a primarily consultative function and is only a supportive body rather than a decision-making one but enshrines the quintessentially Brazilian multistakeholder approach to digital governance.¹⁰⁴

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

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

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

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

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

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

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

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

The enthusiasm with the enormous potential of this multistakeholder council, however, must be tempered with a good dose of pragmatism. Having held its first meeting¹⁰⁶ only in November 2021, the National Council for the Protection of Personal Data and Privacy is in its early phase of implementation but, its activities have not received particular attention and even finding basic information about the activities of this body on the ANPD website is a remarkably challenging task. While it is still impossible to measure the impact that such multistakeholder body can have, especially at such an early phase of its experimentation, it is safe to argue that it represents one of the most innovative features, if not the most innovative, of the Brazilian data protection architecture. The Council has indeed the potential to act as a small *xitong*,¹⁰⁷ dedicated to personal data governance, thus creating a valuable forum for stakeholders to address shared concerns and identify shared solutions.

B. China

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

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

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

¹⁰⁷ See (n 47).

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

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

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

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

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

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

¹¹⁰ See Leplay (n 36) 63.

¹¹¹ *ibid.*

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

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

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

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

¹¹⁴ Cybersecurity Law of China 2017, art 15.

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

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

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

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

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

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

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

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

approach¹¹⁹, offering detailed instructions and concrete examples – especially in its appendix – illustrating how to comply with normative provisions. Notably, the Specification Annexes provide examples of what is to be considered personal information (annex A); a guide on how to identify sensitive personal information (Annex B); methods to safeguard independent choice of personal information subject (Annex C); and a model explaining how to draft a Personal information protection policy (Annex D).¹²⁰

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

While this might sound peculiar to Western observers, generally suspicious of Chinese data protection practices, it is important to remind that, since the introduction of the CSL, consent has acquired an increasingly important role in the Chinese data architecture and has been further specified by several norms. Notably, Article 25 of the Personal Information Security Specification mentions that the personal information processor cannot disclose the information of an individual without their consent and in consonance with laws and administrative regulations.¹²¹ Article 26 stipulates how image capturing can be used only for public security and, whenever this type of surveillance technology is used for any other purpose, the individual's consent must be obtained.¹²² Article 27 stipulates that when processing individuals' personal information can have an adverse impact on their interests and rights, the same cannot be done without their consent.¹²³ Further, under Article 29, sensitive personal information – which include biometric information, health records, financial data, and any other information which if abused would infringe the dignity of individuals or cause harm to their person and property¹²⁴ – cannot be processed without the explicit consent of individuals.¹²⁵

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

¹¹⁹ Belli, Chang and Chen (n 51).

¹²⁰ Personal Information Security Specification, 2020, annex A, B, C, D.

¹²¹ Protection of Personal Information Law 2021, art 25.

¹²² Protection of Personal Information Law 2021, art 26.

¹²³ Protection of Personal Information Law 2021, art 27.

¹²⁴ Protection of Personal Information Law 2021, art 28.

¹²⁵ Protection of Personal Information Law 2021, art 29.

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

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

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

¹²⁶ See s 2.1 of this paper.

¹²⁷ See (n 8).

¹²⁸ Cybersecurity Law of China, 2017, art 28.

¹²⁹ See Leplay (n 36).

¹³⁰ Lorena Abbas da Silva, Bruna Diniz Franqueira and Ivar A. Hartmann, ‘What the Eyes don’t See, the Cameras Monitor’ (2021) 8(1) *Digital Journal of Administrative Law* 171, 204.

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

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

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

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

¹³¹ Personal Information Protection Law 2021, art 73.

¹³² Personal Information Protection Law 2021, art 34.

¹³³ Personal Information Protection Law 2021, arts 35 and 18.

¹³⁴ Personal Information Protection Law 2021, art 37.

¹³⁵ Personal Information Protection Law 2021, art 61.

¹³⁶ Constitution of the People’s Republic of China 1982, art 40.

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

i. Data Security with Chinese Characteristics

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

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

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

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

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

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

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

Hence the Data Security Law can be seen as an extension of the Cybersecurity Law of 2017, which provided far-reaching mechanisms for data protection and cybersecurity in the country. Indeed, for the Chinese State, cybersecurity is an essential facet of national security¹⁴⁴ and the introduction of the Data Security Law can be deemed as one of the most relevant elements of the new data architecture of China. The Law is based on the Chinese conceptualisation of information security, which is deemed as an essential tool to preserve and guarantee the stability and sustainability of the Chinese State, Communist Party, and nation.

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

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

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

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

¹⁴⁴ See Jiang (n 38) 183-226.

¹⁴⁵ *ibid.*

¹⁴⁶ *ibid.*

¹⁴⁷ *ibid.*

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

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

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

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

¹⁴⁸ *ibid.*

¹⁴⁹ Data Security Law 2021, art 1.

¹⁵⁰ Data Security Law 2021, art 2.

¹⁵¹ Data Security Law 2021, art 4.

¹⁵² Data Security Law 2021, art 5.

¹⁵³ Data Security Law 2021, art 6.

¹⁵⁴ Data Security Law 2021, art 10.

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

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

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

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

¹⁵⁵ Data Security Law 2021, art 12.

¹⁵⁶ Data Security Law 2021, art 17.

¹⁵⁷ Data Security Law 2021, art 18.

¹⁵⁸ See (n 108).

¹⁵⁹ Data Security Law 2021, art 21.

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

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

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

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

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

¹⁶⁰ Data Security Law 2021, art 23.

¹⁶¹ Data Security Law 2021, art 24.

¹⁶² Data Security Law 2021, art 26.

¹⁶³ Data Security Law 2021, art 29.

¹⁶⁴ Data Security Law 2021, art 30.

¹⁶⁵ Data Security Law 2021, art 32.

¹⁶⁶ Data Security Law 2021, art 35.

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

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

C. India

The current Indian data protection framework is primarily shaped by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ('SPDI Rules') notified under the Information Technology Act, 2000 ('IT Act'), together with the sectorial laws mentioned in section 1.¹⁷³ The Data Protection Rules impose certain obligations and compliance requirements on organisations that collect, process, store and transfer sensitive personal data or information of

¹⁶⁷ Data Security Law 2021, art 38.

¹⁶⁸ Data Security Law 2021, art 40.

¹⁶⁹ Data Security Law 2021, art 42.

¹⁷⁰ Data Security Law 2021, art 49.

¹⁷¹ Data Security Law 2021, art 50.

¹⁷² Data Security Law 2021, art 52.

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

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

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

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

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

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

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

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

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

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

¹⁷⁴ See Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

¹⁷⁵ See SPDI Rules 2011, r 5(7).

¹⁷⁶ *ibid.*

¹⁷⁷ *ibid.*

¹⁷⁸ See SPDI Rules, 2011, r 5(6).

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

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

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

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

¹⁷⁹ See s 2.2.

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

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

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

¹⁸³ *ibid.*

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

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

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

¹⁸⁵ Personal Data Protection Bill 2021, s 14; Digital Personal Data Protection Bill 2021, s 8(8).

¹⁸⁶ Personal Data Protection Bill 2021, s 5(a)

¹⁸⁷ Personal Data Protection Bill 2021, s 5(b).

¹⁸⁸ Personal Data Protection Bill 2021, s 6.

¹⁸⁹ Personal Data Protection Bill 2021, s 7.

¹⁹⁰ Personal Data Protection Bill 2021, s 8.

¹⁹¹ Personal Data Protection Bill 2021, s 9.

¹⁹² Personal Data Protection Bill 2021, s 10.

¹⁹³ Personal Data Protection Bill 2021, s 11.

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

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

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

¹⁹⁴ Digital Personal Data Protection Bill 2022, s 4(1).

¹⁹⁵ Digital Personal Data Protection Bill 2022, s 4(2).

¹⁹⁶ Digital Personal Data Protection Bill 2022, s 4(3).

¹⁹⁷ Personal Data Protection Bill 2021, s 2(d).

¹⁹⁸ Digital Personal Data Protection Bill 2022, s 18(2).

¹⁹⁹ Belli and Doneda, ‘Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence’ (n 6).

ii. The Data Empowerment and Protection Architecture

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

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

Importantly DEPA needs to be considered in the context of the Digital India programme²⁰¹, launched by the Indian Government in 2015, to foster a radical digital transformation of the country. The three main pillars of Digital India are connectivity, eGovernment, and the establishment of a Digital Public Infrastructure. This last pillar is fundamental to understand DEPA as well as the Indian government vision consisting in the development of technology to implement regulation. Indeed, the Digital Public Infrastructure is a set of Application Programming Interfaces (APIs)²⁰² commonly referred to as the 'Indian Stack'²⁰³ which the Indian Government sees

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

²⁰⁰ See NITI Aayog (n 82).

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

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

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

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

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

It is important to clarify how users concretely express consent with DEPA. The Account Aggregator (AA) framework is a consent manager for financial data. A consent manager²⁰⁷ may exist for a variety of data, like health or telecom. This is the real institutional innovation that India has come up with. These fiduciaries exist in the Indian technical and legal ecosystem today, where the user may discover where their data resides. Data are stored in a decentralised manner and the identity behind it is also federated, with no unique ID creation unless the user decides to collate data and create one.

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

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

²⁰⁵ See NITI Aayog (n 82) 26-27.

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

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

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

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

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

III. CONCLUSION: THE EMERGENCE OF A POST-WESTERN MODEL OF DATA GOVERNANCE

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

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

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

It is important to reiterate that, in light of their relevance, these countries are likely to become not only regional but global leaders in data regulation, and their national innovations may become core elements of what could be defined as new post-Western approach to data governance. This represents a credible alternative to the traditional dichotomy between a minimalist US approach and maximalist EU approach. As argued in the introduction of this paper, the US approach suffer from an excessively laissez-faire approach, which has led an increasingly absolute majority of countries (currently 145 countries²⁰⁹) to adopt data protection laws de facto preferring a European approach based on comprehensive regulation. However, the European approach is not exempt from criticism, giving rise to a particularly complex and burdensome compliance, while simultaneously failing to tackle major data protection and data security problems and create effective protections for individuals.

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

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

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

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

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

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

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

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

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

DESIGNING THE NARRATIVES OF PROTESTS: THE ROLE OF DESIGN IN THE PORTRAYAL OF PROTESTS ON SOCIAL MEDIA PLATFORMS IN INDIA

*Saumyaa Naidu**

ABSTRACT *In recent years, social media platforms have played a significant role in the political discourse in India. Political narratives around protests and movements have been widely seen on social media. The design of platform interfaces has also been questioned for the influence it can have on people’s behaviour online. This study examines the impact that interface design of platforms has in enabling the spread of political messaging around the anti-CAA NRC and anti-farm bill protests. Focusing on four social media platforms; Facebook, YouTube, Twitter, and Instagram, the study critically analyses the use of interface design elements such as comments, hashtags, News Feed, and Threads, in the political discourse. It further contextualises the findings to the impact on individual rights of people, and highlights the existing policy and regulatory gaps.*

<p>I. Introduction 204</p> <p>II. Literature Review 206</p> <p>III. Scope and Methodology 211</p> <p>IV. Initial Observations and Patterns in Popular Content 212</p> <p style="padding-left: 20px;">A. Top posts on the anti-CAA NRC protests. 213</p> <p style="padding-left: 20px;">B. Top posts on anti-Farm Bill protests 216</p> <p style="padding-left: 20px;">C. Insights on the nature of top posts 218</p> <p>V. Enabler in Fuelling Rage 219</p> <p style="padding-left: 20px;">A. Comments 219</p> <p style="padding-left: 20px;">B. Fake accounts and fake news 222</p> <p>VI. Tools for Propaganda 223</p> <p style="padding-left: 20px;">A. Hashtags 224</p>	<p style="padding-left: 20px;">B. Trending topics and recommendations 225</p> <p style="padding-left: 20px;">C. Political advertisements. 225</p> <p>VII. Built for Higher Engagement. 227</p> <p style="padding-left: 20px;">A. Sensational imagery and titles 227</p> <p style="padding-left: 20px;">B. News Feed. 229</p> <p style="padding-left: 20px;">C. Longer lifespan of content. . . 229</p> <p>VIII. Rewarding Quick Content Creation. 230</p> <p style="padding-left: 20px;">A. Posts 231</p> <p>IX. Ambiguity in Credibility 233</p> <p style="padding-left: 20px;">A. Verified profiles 233</p> <p style="padding-left: 20px;">B. Order and design of content . 233</p> <p>X. Impact on Rights and Connected Regulatory Gaps 234</p>
---	--

* Saumyaa works on research that critically examines the role of design in digital technology, specifically in areas such as privacy, accessibility, and digital identities. Her research interests include design studies and digital cultures. Esha Goyal, BA LLB (Hons) student at NLSIU Bengaluru provided research assistance for this article.

A. Regulations on intermediary liability	234	Annexure 3: Posts on anti-CAA NRC protests observed on Instagram	247
B. Regulatory gaps in addressing hate speech	236	Annexure 4: Posts on anti-CAA NRC protests observed on Twitter	252
C. Regulatory gaps in addressing fake news.	236	Annexure 5: Posts on anti-Farm Bill protests observed on YouTube	257
D. Transparency and accountability	237	Annexure 6: Posts on anti-Farm Bill protests observed on Facebook	260
XI. Conclusion.	238	Annexure 7: Posts on anti-Farm Bill protests observed on Instagram	265
Annexure 1: Posts on anti-CAA NRC protests observed on YouTube	240	Annexure 8: Posts on anti-Farm Bill protests observed on Twitter .	267
Annexure 2: Posts on anti-CAA NRC protests observed on Facebook	243		

I. INTRODUCTION

In the last two years, India saw several significant protests and political movements at a vast scale despite the ongoing COVID 19 pandemic.¹ Beginning with the protests against the Citizenship Amendment Act (CAA) and National Register of Citizens (NRC) and then the protests against the Farm Bills, the years 2020 and 2021 witnessed many other public protests and movements. These included the protests and reverse-migration of migrant labourers, protests by doctors and nurses, protest over the new labour laws, and protest for justice in the Hathras rape case.² There has also been an ongoing political narrative attached to many of these movements and social media has played a key role in spreading them.

Social media can be beneficial to democracy in terms of providing a platform for activists, forcing political parties to face greater accountability, and making it easier to mobilise people and organise protests.³ Even as social media platforms such as Instagram, Twitch, and Discord proved to be an

¹ 'Coronavirus Disease (COVID-19) – World Health Organisation' (World Health Organisation, 2022) <<https://www.who.int/emergencies/diseases/novel-coronavirus-2019>> accessed 21 January 2022.

² Trishna Wahengbam, 'Protests in A Pandemic: A Timeline of Protests in 2020' *EPW Engage* (2021) <<https://www.epw.in/engage/article/protests-pandemic-timeline-protests-2020>> accessed 12 December 2021; Shreya Sinha, 'Year-ender: 2020 in Protests, Riots, Scams and Scandals in India' *India Today* (16 December 2020) <<https://www.indiatoday.in/india/story/202-coronavirus-caa-protest-farmers-protest-sushant-singh-rajpoot-1749923-2020-12-16>> accessed 12 December 2021.

³ Yash Sharma, 'Social Media, Democracy and Democratisation' [2021] (*The Diplomatist*, 13 August 2021) <<https://diplomatist.com/2021/08/13/social-media-democracy-and-democratization/>> accessed 6 December 2021.

essential factor for protests for the student community,⁴ and young people across the country,⁵ a large section of the population in India still cannot access these platforms. While these platforms have allowed wider reach to political parties, their supporters, media houses, and protestors, it has also caused severe consequences for protestors. Disha Ravi⁶, for instance, was arrested for editing a protest toolkit which was shared by Swedish climate activist Greta Thunberg on Twitter in support of the anti-Farm Bill protest.⁷ The tweet led to an outpour of reactions from political leaders and Indian authorities, projecting it as interference in the country's internal affairs, deeming it a tactic to defame the country, and claiming that the toolkit was linked to a conspiracy by separaist groups.⁸ Disha was arrested by the Delhi Police soon after.

The reach and influence of social media has been studied extensively in recent years, specifically in the context of electoral campaigns. The Facebook–Cambridge Analytica data scandal⁹ in the United States in 2018, was in many ways the watershed moment in understanding the role of social media in democracy. In India too, we saw social media play a crucial role during the 2014 and 2019 elections.¹⁰ There has been detailed analysis of the resources and techniques used for political campaigns by parties on social media in India.¹¹

⁴ Nehmat Kaur, 'To Understand the CAA-NRC Protests, Open Instagram' *HuffPost India* (December 18, 2019) <https://www.huffpost.com/archive/in/entry/caa-nrc-protest-instagram_in_5df9ce8be4b08083dc5b74cc> accessed 17 December 2021.

⁵ Shephali Bhatt, 'India's Farmer Protests go Global on Twitch, Discord' *The Economic Times* (Mumbai, 11 February 2021) <<https://economictimes.indiatimes.com/tech/technology/indias-farmer-protests-go-global-on-twitch-discord/articleshow/80814303.cms?from=mdr>> accessed 17 December 2021.

⁶ 'Disha Ravi: India Activist Arrest Decried as 'Attack on Democracy' *BBC News* (15 February 2021) <<https://www.bbc.com/news/world-asia-india-56066478>> accessed 5 January 2022.

⁷ *ibid.*

⁸ 'How Greta Thunberg's "Toolkit" Tweet Set India Abuzz' *Deccan Herald* (16 February 2021) <<https://www.deccanherald.com/national/how-greta-thunbergs-toolkit-tweet-set-india-abuzz-951755.html>> accessed 10 January 2022.

⁹ Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (17 March 2018) <<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>> accessed 19 February 2022.

¹⁰ Rishi Iyengar, 'In India's Last Election, Social Media was used as a Tool. This Time it Could become a Weapon' *CNN Business* (New Delhi, 13 March 2019) <<https://edition.cnn.com/2019/03/11/tech/india-election-whatsapp-twitter-facebook/index.html>> accessed 9 January 2022.

¹¹ Dr Sangeeta Mahapatra and Dr Johannes Plagemann, 'Polarisation and Politicisation: The Social Media Strategies of Indian Political Parties' (*German Institute for Global and Area Studies*, 2019) <<https://www.giga-hamburg.de/en/publications/giga-focus/polarisation-politicisation-social-media-strategies-indian-political-parties>> accessed 9 January 2022.

The interface design of social media platforms has been examined and critiqued¹² extensively as well for tricks that websites and apps use to manipulate people into making decisions they do not intend to.¹³ These manipulative features ingrained in the social media platforms are deeply connected to the creation of desired political narratives around protests and movements. This article explores these connections between the interface design of social media platforms and political messaging during protests. It also aims to study the impact of these connections on individual rights such as freedom of expression. The article argues that a range of interface design elements such as comments, hashtags, Threads, and emojis can enable the spread of political propaganda. The scope of the term interface design in this study includes visual layout, structure, and processes involved in a platform. It also comprises visual design of elements and the strategy behind the various features or interactions. The research demonstrates that the design of features such as comments contributes to rage online. Hashtags, trending topics, and political advertising enable targeted amplification of political messaging. Media platforms use sensational imagery and algorithmic features to increase the engagement and reach of content. Social media platforms reward quick content creation through posts and reactions. Lastly, they create a false sense of credibility using verified profiles, and the order and design of content. These lead to the increased spread of hate speech and misinformation on social media platforms.

II. LITERATURE REVIEW

The study includes a detailed literature review of the relevant subject areas. This consists of the overarching field of design and democracy and the impact of social media on democracy. The literature discusses the absence of questioning design activities in the present design discourse. Design is seen as a potentially critical response to capitalism, wherein designers must create products that interact with the sociotechnical challenges.¹⁴ Design is also believed to be capable of improving the quality of the democratic institutions and procedures. There is emphasis on the growing need for design

¹² Arielle Pardes, 'How Facebook and other Sites Manipulate Your Privacy Choices' *Wired* (2020) <<https://www.wired.com/story/facebook-social-media-privacy-dark-patterns/>> accessed 10 December 2021.

¹³ Arushi Jaiswal, 'Dark Patterns in UX: How Designers Should be Responsible for their Actions' (*Medium*, 15 August 2018) <<https://uxdesign.cc/dark-patterns-in-ux-design-7009a83b233c>> accessed 15 December 2021.

¹⁴ Gui Bonsiepe, 'Design and Democracy' (2006) 22(2) *Design Issues* 27.

capabilities to generate new instruments for social transformation.¹⁵ The impact of social media has also been thoroughly examined in relation to democracy. Social media is beneficial in democracy as it provides a platform for activists. On the other hand, it can prove to be detrimental to democracy when authoritarian states use it to control information or to spread misinformation.¹⁶ Another disadvantage of social media is the creation of echo chambers which leads to increased political polarisation.^{17,18} Extreme groups can use social media to disseminate hate messages to their members and distribute propaganda to recruit new members.¹⁹

In the Indian context, studies highlight the routine use of hate speech and extreme speech in online political communication and participation. There is a prevalence of fearmongering and the politics of hate being propagated. Political parties and their proxies are also found to share large amounts of fake news and misinformation.²⁰ Social media could be used to deepen divisions, particularly through misinformation around the elections, and trigger violence.²¹ The affordances of platforms in the dissemination of information, including hate speech, were closely studied in the context of political discourses in India.²²

¹⁵ Victor Margolin, 'Design and Democracy in a Troubled World' (Carnegie Mellon University, 2012) <<http://democracy-design.designpolicy.eu/wp-content/uploads/2017/05/Design-and-Democracy-in-a-Troubled-World-.pdf>> accessed 28 September 2022.

¹⁶ Sharma (n 3); Charles Koch Foundation 'How does Social Media Impact Democracy?' (*Charles Koch Foundation*, 3 March 2021) <<https://charleskochfoundation.org/stories/how-does-social-media-impact-democracy/>> accessed 5 December 2021.

¹⁷ Cass R Sunstein, 'A Prison of Our own Design: Divided Democracy in the Age of Social Media' (*Democratic Audit UK*, 3 April 2017) <<https://www.democraticaudit.com/2017/04/03/a-prison-of-our-own-design-divided-democracy-in-the-age-of-social-media/>> accessed 5 December 2021.

¹⁸ Samidh Chakrabarti, 'Hard Questions: What Effect Does Social Media have on Democracy?' (*Meta*, 22 January 2018) <<https://about.fb.com/news/2018/01/effect-social-media-democracy/>> accessed 5 December 2021.

¹⁹ Bolane Olaniran and Indi Williams, 'Social Media Effects: Hijacking Democracy and Civility in Civic Engagement' (2020) *Platforms, Protests, and the Challenge of Networked Democracy* 77.

²⁰ Anuradha Rao, 'How did Social Media Impact India's 2019 General Election?' *EPW Engage* (27 December 2019) <<https://www.epw.in/engage/article/how-did-social-media-impact-india-2019-general-election>> accessed 10 December 2021.

²¹ Iyengar (n 10).

²² Anmol Panda, Sunandan Chakraborty, Noopur Raval, Han Zhang, Mugdha Mohapatra, Syeda Zainab Akbar, and Joyjeet Pal, 'Affording Extremes: Incivility, Social Media and Democracy in the Indian Context' (17 June 2020) 1-12 *ICTD2020: Proceedings of the 2020 International Conference on Information and Communication Technologies and Development* <<https://doi.org/10.1145/3392561.3394637>> <https://dl.acm.org/doi/pdf/10.1145/3392561.3394637?casa_token=HJyzDI2mJ9EAAAAA:E057J8igknyPgh-2R2bSfQN3zbleytD3P-C5ateKj3f8UD0iHRAWblWUH0vPGMnR0HAsddXdVO4k> accessed 10 December 2021.

The study further examines the use of social media in election campaigns in India.²³ The use of political advertising on social media has increased dramatically since the elections in 2014.²⁴ There was a visible shift in the 2014 electioneering strategy, with the use of data and digital platforms occupying a central role.²⁵ However, the slow growth of internet penetration and a lower relative degree of digital literacy are still a hindrance in enabling a democratic discourse with pluralistic views on social media platforms.²⁶ The existing guidelines issued by the Election Commission concerning the use of social media in election campaigning includes pre-certification of political ads on social media and transparency on expenditure on social media advertisements.²⁷ Based on a voluntary code of ethics, platforms have identified what constitutes political content and/or advertising in the articulation of their political content policies.²⁸ There is also the emergence of WhatsApp as a platform politicians prefer due to its tremendous reach that goes beyond a party's voter base, and also because of the lack of gatekeepers.²⁹ Political content on these platforms influences perceptions by drowning out criticism

²³ Sahana Udupa, Shriram Venkatraman, & Aasim Khan, "Millennial India": Global Digital Politics in Context' (2020) 21(4) Television & New Media 343.

²⁴ Anumeha Chaturvedi, 'BJP Top Spender on Political Ads on Digital Platforms' *The Economic Times* (New Delhi, May 16, 2019) <<https://economictimes.indiatimes.com/news/elections/lok-sabha/india/bjp-top-spender-on-political-ads-on-digital-platforms/articleshow/69351792.cms?from=mdr>> accessed 10 December 2021; Ajinkya B Metkar and Aakash Aade, 'Role of Social Media in Political Management in India' (SSRN Papers, 29 June 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3637843> accessed 10 December 2021.

²⁵ Varoon Bhashyakarla, 'India: Digital Platforms, Technologies and Data in the 2014 and 2019 Elections' (Our Data Ourselves: Tactical Tech, 24 August 2018); <<https://ourdataourselves.tacticaltech.org/posts/overview-india/>> accessed 10 December 2021 'During 2019 campaign, Modi used Twitter to Reach out to Urban Middle Class, Party Cadre: Study' *The Hindu Business Line* (Washington, 10 September 2021) <<https://www.thehindubusinessline.com/news/during-2019-campaign-modi-used-twitter-to-reach-out-to-urban-middle-class-party-cadre-study/article36395866.ece>> accessed 11 December 2021; Mahapatra and Plagemann (n 11).

²⁶ Syed SKazi, Mandira Narain and Kaustuv Kanti Bandyopadhyay, 'Social Media Influence on Electoral Democracy: A Perspective from India' (*Asia Democracy Research Network*, 2020) <https://www.pria.org/knowledge_resource/1610948356_Social%20Media_ADRN_Special%20Report%20-%20India%20Chapter%20by%20PRIA%20and%20DEF.pdf> accessed 10 December 2021.

²⁷ Jinala Sanghvi, 'Role of Social Media in Indian Politics' (*Legal Desire*, 2021) <<https://legaldesire.com/role-of-social-media-in-indian-politics/>> accessed 11 December 2021.

²⁸ Gunjan Chawla and Nidhi Singh, 'Election Advertising on Social Media Platforms' (*The Leaflet*, 7 April 2019) <<https://www.theleaflet.in/election-advertising-on-social-media-platforms/>> accessed 11 December 2021.

²⁹ Vasudha Venugopal, 'Taliban Dominates BJP's Social Media Campaign in Uttar Pradesh' *The Economic Times* (11 September, 2021) <https://economictimes.indiatimes.com/news/elections/assembly-elections/uttar-pradesh/taliban-dominates-bjps-social-media-campaign-in-up/articleshow/86102596.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> accessed 11 December 2021.

with only positive narratives around a party, or by spreading disinformation based on personal beliefs of people.³⁰

Narrowing down to protests and political messaging around it, the literature focuses on the coverage of protests on social media in India. The farmers' protests received widespread attention at a global level.³¹ In the wake of the farmers' protests, the Indian government introduced stricter rules for social media platforms.³² The Uttarakhand government also issued a warning stating that posting content that is considered 'anti-national' on social media will lead to withholding of police verification for passports.³³ The Indian government asked Twitter to block more than 500 accounts belonging to Indian activists, opposition politicians, and media, which Twitter later reinstated. This led to the government further issuing a non-compliance notice to the company.³⁴ During the anti-CAA NRC protests, politicians and supporters used social media to gather support for the laws.³⁵

Lastly, the study looks at the interface design of social media platforms and the manipulative patterns they employ. Studies talk about the customisation of the Facebook News Feed, and the use of personal data by its algorithm to achieve higher engagement with the platform.³⁶ Designing better

³⁰ Jelvin Jose, 'The Politicization of Social Media in India' (*South Asian Voices*, 13 July 2021) <<https://southasianvoices.org/the-politicization-of-social-media-in-india/>> accessed 11 December 2021.

³¹ Pheroze L Vincent, 'Non-profit Uncovers Social Media Plot to Malign Farmers' Protest' *The Telegraph* (New Delhi, 21 March 2022) <<https://www.telegraphindia.com/india/british-non-profit-uncovers-social-media-plot-to-malign-farmers-protest/cid/1840498>> accessed 14 December 2021.

³² James Oaten and Som Patidar, 'India Unveils Tougher Rules for Social Media such as Facebook, Twitter and WhatsApp' *ABC News* (25 February 2021) <<https://www.abc.net.au/news/2021-02-26/india-unveils-tougher-rules-for-social-media-facebook-twitter/13194452>> accessed 14 December 2021.

³³ DNA Webdesk, 'Participating in Violent Protests, and Social Media Posts will have Dire Consequences in these States– Details Inside' *DNA* (4 February 2021) <<https://www.dnaindia.com/india/report-participating-in-violent-protests-and-social-media-posts-will-have-dire-consequences-in-these-states-details-inside-2873118>> accessed 14 December 2021.

³⁴ Lauren Frayer and Shannon Bond, 'Twitter In Standoff With India's Government Over Free Speech and Local Law' *NPR* (18 February, 2021) <<https://www.npr.org/2021/02/17/968641246/twitter-in-standoff-with-indias-government-over-free-speech-and-local-law>> accessed 14 December 2021.

³⁵ Buddhadeb Halder, 'How the BJP Tried to Manipulate Public Opinion on Social Media in Favour of the CAA' *The Wire* (17 December 2020) <<https://thewire.in/politics/how-bjp-tried-manipulate-public-opinion-social-media-favour-caa>> accessed 14 December 2021.

³⁶ Stephanie Hankey, Julianne Kerr Morrison and Ravi Naik, 'Data and Democracy in the Digital Age' (*The Constitution Society*, 2018) <<https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf>> accessed 4 December 2021; April Doss, 'How Social Media's Use of Personal Data Affects Democracy' (*IAPP*, 29 September 2020) <<https://>

social media platforms could entail providing people with control of their own algorithmic content, and flagging and filtering negative content.³⁷ Over the years, the platforms have been redesigned to introduce new features and interfaces with the aim of higher reach and engagement, which has benefited marketers.³⁸ Much emphasis is placed on the usability, learnability, efficiency, and responsiveness of the platforms while designing their user experience.³⁹ There have also been design attempts for forming communities and increasing privacy, but the enabling of online outrage and hostility has been more prominent.⁴⁰ Political parties are also gradually attempting to capitalise on

iapp.org/news/a/how-social-medias-use-of-personal-data-affects-democracy/> accessed 10 December 2021..

³⁷ Tobias Rose-Stockwell, 'How to Design Better Social Media' (*Medium*, 13 April 2018) <<https://medium.com/s/story/how-to-fix-what-social-media-has-broken-cb0b2737128>> accessed 5 December 2021.

³⁸ Jonathan Haidt and Tobias Rose-Stockwell, 'The Dark Psychology of Social Networks' *The Atlantic* (December 2019) <<https://www.theatlantic.com/magazine/archive/2019/12/social-media-democracy/600763/>> accessed 4 December 2021; 'Breaking News: Twitter's New User Interface and What it Means to You' (*Forrester*, 14 September 2010) <https://www.forrester.com/blogs/10-09-14-breaking_news_twitthers_new_user_interface_and_what_it_means_to_you/> accessed 16 December 2021.

Adolfo Ramírez Corona, 'A Bad UI that has Good UX' (UX Collective on Medium, 21 January 2020) <<https://uxdesign.cc/a-bad-ui-that-has-good-ux-4cd5d9ea4796>> accessed 16 December 2021; José Van Dijck, 'Tracing Twitter – The Rise of a Microblogging Platform' (2011) 7(3) *International Journal of Media and Cultural Politics* 333; Kshipra Sharma, 'The Powerful Interaction Design of Instagram Stories' (*UX Collective on Medium*, 10 December 2019) <<https://uxdesign.cc/the-powerful-interaction-design-of-instagram-stories-47cdeb30e5b6>> accessed 16 December 2021; Anders Olof Larsson, 'Thumbs up, Thumbs Down? Likes and Dislikes as Popularity Drivers of Political YouTube Videos' (August 2018) 23, 8 - 6 *First Monday* <<http://dx.doi.org/10.5210/fm.v23i8.8318>><<https://firstmonday.org/ojs/index.php/fm/article/view/8318/7553>> accessed 20 December 2021.

³⁹ Vandita Grover, '5 User Experience Design Lessons from Facebook, Twitter, & LinkedIn's User Interface' (*Toolbox*, 16 December 2021) <<https://www.toolbox.com/marketing/content-marketing/articles/5-ux-lessons-from-the-ui-of-facebook-twitter-and-linkedin/>> accessed 16 December 2021.

⁴⁰ Arielle Pardes, 'The Inside Story of Twitter's New Redesign' *Wired* (15 July 2019) <<https://www.wired.com/story/twitter-website-redesign/>> accessed 16 December 2021; Michael James Walsh and Stephanie Alice Baker, 'Twitter's Design Stokes Hostility and Controversy. Here's Why, and how it Might Change' (*The Conversation*, 30 August 2021) <<https://theconversation.com/twitthers-design-stokes-hostility-and-controversy-heres-why-and-how-it-might-change-166555>> accessed 16 December 2021; Jason Aten, 'Here are 3 Reasons Facebook's New Design Matters more than You Might Think' (*Inc.com*, 1 May 2019) <<https://www.inc.com/jason-aten/here-are-3-reasons-facebooks-new-design-matters-more-than-you-might-think.html>> accessed 16 December 2021; Jennifer Sano-Franchini, 'Designing Outrage, Programming Discord: A Critical Interface Analysis of Facebook as a Campaign Technology' (2018) 65(4) *Journal of the Society for Technical Communication* <<https://www.stc.org/techcomm/2018/11/08/designing-outrage-programming-discord-a-critical-interface-analysis-of-facebook-as-a-campaign-technology/>> accessed 16 December 2021..

platforms such as Instagram to reach younger voters, and Youtube as a participatory medium of communication in political campaigns.⁴¹

III. SCOPE AND METHODOLOGY

For the primary research, I defined the scope of this study to examine two of the largest protests that were organised in India, in the years 2020 and 2021. These are the anti-CAA NRC protests and the anti-Farm Bills protest.⁴² I then identified four social media platforms for this research based on their popularity; YouTube, Facebook, Instagram, and Twitter.⁴³ This excluded chat platforms. A critical design analysis of the platforms was conducted based on the content related to protests on them. This involved evaluating the interface design of platforms to assess the impact of design on people's behaviour. The study was anchored in the two protests and their coverage on the selected social media platforms. I identified the content related to the protests on the platforms based on its popularity. The process of identification of popular content varied based on the different platforms. While YouTube allows for filters that help to find videos based on view count and date of uploading, Facebook and Instagram do not provide such search features. The searchability on Instagram was most challenging as it does not allow people to view posts without being signed in. Top posts on Facebook and Instagram were identified by only running a search using specific hashtags. Twitter offers ways to streamline the search based on words, hashtags, time, and engagement metrics such as Likes and Retweets. These keywords and hashtags included the names by which the two protests have been referred to with and without the term 'protest'. The results gathered from using different hashtags and keywords were further filtered to select the top 10-12 posts based on the most viewed on YouTube, most Liked on Facebook, and

⁴¹ Niamh McIntyre, Pamela Duncan and David Pegg, 'Which Parties are Using Instagram Most Successfully?' *The Guardian* (29 November 2019) <<https://www.theguardian.com/politics/2019/nov/29/which-parties-are-using-instagram-most-successfully>> accessed 18 December 2021; Seerat Sohal and Harsandaldeep Kaur, 'Communicating with Voters on YouTube: Content Analysis of the Relationship between Advertisement Message Characteristics and Viewers' Responses' (2019) 44(1) *Management and Labour Studies* 17; Hendrik Heuer, Hendrik Hoch, Andreas Breiter, Yannis Theocharis, 'Auditing the Biases Enacted by YouTube for Political Topics in Germany' (21 July 2021) <<https://arxiv.org/pdf/2107.09922.pdf>> accessed 20 December 2021. .

⁴² 'Global Protest Tracker' (*Carnegie Endowment for International Peace*, 2022) <<https://carnegieendowment.org/publications/interactive/protest-tracker>> accessed 20 January 2022.

⁴³ 'India Social Media Statistics 2022 | Mobile & Internet Statistics' (*The Global Statistics*, 2022) <<https://www.theglobalstatistics.com/india-social-media-statistics/>> accessed 20 January 2022.

most Retweeted on Twitter. On Instagram, all 9 posts were considered in the search results of the two hashtags. I observed publicly available content posted in the years 2020 and 2021 across all platforms. Moreover, in order to ensure an unbiased search, the platforms were not signed into during the research, and the location where the searches were conducted were also disabled.

The interface design analysis consisted of studying various components of the platforms including its structure, strategy, and individual features such as thumbnail images, titles, comments, Likes, Shares, Views, hashtags, News Feed/Timeline, Threads, and Stories. The top videos/posts/tweets were observed for hate speech and misinformation and how they are enabled through the design features. The content was analysed in the context of the interface design of the specific platform. The research and analysis were grounded in the following key research questions:

- What are the strategies through which narratives and political messaging around protests are spread on social media?
- What are the specific design features on the platforms that influence the ways in which this content is consumed, responded to, and propagated?
- How does the narrative around protests on social media have an impact on constitutional guarantees such as free speech and democracy?

IV. INITIAL OBSERVATIONS AND PATTERNS IN POPULAR CONTENT

The anti-CAA NRC protests began in December 2019, after the enactment of the Citizenship Amendment Act (CAA) by the Government of India on 12 December 2019. The protest against the act extended to its associated proposals of the National Register of Citizens (NRC). The demonstrations began in Assam and rapidly spread to other parts of the country. The protestors opposed the act for being discriminatory against Muslim immigrants, excluding them from being able to acquire citizenship under the CAA. The anti-Farm Bills protest was started with the passing of the three Farm Laws in the Parliament of India in September 2020.⁴⁴ The agitation, led by the farmers' unions, began in Punjab and the protestors later travelled to the outskirts of Delhi and camped there for more than a year. The farmers

⁴⁴ Wahengbam (n 2).

protesting the laws criticised them for favouring corporations and being exploitative of the farmers.⁴⁵

The two protests saw the spread of extreme political narratives on social media platforms by individuals, political parties, and media outlets. On studying this content, it was observed that each social media platform presented a set of patterns in their top posts on both the protests. The keywords or hashtags used to search for the top posts produced a varying set of search results that also revealed the opposing political narratives behind the use of these hashtags. Based on the top content studied, the posts were classified into 3 main categories; supporting the laws, supporting the protests, and neutral content. These have been defined in detail in table 1 below.

Category	Definition
Supporting the laws	Content stating the benefits of the laws, using negative phrases against protestors/minorities, commending the government on the laws, questioning the legitimacy of the protests
Supporting the protests	Content highlighting the disadvantages of the laws, its impact against minorities, showing the extent of the protests and the viewpoint of protestors
Neutral	Content providing explanations of the laws and events around the protests, speaking of both the advantages and disadvantages of the laws

Table 1 - Definitions of supporting the laws and protests, and neutral stances in posts

A. Top posts on the anti-CAA NRC protests

On YouTube, the top videos under the keyword ‘CAA NRC Protests’ (see annexure 1) consisted of 5 videos by news channels on debates around the laws, and interviews with protestors.⁴⁶ But, dropping the keyword ‘protests’ from the search yielded results that contained 2 videos supporting CAA NRC and 3 that took a neutral stance on the protests, along with a number of explainer videos.⁴⁷ The most popular video was by an individual YouTuber,

⁴⁵ Express Web Desk, ‘Farmers End Year-long Protest: A Timeline of how it Unfolded’ *The Indian Express* (New Delhi, 9 December 2021) <<https://indianexpress.com/article/india/one-year-of-farm-laws-timeline-7511961/>> accessed 17 February 2022.

⁴⁶ The Wire, “‘We Don’t Want to Create Ruckus, We’re here for Our Rights’ The Wire | Shekhar Tiwari CAA Protest’ (20 December 2019) <<https://www.youtube.com/watch?v=M66MtJZSUT8>> accessed 20 December 2021.

⁴⁷ Dhruv Rathee, ‘Reality of Citizenship Bill (CAA) | Opinion by Dhruv Rathee’ (12 December 2019) <<https://www.youtube.com/watch?v=uS84V63IZUs>> accessed 20 December 2021.

RachitRojha praising the Indian Army and speaking of patriotism and religious harmony.⁴⁸

The search on Facebook was carried out using the hashtags #caanrcprotests and #caanrc. The popular posts under #caanrcprotests were by news channels and other online media groups, in support of the protest (see annexure 2).⁴⁹ Under #caanrc, 3 of the 4 posts were against the protestors and 2 of these were posted by individuals (see annexure 2). These also included posts by local language news channels in Hindi, Malayalam, and Tamil. This search also led to one of the largest Groups on Facebook supporting CAA NRC. The Group called ‘The population control act support group’⁵⁰ contains criticism of opposition party members, Islamophobic messages, calls for violence against minorities, and support for Prime Minister Narendra Modi.

The top posts on Instagram while searching through #caanrc, were also against protestors and minorities, and celebrated the ruling Bhartiya Janata Party (BJP) and Hindutva, the Hindu nationalist political ideology (see annexure 3). One of the top posts declared that the Hindus in Assam strongly support CAA NRC, as they formed the BJP government by a huge majority (see Image 1). Another image among the top posts in this search targeted Owaisi and claimed that CAA NRC would never be repealed (see Image 1). These were posted by groups promoting Hindu nationalism. The top posts under #caanrcprotests included all 9 posts in support of the protests by media publications and individuals (see Image 2).

⁴⁸ Rachit Rojha, ‘The Real Indian - CAA and NRC || Republic Day Special || Rachit Rojha || Rohit Sharma’ (25 Jan 2020) <https://www.youtube.com/watch?v=J-NlJaIaDO4&ab_channel=RachitRojha> accessed 11 January 2022.

⁴⁹ Gulbarga Live, ‘Historical Women’s Protest Against CAA & NRC in Gulbarga’ (26 December 2019) <<https://www.facebook.com/watch/?v=669164156950861>> accessed 20 December 2021.

⁵⁰ ‘जनसंख्यानियंत्रणकानूनसमर्थकग्रुप | Population Control Act Support Group’ Facebook Public Group <<https://www.facebook.com/groups/1855870747892234/posts/2095153503963956/>> accessed 20 December 2021.



Image 1 - Screenshot from Instagram search using #caanrc (accessed on January 11, 2022)⁵¹

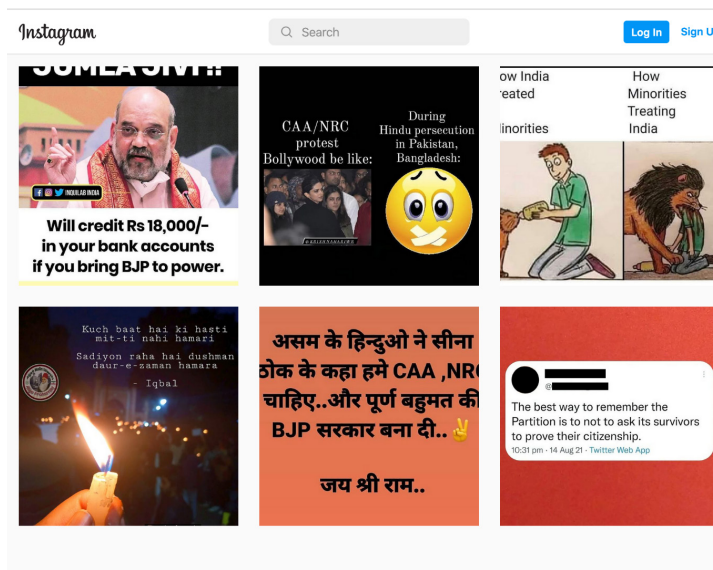


Image 2 - Screenshot from Instagram search using #caanrc (accessed on January 11, 2022)⁵²

⁵¹ Translation (left to right): “CAA, NRC will not be repealed even if your ancestors come alive from their graves, got it Asaduddin Owaisi!”.

“Bad words from Munawwar Rana! Says that if it were any other nation, PM Modi would have been hanged. Controversial Urdu poet said that CAA-NRC will face the same fate as the Farm Bill!”.

⁵² Translation: The Hindus in Assam have declared that they want CAA, NRC.. and have formed the BJP government by absolute majority.. Jai Shri Ram..”.

On searching Twitter for tweets under the categories #caanrcprotests, #caanrc, #caa, and #nrc, I found that besides the top 2 initial tweets, all others supported CAA NRC in the results (see annexure 4). 5 of the 8 popular tweets were by individual handles who belong to news agencies or political parties. Many of the tweets made by right-wing politicians and news agencies were spreading misinformation through videos, news articles, and polls (see annexure 4).

B. Top posts on anti-Farm Bill protests

The most popular video for ‘Farmers Protest’ on YouTube was a Punjabi music video called *Kisaan Anthem*⁵³ created by singer and lyricist Shree Brar. The song is a collaboration between multiple artists in support of the farmers’ protest. The other top 2 videos that follow were explainers for the Farm Bill in Hindi (see annexure 5). These explainer videos take a neutral standpoint on the Bill.⁵⁴ Both top videos under the keyword ‘Farmers Protest’, were in support of the protestors. Under the keywords ‘Farm Laws’/ ‘Farm Bill’, there were 2 explainer videos, and 2 videos against the protestors among the top content. On conducting a search with the term ‘Khalistani’, news reports associating the protest with the Khalistani movement were the most popular (see annexure 5).

On Facebook, the search with hashtag #farmersprotests yielded top posts such as videos and images of farmers’ victory march,⁵⁵ and of those who died in the protests.⁵⁶ Many reports by Punjabi news channels along with posts from the Farmers Union groups, and opposition party leaders made for the other top posts (see annexure 6). Going further into the search results, videos and posts by unofficial political party groups and news channels showed messaging against protestors, calling them divisive and violent (see annexure 6). The hashtag #farmlaws led to more news about the repeal of the

⁵³ Shree Brar, ‘Kisaan Anthem | Mankirtl Nishawnl Jass | Jordanl Fazilpurial Dilpreetl Flowl Shreel AfsanalBobby’ (8 December 2020) <https://www.youtube.com/watch?v=oNjiVuPmh9A&ab_channel=ShreeBrar> accessed 20 December 2021.

⁵⁴ A neutral standpoint here is being referred to as an objective explanation of the Bill along with both its advantages and disadvantages. However, many explainer videos are influenced by the political perspectives of the speaker.

⁵⁵ Mandeep Sandhu, Translation: Many will die, Night at sambhu border, Those hearts that beat and suffer for the community, That’s why the government is jealous!, (14 December 2021) <<https://www.facebook.com/groups/839843826572746/posts/1013902549166872/>> accessed 11 January 2022.

⁵⁶ Harish Meena, ‘या तो सच्चे किसान बनो या सच्चे गुलाम क्योंकि शुद्धता की ही कीमत और इज़्जत होती है।’ Translation: Either become a true farmer or a true slave because purity has value and respect (11 January 2022) <<https://www.facebook.com/groups/154509932659108/posts/504135841029847/>> accessed 11 January 2022.

Bill in recent searches. As noted in YouTube, severe criticism of the protest was seen under the hashtag #Khalistani. The narrative propagated in these posts attempted to prove that the repeal of the Bill is a step towards destroying Khalistani ambitions (see annexure 6). One of the top posts accused Disha Ravi of spreading lies about the government and being associated with Khalistani groups. Posts by news channels claimed to share evidence of Khalistani groups causing violence during the Republic Day demonstrations (see annexure 6). These posts use visuals such as images of the Indian flag to emphasise the nationalist narrative. Many popular posts on Facebook were in local languages.

The hashtag #farmersprotest on Instagram showed top posts as images of Punjabi artists at the protest (see annexure 7). On exploring #farmbill, 8 of the 9 top posts were found to be against the protestors. These posts build a narrative that the repeal was done in national interest (see Images 3 and 4). The posts showed images of PM Modi and sent the message that repeal of the Bill was a gift for farmers. The Twitter search with all hashtags #farmersprotests, #farmersprotest, #farmlaws, #farmbill, and #khalistani, led to top posts with a large amount of disinformation building a narrative critical of the protests. These included videos of the Republic Day demonstration, where protestors are shown to be attacking the Delhi Police (see annexure 8). Other top tweets were in support of the farmers by many global artists and activists. 7 of the 9 top tweets contained the hashtag ‘Khalistani’, calling the protests a Khalistani operation to divide the country (see annexure 8).

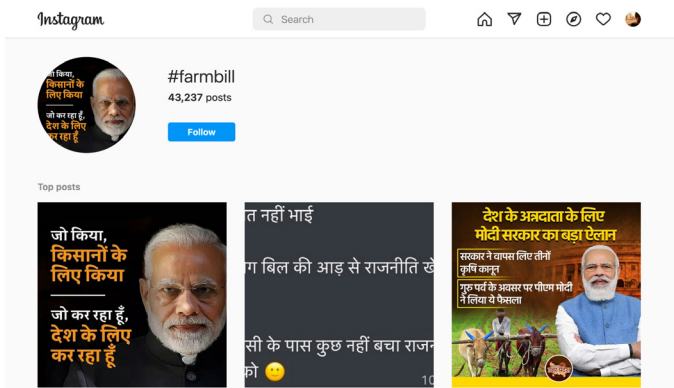


Image 3 - Screenshot from Instagram search using #farmbill (accessed on January 12, 2022)⁵⁷

⁵⁷ Translation (left to right): “Whatever I did was for the farmers, what I am doing now is for the benefit of this nation”.

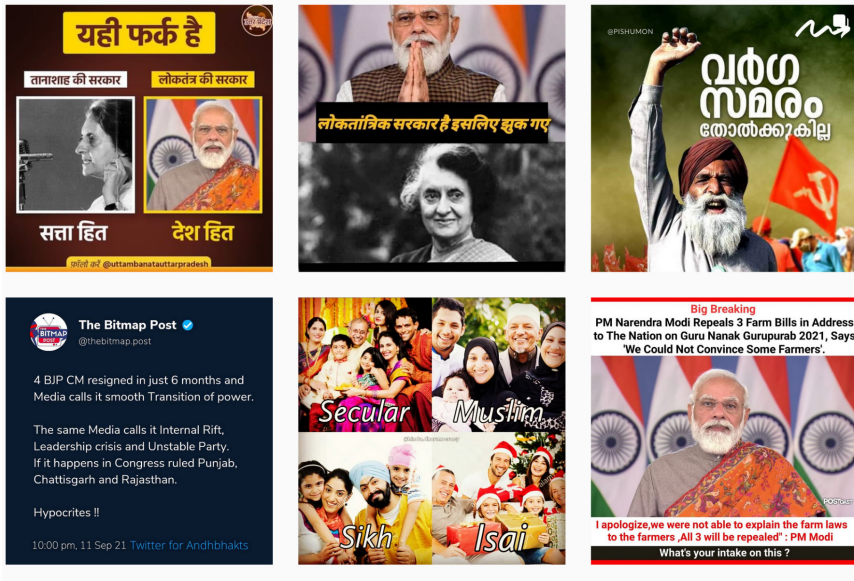


Image 4 - Screenshot from Instagram search using #farmbill (accessed on January 12, 2022)⁵⁸

C. Insights on the nature of top posts

Through this research, it was noted that the top content on Twitter, Facebook, and Instagram contained hate speech⁵⁹ against protestors and minorities, and islamophobic content. YouTube top content was noted to contain hate speech in 2 out of the 20 videos. This could be attributed to the fact that content is more difficult to create and share on YouTube when compared to creation and sharing on other platforms.⁶⁰ The platforms were also observed to contain misinformation and fake news.⁶¹ Media publications and political

“It’s alright, some people were playing political games in the garb of the Bill, now they don’t have anything left to use for political gains.”

“Modi governments’ big announcement for the country’s food provider (farmers). The government has rolled back the three farm laws. Modi took the decision on the occasion of Guru Purab (birth anniversary of the first Sikh Guru)”.

⁵⁸ Translation (top left to bottom right): “This is the difference. Dictator’s government (referring to Indira Gandhi’s image) in interest of power; Democratic government (referring to Narendra Modi’s image) in interest of the nation.”

“This is a democratic government, hence we bent (referring to the repeal of farm laws)”

“Class Struggle will not be defeated”

⁵⁹ Content containing insulting words or slurs, negative action verbs, or calls for violence are defined as hate speech here.

⁶⁰ This has been discussed further in s 8.1 of this article.

⁶¹ Fake news and misinformation was identified by cross-checking the content on fact checking platforms and media publications. Most posts and tweets had already been reported as

leaders have the strongest reach on the platforms. But many unofficial political groups and individual supporters shared posts that propagated hate speech against minorities and discredited the protestors. On Facebook, a clear pattern emerged where videos have far more engagement⁶² than images. The posts in local languages on all the platforms studied had higher reach than posts in English.

A strong visual language could be seen in the top posts spreading misinformation and islamophobic content. Images of PM Modi, Indian flag, and Indian Army were some of the recurring images in these posts. Many individual posts criticising the protests or supporting the laws used images with saffron background over which text would be displayed (see Images 10 and 11). The commonly used emojis in these posts were Indian flag, red flags, and ‘om’ emojis. The research demonstrated that this consistent visual language through images, colours, and emojis across social media platforms, was being used by groups and individuals supporting the Hindu nationalist sentiment.

V. ENABLER IN FUELLING RAGE

Social media platforms have been observed to thrive on spreading anger and violence among its users.⁶³ Many interface design elements contribute to this characteristic. This section draws from the research to examine how some of these elements are used to promote rage and hostility on social media.

A. Comments

Comments are highly revealing of violence on platforms. They are, in many instances, used by people to make personal attacks, make threats, and share hate speech. On Facebook, the comment function over time has been expanded to include visual responses such as emojis, images, GIFs, and stickers. Jennifer Sano-Franchini, in her article, “Designing Outrage, Programming Discord: A Critical Interface Analysis of Facebook as a

fake news by media publications.

⁶² Engagement on different platforms was measured based on their respective indicators. The view count was seen as an indicator of engagement on YouTube. On Facebook and Instagram, the number of Likes was used as a measurement of engagement. The number of Likes and/or Retweets was used to measure engagement on Twitter. On Facebook, engagement on videos were measured using view count. The number of comments and varying reactions were not counted as part of measuring engagement.

⁶³ Bill Hathaway, “Likes” and “Shares” Teach People to Express More Outrage Online’ *Yale News* (13 August 2021) <<https://news.yale.edu/2021/08/13/likes-and-shares-teach-people-express-more-outrage-online>> accessed 22 February 2022.

Campaign Technology”, speaks about how these responses make it easier for people to add quick comments with minimal effort, without taking the time to reflect on the subject, which can contribute to political polarisation and discord.⁶⁴ Comments on political issues can rapidly take the form of hate speech and can result in inciting violence against minorities and vulnerable communities.

An example of hate speech was noted in the research when one of the popular videos on Facebook of a standup comedy performance by Rehman Khan had been criticised for its stance on the anti-CAA NRC protests and the repercussions for Muslims in India (see Image 5). The top comments have numerous Islamophobic responses. The posts on Facebook supporting CAA NRC also have many angry comments calling minorities and protestors anti-nationals. The top 10 posts studied on Facebook contained 20 comments in their top 10 comments which consisted of hate speech and Islamophobic language. Similarly, the top 10 YouTube videos contained a total of 8 Islamophobic comments and hate speech in their top 10 comments (see annexure 1).



Image 5 - Screenshot of derogatory comments from Facebook on Rehman Khan's video⁶⁵

⁶⁴ Sano-Franchini (n 40).

⁶⁵ Translation of comments: “[Referring to a Muslim commentor] Your heroes Saddam Hussain, Osama Bin Laden, Al-Zawahiri are all your role models. When people who think

On Facebook, Sano-Franchini further highlights that presenting the comment threads in reverse-chronological order or showing the top comments, and allowing people to engage in conversations through comments with people beyond their network of Facebook friends, can encourage arguments as people who have no prior relationship are able to engage in debates on deeply personal and polarising political issues.⁶⁶ Interactions with comments in the form of Likes, Dislikes, and Replies also pushes enraged responses.

It is fundamentally in the interest of the platform to keep people angry. The News Feed on Facebook is informed largely by the platform algorithms' assessment of the person, their interests, and content that will keep them engaged. This usually translates to keeping people fearful or enraged online.⁶⁷ Two Facebook whistle-blowers, Frances Haugen and Sophie Zhang have both claimed that the company harms and undermines democracy in pursuit of growth and profits.^{68, 69} Facebook's former executive, Tim Kendal testified before the Congressional House Consumer Protection and Commerce Subcommittee in the United States, that they designed the platform to be addictive as maximising user engagement would result in higher profits for the company. Kendal stated that to this end, Facebook promotes shocking images, graphic videos, and headlines that incite outrage. Further, using the data on people's engagement with the platform, Facebook is able to direct specific audiences towards provocative content. The platforms' algorithm maximises people's attention by provoking, shocking, and enraging them with content. The platform hence incentivises harmful behaviours for profitability and prioritises sensationalism, fear, and outrage over substance or enrichment in order to keep people on the site.⁷⁰ These hostile comments and interactions with them propagate hate towards minorities and make them vulnerable to further discrimination and violence. The unchecked

of the nation came [into power] your community has a problem.”

“[Referring to a Muslim commentator] Have you studied in a Madrasa?...[You] should have either learnt English or written in Hindi. [I] could not understand what you have written.”

“[Referring to a Muslim commentator] You are not doing anything for the country yourself. Let the ones who are doing something do”

⁶⁶ Sano-Franchini (n 40).

⁶⁷ Doss (n 36).

⁶⁸ Bobby Allyn, ‘Here are 4 Key Points from the Facebook Whistleblower’s Testimony on Capitol Hill’ *NPR* (5 October 2021) <<https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress>> accessed 23 February 2022.

⁶⁹ India Today Tech, ‘FB Whistleblower Says She will Testify Before Lok Sabha if Govt Wants to Look into Facebook Practices in India’ *India Today* (New Delhi, 27 October 2021) <<https://www.indiatoday.in/technology/news/story/fb-whistleblower-says-she-will-testify-before-lok-sabha-if-govt-wants-to-look-into-facebook-practices-in-india-1869990-2021-10-27>> accessed 23 February 2022

⁷⁰ Sano-Franchini (n 41).

propagation of hate speech by platforms points to the several regulatory limitations in India regarding hate speech on social media platforms.

Hate speech remains undefined with a lack of appropriate codes or regulations for intermediaries. The provisions on hate speech under the Information Technology (IT) Act are vaguely worded, and lack consistent interpretation of the existing framework across courts.⁷¹ This has led to incidents such as the Delhi riots in February 2020 where Facebook's inaction on hate speech by Hindutva groups caused mobilisation and violence against Muslims.⁷² There has been a clear lack of accountability and transparency in the content moderation and removal practices of social media platforms in India. The proposed amendments to the Intermediary Guidelines Rules under the IT Act in 2018, later enacted in 2021, sought excessive removal of content, imposed an obligation on platforms to identify the originator of private messages, and proactively monitor communication.⁷³ These amendments have been called out for threatening free speech and privacy of citizens, while also not effectively countering hate speech on the platforms. It is therefore critical to conceptualise policies that balance free speech and privacy along with clearer laws on hate speech. The absence of a comprehensive anti-discrimination law in India adds to this regulatory gap. The existing laws do not cover the various forms of discrimination, specifically from private organisations or individuals.⁷⁴

B. Fake accounts and fake news

Twitter has also been observed to enable online violence. More abusive tweets garner more attention, and hence more followers for the account holder.⁷⁵ The platform has been reported by a study⁷⁶ to have fake social media

⁷¹ Archit Lohani, 'Countering Disinformation and Hate Speech Online: Regulation and User Behavioural Change' (ORF, 25 January 2021) Observer Research Foundation <<https://www.orfonline.org/research/countering-disinformation-and-hate-speech-online/>> accessed 3 March 2022.

⁷² Shweta Desai, 'The Hateful Facebook Adventures of Ragini Tiwari & Friends' (*Article 14*, 6 October 2020) <<https://www.article-14.com/post/the-hateful-facebook-adventures-of-ragini-tiwari-friends>> accessed 16 March 2022.

⁷³ Akriti Gaur, 'Moderate Globally Impact Locally: Tackling Social Media's Hate Speech Problem in India' (*Yale Law School*, 28 September 2020) <<https://law.yale.edu/moderate-globally-impact-locally-tackling-social-medias-hate-speech-problem-india>> accessed 16 March 2022.

⁷⁴ Tarannum Vashisht, 'The need for an Anti-discrimination Law' (iPleaders, 19 December, 2020) <<https://blog.iplayers.in/need-anti-discrimination-law/>> accessed on 21 September, 2022.

⁷⁵ Hathaway (n 63).

⁷⁶ Regina Mihindukulasuriya, 'Nearly 18,000 Twitter Accounts Spread 'Fake News' for BJP, 147 do it for Congress: Study' *The Print* (31 January, 2022) <<https://theprint.in/>

handles spreading disinformation and gathering nationalist support against perceived ‘anti-nationals’. Many verified handles of politicians and journalists have also tweeted fake videos. One such instance occurred in early 2020, when BJP IT wing head Amit Malviya posted a fake video of anti-CAA NRC protestors raising “Pakistan Zindabad” banners.⁷⁷ Such instances promote communal differences and lead to calls for violence on the platform.

Fake news can have a severe impact on democracy as it can lead to a diverse set of harms ranging from violence, damage to the electoral system, and increased political polarisation.⁷⁸

Repeated spread of fake news can gradually change people’s perception and can be used as a means to control their behaviour.⁷⁹ Social media platforms offer an ideal environment of surplus information for fake news to thrive. Platforms have initiated public awareness campaigns to counter fake news. They have also been operating on self-regulation where they moderate content using their own policies and community guidelines. However, self-regulation has been criticised by policy-makers due to the lack of transparency and accountability of social media platforms. Human rights groups and activists have also expressed scepticism against government-led policies and regulations as it could lead to arbitrary imposition of bans, content moderation, or internet shutdowns. Presently, there are no specific regulations for fake news in India. The regulatory challenge includes addressing the different types of fake news such as disinformation and misinformation. Further, the regulations must be comprehensive enough to tackle the rapid pace of social media.⁸⁰

VI. TOOLS FOR PROPAGANDA

Authoritarian regimes around the world have developed several online tools such as bots or algorithmically controlled accounts and hashtags to influence their online conversations and messaging. Many of these tools are being used by small groups with extremist ideologies in democratic societies to amplify

politics/nearly-18000-twitter-accounts-spread-fake-news-for-bjp-147-do-it-for-congress-study/356876/> accessed on 20 September, 2022.

⁷⁷ Jose (n 30).

⁷⁸ Vasudev Devadasan, “‘Fake News’ and the Constitution” (*Indian Constitutional Law and Philosophy*, 17 June 2020) <<https://indconlawphil.wordpress.com/2020/06/17/fake-news-and-the-constitution/>> accessed 16 March 2022.

⁷⁹ Fred Smith, ‘The Dangers of Fake News’ (*The Elm: University of Maryland*, 11 November 2020) <<https://elm.umaryland.edu/elm-stories/Elm-Stories-Content/The-Dangers-of-Fake-News.php>> accessed 14 March 2022

⁸⁰ Lohani (n 71).

their presence online and to make their positions seem more popular than they are.⁸¹

A. Hashtags

As noted from the top posts, the use and removal of the term ‘protest’ from hashtags changed the visible discourse entirely on platforms such as Facebook and Instagram (see annexures 2 and 3). The use of hashtags is important in understanding how content including extreme speech is spread on social media. They are one of the key tools used in political propaganda.⁸² It can be used to get higher reach, and also to analyse the larger public sentiment on a subject. During the anti-CAA NRC protests, the government changed its campaign strategy based on the mapping of the online sentiments of protestors and countered it by campaigning in support of the hashtag #IndiaSupportsCAA.⁸³

The anti-Farm Bill protests also saw a massive propaganda campaign using hashtags and fake accounts, in order to delegitimize the protests by branding the farmers as Khalistani supporters.⁸⁴ A report titled “Analysis of the #RealSikh Influence Operation”, published online by the Centre for Information Resilience (CIR), revealed a coordinated conspiracy to link the farmers to Khalistani groups through inauthentic social media posts on Twitter, Facebook, and Instagram. A network of 80 fake accounts was discovered conducting propaganda that supports the Indian government’s narrative on the farmer agitation, condemning separatism in Punjab, and glorifying the Indian army. According to the report, these accounts appear to be manually operated, with the same personas replicated over multiple platforms and repeating the same content. The hashtags used included #Khalistanis, #Real Sikhs Against Khalistan, #Sikhs Reject Khalistan and #Shame On Khalistanis.⁸⁵ The design of platforms currently does not prevent such an operation involving numerous fake accounts. There is a clear need for platforms to employ barriers that can deter fake accounts.

Hashtags have also been used by protestors in order to create an impact on social media. During the anti-Farm Bill protest, the violence during Republic Day demonstrations led to people using hashtags accusing PM Narendra Modi of genocide against farmers. The Indian government ordered Twitter to block more than 500 accounts belonging to Indian activists, opposition

⁸¹ Charles Koch Foundation (n 16).

⁸² Panda, Chakraborty, Raval, Zhang, Mohapatra, Akbar, and Pal (n 22).

⁸³ Kazi, Narain, and Bandyopadhyay (n 26).

⁸⁴ Jose (n 30).

⁸⁵ Vincent (n 31).

politicians, and media.⁸⁶ The ruling party has been accused of invoking free speech in cases of fake news and hate speech, while misusing the free speech regulations to censor online content.

B. Trending topics and recommendations

The trending news on Twitter also plays a role in forming a false narrative. Twitter's algorithm determines trending news stories based on how quickly a large number of Tweets are posted using a certain hashtag. This can be manipulated using fake accounts and hashtags, as mentioned above. These trending news stories are further reported on television and print news as well. This nature of content circulation can lead to increased ideological differences and lack of varying perspectives in the media.⁸⁷ In recent times, trending topics have been used to spread hatred against communities, impacting their rights and freedom.

Through the research, it was observed that YouTube's algorithm recommends content that matches with topics the majority is interested in, and thus specific content gets more popular.⁸⁸ In the related videos section, it was seen that the first few videos are relatively close to the protests, but the later recommendations are quite unrelated and are only based on their popularity. This has been confirmed by a 2021 study conducted to audit YouTube's recommendation system for political topics in Germany by Hendrik Heuer, Hendrik Hoch, Andreas Breiter, and Yannis Theocharis.⁸⁹ It finds that YouTube recommends increasingly popular but topically unrelated videos. YouTube's recommendation system favours popular content over politically extreme content. Thus, the top posts on YouTube are not as extreme in the case of protests as well.

C. Political advertisements

Paid advertisements are another way in which propagandists use social media for manipulating people. In December 2019, a video by Jaggi Vasudev, popularly known as Sadhguru, was posted on YouTube in support of the CAA.⁹⁰ The BJP began promoting this video in order to garner support for the CAA, amidst rising public protests against it. The video shows Vasudev asking

⁸⁶ Frayer and Bond (n 34).

⁸⁷ Kazi, Narain, and Bandyopadhyay (n 26).

⁸⁸ Heuer, Hoch, Breiter, and Theocharis (n 41).

⁸⁹ *ibid.*

⁹⁰ Sadhguru, 'CAA Protests – Sadhguru on Citizenship Amendment Act & NRC' (28 December 2019) <<https://www.youtube.com/watch?v=11RgVkJzCpY>> accessed 11 January 2022.

students to read the Act before protesting, and implying that the youths protesting in universities are irresponsible and uninformed. The video was then tweeted by PM Modi as a starter to the 'India Supports CAA' campaign. Following this, several ads using the video dubbed in Hindi, were launched on BJP's Facebook page. These Facebook ads were active from the end of December, 2019 through January 2020. This was complemented by paid ads run by other associated entities like BJP leaders, state BJP units, other fan pages run by BJP supporters, and some pro-government media houses.⁹¹ Protestors cannot match the frequency and reach of paid political ads due to lack of resources. Such a blatant use of power demonstrated that governments can easily buy their way into promoting their idea of the required laws and regulations.

Online political advertising differs from other political ads due to its ability to target specific groups based on their personal information, and the invisibility of this targeted advertising.⁹² Microtargeting of political ads on social media can polarise communities and reduce democratic public discourse.⁹³ Social media can hence be used by governments to undermine democratic values and create divisive narratives in society. In the absence of regulation, paid political ads on platforms can threaten financial transparency and accountability in the political process.⁹⁴ The lack of regulations also allows platforms undue influence over political discourse as they practise a high degree of opacity in the placement, payment, and targeting of online political ads. Hence, the regulation should be updated to include a clear legal definition of political advertising to accommodate characteristics of social media. Besides ads purchased by political parties and candidates, it should take into consideration ads that advocate for a clearly identified candidate or political party and/or are purchased by individual supporters of a political party.⁹⁵ The political financing regulations should also be updated to include these ads. Platforms should be held accountable for transparency

⁹¹ Halder (n 35).

⁹² P J George, 'Should Online Political Advertising be Regulated?' *The Hindu* (8 November 2019) <<https://www.thehindu.com/opinion/op-ed/should-online-political-advertising-be-regulated/article62108953.ece>> accessed 12 March 2022.

⁹³ Dr Judit Bayer, Dr Irini Katsirea, Dr Olga Batura, Prof Dr Bernd Holznagel, Dr Sarah Hartmann, and Katarzyna Lubianiec, 'The Fight against Disinformation and the Right to Freedom of Expression' (*European Parliament*, 2021) <[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695445/IPOL_STU\(2021\)695445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695445/IPOL_STU(2021)695445_EN.pdf)> accessed 1 March 2022.

⁹⁴ 'Regulate Online Political Ads for Greater Political Integrity' (*Transparency International*, 10 March 2021) <<https://www.transparency.org/en/news/regulate-online-political-ads-for-greater-political-integrity>> accessed 1 March 2022.

⁹⁵ Chawla and Singh (n 28).

of ads. There should be restrictions on microtargeting and use of personal data.⁹⁶

VII. BUILT FOR HIGHER ENGAGEMENT

One of the core goals of social media is to prolong people's consumption and engagement with the content online. Media outlets and political parties leverage this characteristic of platforms to get more visibility and traction. Many of the design features that favour greater engagement with the platform may not have a direct impact on the political narratives on protests, but have more subtle ways of influencing the behaviour of people consuming content online.

A. Sensational imagery and titles

The graphics and text on social media posts usually rely on sensationalisation for higher reach and engagement. Sensationalisation here refers to content that is intended to shock or provoke interest. Content that uses such language or visuals was classified as using sensationalism. It includes selectively highlighting information to get attention, which can result in the circulation of misinformation (see Image 6). Many news channels translate their television visual language to the thumbnails of their YouTube videos by using shocking images and headlines (see Image 7). This sensationalisation extends to hashtags, descriptions, and the text on thumbnails. Large, bold texts in the thumbnail serve the purpose of catching attention even when in YouTube's default view where the video occupies only a part of the desktop screen. It remains visible in the related videos on the right column as well. In many instances, the title of the post is itself repeated more dramatically on the thumbnail image or a dramatic quote from the video is presented as text on the thumbnail.

⁹⁶ Transparency International (n 94).



Image 6 - Screenshot of thumbnail image from News report on YouTube⁹⁷



Image 7 - Screenshot of thumbnail image from News report on YouTube⁹⁸

Often on YouTube videos, the number of Views are later added as text on the thumbnail images (see Image 8). The Views influence the perceived validity of the post and helps it get further momentum.

⁹⁷ Translation: “We won’t take CAA back, do whatever you can”.

⁹⁸ Translation: “..So that is how Khalistan can be created!”.

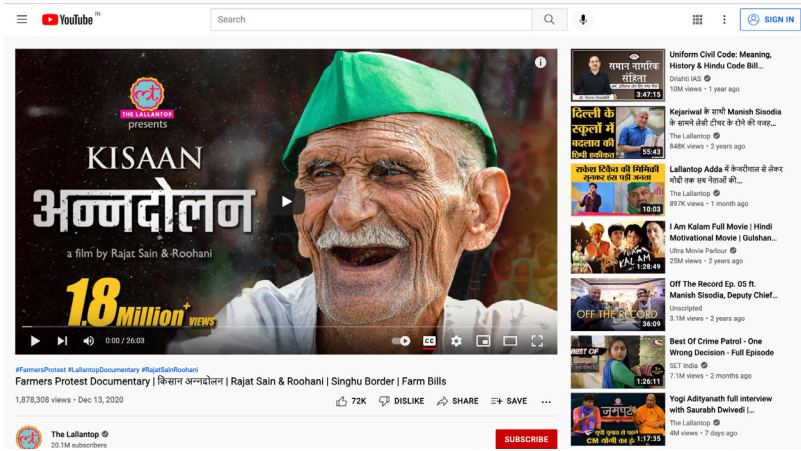


Image 8 - Screenshot of the thumbnail image of a documentary on the anti-Farm Bill protest on YouTube

B. News Feed

As discussed earlier, Facebook's algorithm shows posts on the News Feed, not chronologically but based on people's interactions with other posts. The design is aimed at higher engagement and hence more profitability for the company. The platform is designed to make people spend substantial amounts of time browsing the News Feed as the page allows infinite scrolling. The Feed appears to be reverse chronological, but the algorithm takes into account factors like with whom people are Facebook friends, their groups, their activities, their Likes, their friends' activities and likes, and the activity surrounding a post.⁹⁹ The design changes in recent years in the platform have also been motivated by profitability. Facebook's 2019 design iteration made the Groups and Events sections appear more prominent than earlier, as these are Facebook's two fastest-growing features.¹⁰⁰

C. Longer lifespan of content

All social media platforms have affordances that allow for people to increase the lifespan of their content. On Twitter, Retweet-ing the top tweets can ensure that it shows up on other people's timelines, and hence have better engagement.¹⁰¹ This occurs on Facebook when people comment or reply to a

⁹⁹ Sano-Franchini (n 40).

¹⁰⁰ Aten (n 40).

¹⁰¹ Alfred Lua, 'Can Twitter Threads Increase Reach, Engagement, and Referral Traffic? An Experiment' (*Buffer*, 6 December 2018) <<https://buffer.com/resources/twitter-thread-experiment/>> accessed 15 January 2022.

comment under a post. This was observed in various posts against protesters where a simple word like ‘yes’, the phrase ‘Jai Hind’, or just an emoji would be commented on posts which kept the engagement going (see Image 9).



Image 9 - Screenshot of comments from a pro-CAA NRC Facebook group

The higher amount of disinformation and hate speech around the protests on Twitter can also be attributed to the fact that the platform’s metrics can be gamed to elevate false content.¹⁰²

VIII. REWARDING QUICK CONTENT CREATION

Besides consumption, social media also relies heavily on creation of content. Over the years, many platforms have made their interfaces more aligned towards allowing increased posting and sharing through newer features.

¹⁰² Walsh and Baker (n 40).

A. Posts

Sano-Franchini mentions that Facebook rewards brief posts. Shorter posts can appear more prominently in larger, bolded font, and formatted with a colourful background.¹⁰³ It takes less effort to post and share content, which can lead to less responsible engagement. In the context of the protests, this means that it is easier to spread disinformation on Facebook, also aided by the frequency of posts and functioning of the network.

Instagram, primarily being an image sharing platform, also enables easy posting and sharing. The pre-designed templates of text styles and colours can be used to create emphasis in the content. Through this research, Instagram was observed to have more memes, quotes, and screenshots (see annexures 3 and 7) as these can be reshared from other platforms without creating new content on Instagram. This also demonstrates that the platform encourages visual content.

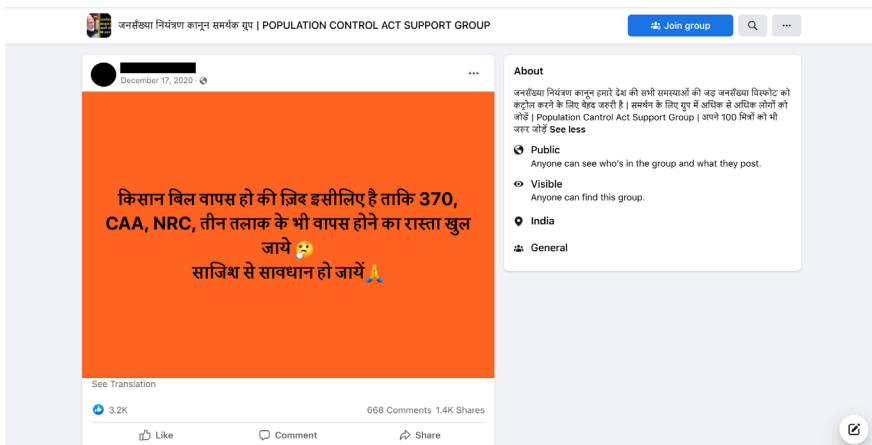


Image 10 - Screenshot of post with saffron coloured background on Facebook¹⁰⁴

¹⁰³ Sano-Franchini (n 40).

¹⁰⁴ Translation: “The demand for taking back the Farm Bill is so that the path to repeal [section] 370, CAA, NRC, and Triple Talaq [Act] also clears up. Beware of the conspiracy”.

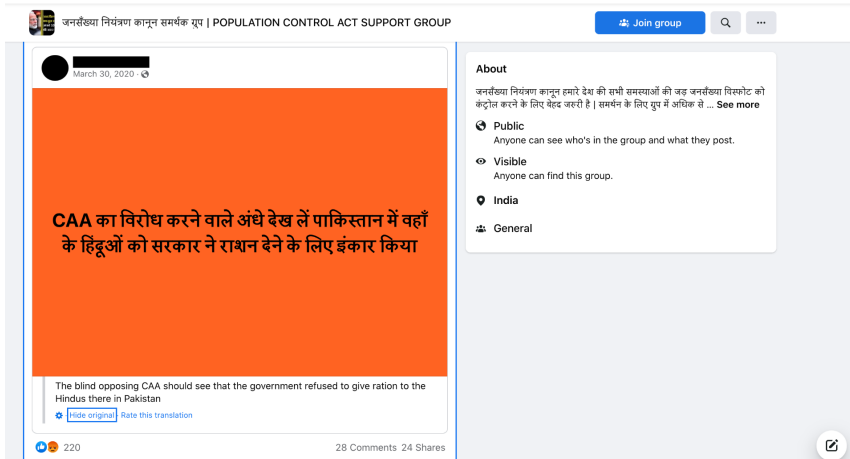


Image 11 - Screenshot of post with saffron coloured background on Facebook¹⁰⁵

Similarly, Twitter also offers faster content creation through its character limit. Other features such as Likes, Retweets, Quote Tweets, and Mentions, and the choice for people to be anonymous on the site facilitate unrestricted, brief, and impulsive conversations. In its redesign in 2017, along with the introduction of Threads, Twitter doubled the length of tweets from 140 to 280 characters. This attempt at improving conversations has not been successful for the platform.¹⁰⁶ Conversations on Twitter remain hostile as the site can be manipulated through fake accounts, Retweets, and Likes to push abusive content.

Creating and sharing content on YouTube takes a lot more effort. These nudges on the platform slow down the spread of misinformation.¹⁰⁷ While studying videos related to the keywords 'CAA NRC', I found that most videos were posted by news channels and very few were by individual YouTubers (see annexure 1). The news reports covered debates and the protest, along with speeches by politicians. The explainer videos mostly belonged to individual YouTubers who have been creating content for several years. YouTube is more aligned towards creators and requires more resources to create and share content. These resources include recording and editing equipment, which are only accessible to organisations or YouTubers with a large number

¹⁰⁵ Translation: "The people who are blindly opposing CAA should see how in Pakistan the government has refused to provide ration to Hindus."

¹⁰⁶ Walsh and Baker (n 40)

¹⁰⁷ Marcus Schultz-Bergin, 'The Primacy of the Public' (MSL Academic Endeavors | 2021) ch 4 Experimental Technology & The Principles of Engineering Ethics <<https://pressbooks.ulib.csuohio.edu/principles-of-engineering-ethics/chapter/the-principles-of-engineering-ethics/>> accessed 15 January 2022.

of subscribers. This characteristic of the platform has led to relatively less misinformation and hate speech around the protests.

IX. AMBIGUITY IN CREDIBILITY

Many interface design elements unintentionally lend to the credibility of content on social media. These could be metrics of popularity such as the number of Likes, Views, or Retweets, or the markers of authenticity such as bios and follower counts. These elements are often the source of the spread of fake news.

A. Verified profiles

Through the research, it was noted that in case of both protests, the top posts belonged to verified accounts across platforms. The purpose of verified accounts is to prove that the account is legitimately held by the person/business they claim to be. Verification is denoted by a tick mark alongside a profile. Verification also seems to be a visual marker that is somehow perceived to imply authenticity of content. Political leaders, journalists, and other well-known public figures in India with verified profiles have higher credibility, and hence higher reach. The feature allows more power and hence control to the state, media, and eventually the platform itself. Despite the claim of credibility, many of these verified accounts have been noted to post false content, which gets shared with the assumption of being accurate.¹⁰⁸ As mentioned in section 5.2, the research also shows that fake news was spread by verified accounts on Twitter on several occasions during both protests (see annexures 4 and 8). This has resulted in pushing forward the government's narrative on the proposed laws of CAA NRC and Farm Bill, while also creating mistrust against protestors. Hence, comprehensive policies to address misinformation and disinformation on social media are necessary for fair democratic processes.

B. Order and design of content

The visual design of external content on social media makes all the sources look similar. When sharing external content on Facebook, content from personal blog posts, established media houses, or a political website, all appear visually the same on social media. The formal appearance of content inspires

¹⁰⁸ Pooja Chaudhuri, 'Tarek Fatah – A case study of unrelenting divisive misinformation' (*Alt News*, 27 January 2020) <<https://www.altnews.in/tarek-fatah-a-case-study-of-unrelenting-divisive-misinformation/>> accessed 26 February 2022.

a sense of credibility, regardless of the accuracy of the information.¹⁰⁹ The order of content is also based on the algorithms of platforms that favour engagement rather than credibility or source. These design aspects enable an environment where fake news thrives.¹¹⁰

X. IMPACT ON RIGHTS AND CONNECTED REGULATORY GAPS

The design of social media platforms impacts the constitutional rights of citizens. The key harms identified have been hate speech, fake news, increased polarisation, suppression of free speech, and microtargeting using personal data. The extreme speech, polarised content, and fake news lead to interference in the electoral system, another key tenet of democracy, as they propagate false messaging among citizens. Further, the lack of consent and manipulative data practices lead to privacy concerns for people using the platforms. This is evident in the use of personal data in microtargeting political advertisements and in algorithmically determining a person's news feed on a platform. In contrast to the utopian vision of social media platforms being democratic spaces of free expression that facilitate informed public engagement, they have rapidly become associated with the propagation of racism, homophobia, and xenophobia.¹¹¹ The platforms benefit from excessive power and control due to the access to immense resources and lack of regulations for accountability.

A. Regulations on intermediary liability

Social media platforms are regulated as intermediaries, and various regulatory frameworks provide the conditions of intermediary liability. In India, Section 79 of the Information Technology (IT) Act, 2000 forms the basis of online intermediary liability. The provision allows safe harbour or immunity from liability for third-party content to platforms provided they do not initiate the transmission, modify its contents, select its recipients, and observe due diligence in carrying out its functions. In 2011, the Intermediaries Guidelines were introduced laying out the standards of due diligence. Amendments to the 2011 Rules were proposed in 2018 in view of the fake news being spread on social media. The Information Technology (Intermediary Guidelines and

¹⁰⁹ Sano-Franchini (n 40).

¹¹⁰ Haidt and Rose-Stockwell (n 38).

¹¹¹ Amber Sinha, 'Beyond Public Squares, Dumb Conduits, and Gatekeepers: The Need for a New Legal Metaphor for Social Media' (*IT for Change*, 1 November 2020) <<https://itforchange.net/digital-new-deal/2020/11/01/beyond-public-squares-dumb-conduits-and-gatekeepers-the-need-for-a-new-legal-metaphor-for-social-media/>> accessed date missing.

Digital Media Ethics Code) Rules, 2021 have been proposed with the aim of addressing social media accountability against its misuse and abuse.¹¹²

As the regulations have evolved, the nature of social media has also drastically changed. Intermediaries in the past rules have been seen as ‘dumb conduits’ or passive carriers of user-generated content. However, they now offer diverse services, and many of them are much larger in scale. As pointed out through the research, social media platforms play a significant role in shaping the form and substance of content with their design features and algorithms that decide how people will consume it. A broad mandate for all kinds of intermediaries would not capture the nuances of their nature and lead to ineffective regulatory outcomes. The 2021 Rules addressed this concern by introducing three categories of entities; Intermediary, Social Media Intermediary (SMI), and Significant Social Media Intermediary (SSMI). Under these rules, SSMI is currently defined as a SMI with fifty lakh, or five million registered users in India. Based on this YouTube (part of Google), Facebook, Instagram, and Twitter, all can be categorised as SSMIs. The rule mandates that SSMIs would be obligated with a much higher standard of transparency and accountability towards their users. However, there are questions about how this user threshold would be calculated.¹¹³ Despite some of these welcome changes in the regulations, the rules around asking users not to post certain content still use undefined terms that are not based on legal standards, but are subjective indicators of personal sensitivities. Rule 3(1)(b) on due diligence by an intermediary in the 2021 Rules asks intermediaries to inform users not to post content that is “racially, ethnically or otherwise objectionable”, “relating or encouraging money laundering or gambling”, “libellous”, “obscene”, or “insulting or harassing on the basis of gender.”¹¹⁴ This could lead to over-censorship and a chilling effect on free speech.

The 2021 Rules also mandate companies to appoint a grievance officer, and disclose the first originator of messages in response to a legal order (specifically in case of messaging services). Besides posing limitations of technical

¹¹² Torsha Sarkar, Gurshabad Grover, Raghav Ahoja, Pallavi Bedi and Divyank Katira, ‘On the Legality and Constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021’ (*Centre for Internet and Society, India*, 21 June 2021) <<https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021>> accessed date missing.

¹¹³ Torsha Sarkar, ‘New Intermediary Guidelines: The Good and the Bad’ (*Down to Earth*, 26 February 2021) <<https://www.downtoearth.org.in/blog/governance/new-intermediary-guidelines-the-good-and-the-bad-75693>> accessed date missing.

¹¹⁴ Sarkar, Grover, Ahoja, Bedi, and Katira (n 112).

implementation, allowing tracing of online communication infringes on the right to privacy.¹¹⁵

B. Regulatory gaps in addressing hate speech

Currently, India does not have any specific laws targeting online hate speech. It is addressed through the Indian Penal Code's sections 153A, 153B, 295B, and 505(2), which place "reasonable" restrictions on freedom of speech and expression. These provisions mention promoting enmity, hatred or disharmony on the basis of religion, caste, colour, race, language, residence, region or community, as grounds for penalisation. Outraging the religion or religious feelings of a community are also criminalised under these sections. Historically marginalised communities are protected from hate speech through The Protection of Civil Rights Act, 1955 and Scheduled Caste and Scheduled Tribes (Prevention of Atrocities) Act, 1989.¹¹⁶ Rule 3(1)(d) in the 2021 IT Rules again vaguely mentions terms like "decency" and "morality" without defining them, and does not explicitly address hate speech. In the Indian context, resolving the disagreement around what constitutes hate speech or harmful expression has been a consistent challenge, which has often resulted in the targeting and silencing of minority voices. Thus, it is necessary to implement a policy framework that enables independent assessment of information and expression on social media platforms, grievance mechanisms, and judicial forums to challenge content takedowns. These steps can address the manipulation of hate speech and fake news regulations to restrict speech.¹¹⁷

C. Regulatory gaps in addressing fake news

As with hate speech, presently, there is no explicit law against fake news in India. The 2021 IT Rules can be used to unduly take down content, not having precisely defined fake news in the IT Act, and lead to violations of free speech. An example of this was seen during the anti-Farm Bill protests, as mentioned earlier, when the government ordered Twitter to block the accounts of civil society activists, lawmakers, and media, alleging that they were spreading false information about the protests. Recently, Rule 16 of the 2021 Rules was used by the Ministry of Information and Broadcasting

¹¹⁵ Sarkar, Grover, Ahooja, Bedi and Katira (n 112).

¹¹⁶ Shehlat Maknoon Wani, 'Why India Needs a Legal Instrument to Tackle Online Hate' (*Bot Populi*, 8 October 2021) <<https://botpopuli.net/why-india-needs-a-legal-instrument-to-tackle-online-hate/>> accessed date missing.

¹¹⁷ Torsha Sarkar and Gurshabad Grover, 'Platforms as Gatekeepers: Threats to Digital Space' (*Centre for Internet and Society, India*, October 2020) <<https://cis-india.org/internet-governance/blog/india-digital-freedoms-4-platform-governance>> accessed date missing.

to block accounts on social media platforms citing ‘anti-India’ fake news networks.¹¹⁸ The regulations thus, need to have clearer definitions and classifications of fake news to tackle its spread on platforms. Misinformation and disinformation must be identified as the different forms of fake news, along with its subtypes such as misleading content, imposter content, fabricated content, false connection, false context, manipulated content, and satire or parody. Defining these categories in the Act can enable the platforms in practising consistent interpretation and implementation of the law.¹¹⁹

D. Transparency and accountability

Earlier criticisms of the Intermediaries Guidelines have included the lack of transparency from social media platforms. The 2021 Rules remedy this by requiring SSIMs to publish monthly “periodic compliance reports” that share detailed information regarding complaints received and action taken, and the number of specific links or parts of information removed by the platform through any automated tools. The rule does not clarify any further details of these complaints received to describe the obligations for removal. Platforms can remove content based on legal takedown orders, complaints received from users, and on a voluntary basis. They also allow users to report content found ‘objectionable’ under their internal ‘community standards’. More details on such obligations would aid in safeguarding free speech. Another change in the rules in terms of accountability has been an added requirement for SSIMs to provide users with a notice and an opportunity to appeal a content removal action. Since the government circumvented parliamentary procedures while introducing these rules and held no public consultation about them, recommendations have emerged to allow a period of industry-wide and public consultation on the rules to ensure that the obligations do not become outdated, or lead to censorship.¹²⁰

¹¹⁸ Brand Wagon Online, ‘Government puts the Onus of Blocking Fake News on Social Media Intermediaries’ *Financial Express* (21 January, 2022) <<https://www.financialexpress.com/brandwagon/government-puts-the-onus-of-blocking-fake-news-on-social-media-intermediaries/2412795/>> accessed date missing.

¹¹⁹ Lohani (n 71).

¹²⁰ Torsha Sarkar, Gurshabad Grover, Raghav Ahoja, Pallavi Bedi and Divyank Katira, ‘On the Legality and Constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021’ (*Centre for Internet and Society, India*, 21 June 2021) <<https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021>> accessed date missing.

XI. CONCLUSION

The narratives around the two protests on social media have various similarities but some key differences which may relate to their outcomes. Both protests opposed laws that were in the process of being passed without much public consultation. The government's claims for these laws and their advantages for the country were contested. CAA-NRC was promoted on social media as an essential law that will protect the country from the Muslim population, and assert the country's identity as a Hindu nation.¹²¹ There are dedicated groups and accounts on various platforms that peddle this narrative (see annexure 2). The propaganda used many of the tools and design features including algorithmic biases, imagery, hashtags, and comments, to label the protestors as anti-nationals. Even as many of the fake accounts and misinformation were debunked, there was a strong messaging against the protest on social media. This is also to do with CAA NRC being based on anti-Muslim sentiment which is already prevalent in the country.¹²²

The anti-Farm Bill protests however, were not rooted in such strong divisive politics on the grounds of religion. The protests had vast public sympathy for farmers, which reflected in the social media narrative around it.¹²³ The propaganda against these protests was based on two primary messaging; the Farm Bills being beneficial for farmers, and people who are protesting are not farmers but have a separatist agenda. A lot of the fake news and campaigning connected to these messages were exposed on social media. The global support on several platforms that the protests received also contributed to its success.

The research highlighted gaps in laws and policies such as the asymmetrical use of free speech regulation by the government during these protests, using the regulations as they suited the political narrative. This emphasised the need for clearer and more effective laws that protect free speech and privacy while countering hate speech and fake news on social media. The Intermediary Guidelines Rules must be revised to include well-defined ambits of content removal and moderation specifically in the context of hate speech and fake news, along with necessary checks against surveillance and excessive control by the State. Platforms can seek collaborative and auditable

¹²¹ Jelvin Jose, 'The Farmers' Movement and "Anti-National" Messaging in India' (*South Asian Voices*, 18 March 2021) <<https://southasianvoices.org/the-farmers-movement-and-anti-national-messaging-in-india/>> accessed 15 January 2022.

¹²² *ibid.*

¹²³ *ibid.*

content moderation policies which are specific to local contexts, involving communities in various processes of evaluation.¹²⁴

The findings also helped in understanding the impact of design on the political narratives around protests. While social media platforms are constantly trying to make design changes for enabling more conversations and more ‘delightful’ experience¹²⁵ such as customisation features, they are not squarely addressing the problems of disinformation, hate speech, harassment, and censorship on the platforms. Recent laws such as the Data Protection Bill explicitly include a Privacy by Design (PbD) approach. However, they are limited in their understanding of application of this approach in the interface design of digital platforms.¹²⁶ Similarly, laws and policies around social media platforms must consider applying a proactive and holistic approach to ensure that interfaces and features are designed to counter hate speech, and safeguard free speech and privacy. The interfaces of platforms should be conceptualised keeping these concerns in mind as opposed to them being an afterthought. The use of manipulative design mechanisms should be curbed using regulatory interventions. The seemingly unintentional impact of design on political discourse must be questioned and accounted for.

¹²⁴ Gaur (n 73).

¹²⁵ Pardes (n 40).

¹²⁶ Saumyaa Naidu, Akash Sheshadri, Shweta Mohandas, and Pranav M Bidare, ‘The PDP Bill 2019 Through the Lens of Privacy by Design’ (*The Centre for Internet and Society*, 12 November 2020) <<https://cis-india.org/internet-governance/blog/the-pdp-bill-2019-through-the-lens-of-privacy-by-design>> accessed 24 March 2022.

ANNEXURE 1: POSTS ON ANTI-CAA NRC PROTESTS OBSERVED ON YOUTUBE

The following posts were identified as some of the top posts on YouTube using varying keywords. These have been listed in order of their reach based on Views.

S. No.	Keywords	Title of Post	Link	Date of Publication	Author	Views	Likes
1	CAA NRC	THE REAL INDIAN - CAA and NRC REPUBLIC DAY SPECIAL RachitRojha Rohit Sharma	https://www.youtube.com/watch?v=J-NlJalaDO4	January 25, 2020	Rachit Rojha	17M	252K
2	CAA NRC Protests	“We Don't Want to Create Ruckus, We're here for Our Rights” I The Wire Shekhar Tiwari CAA Protest	https://www.youtube.com/watch?v=M66MtjZSUT8	December 20, 2019	The Wire	13M	141K
3	CAA NRC	NRC Citizenship Amended Act वर Asaduddin Owaisi Vs Mukhtar Abbas Naqvil Agenda Aajtak CAA protest	https://www.youtube.com/watch?v=dfcU7V9Mevc	December 16, 2019	The Lallantop	13M	162K

4	CAA NRC	ये देश छोड़कर भागना पड़ेगा NRC, CAA, CAB/ Dr. Kanhaiya Kumar Latest Speech On NRC/ DR.KANHAIYA/Jale Translation: "Will have to leave this country and run"	https://www.youtube.com/ watch?v=glxtFNDONrww	February 11, 2020	Islamic Mushaira Media	9.5M	90K
5	CAA NRC Protests	कश्मीरी लड़की ने NRC और CAA पर क्रिया बड़ा खुलासा! जा नकर रह जाणो! दो Voice News Network Translation: "Kashmiri girl made a big disclosure on NRC and CAA! You will be shocked to know"	https://www.youtube.com/ watch?v=TY48uqP44pw	January 10, 2020	Voice News Network	3.7M	128K
6	CAA NRC Protests	Prime Time, Jan 09, 2020 Ravish's Ground Report On The Unshakeable Women Of Delhi's Shaheen Bagh	https://www.youtube.com/ watch?v=TQm7nBa49WQ	January 9, 2020	NDTV	3.6M	112K
7	CAA NRC Protests	Aftermath of CAB + NRC Explained by Dhruv Rathee	https://www.youtube.com/ watch?v=4b-64pnS254	December 17, 2019	Dhruv Rathee	3.4M	315K

8	CAA NRC	Swara Bhasker Gets All Fired Up Over CAA, NRC, NPR ABP News	https://www.youtube.com/watch?v=R4uLZ8Uikig	February 22, 2020	ABP News	2.2M	52K
9	CAA NRC	Not Only Muslims, CAA & NRC Will Affect Hindus Without Documents: CM Kejriwal ABP News	https://www.youtube.com/watch?v=QoscNnzzng8	January 4, 2020	ABP News	1.6M	18K
10	CAA NRC Protests	CAA Protest Shahrugh Khan का बयान Viral हो गया Latest NRC Shaheen Bagh Hindu Muslim Translation: Shahrukh Khan's testimony has gone viral	https://www.youtube.com/watch?v=ToOUbtwJ9p8	January 27, 2020	Zee News	1.3M	19K
11	CAA NRC Protests	Anti-CAA Protests पर PM Modi: अगर हम आज पीछे हटे तो इन लोगों की हिम्मत बढ़ेगी। Translation: If we step back today, the courage of these people will increase	https://www.youtube.com/watch?v=j6Kvhh-8ywe	February 4, 2020	Zee News	1M	17K
12	CAA NRC Protests	Lucknow: Women Sitting On Anti-CAA Protests Refuse To Move ABP News	https://www.youtube.com/watch?v=btKQg5oRl_o	March 19, 2020	ABP News	1M	5K

These posts were accessed on December 20, 2021 and January 11, 2022. The number of views and likes have been recorded on the above-mentioned dates.

ANNEXURE 2: POSTS ON ANTI-CAA NRC PROTESTS OBSERVED ON FACEBOOK

The following posts were identified as some of the top posts on Facebook using varying hashtags. These have been listed in order of their popularity based on Likes. These posts include videos, images, and textual content.

S. No.	Hashtag	Title of Post	Link	Date of Publication	Author	Views	Likes
1	#CAA NRC Protests	NRC-CAA Protest	https://www.facebook.com/watch/?v=446099766271339	January 13, 2020	Indian American Muslim Council	2.7M	194K
2	#CAA NRC	Historic Women's Protest Against CAA & NRC In Gulbarga.	https://www.facebook.com/Gulbargalife/videos/historical-womens-protest-against-caa-nrc-in-gulbarga/669164156950861/	December 26, 2019	Gulbarga Times	1.2M	154K
3	#CAA NRC Protests	NRC, CAA & Muslims	https://www.facebook.com/STAGEdotin/posts/3114731761895125	January 16, 2020	STAGE	-	120K
4	#CAA NRC Protests	Gulbarga Shaheen Bagh Protest	https://www.facebook.com/watch/?v=3029771957079506	February 14, 2020	Gulbarga Times	1M	104K

5	#CAA NRC	#Hathras की संदिग्ध महिला का सच आया सामने Translation: The truth of the suspected woman of Hathras came to the fore	https://www.facebook.com/watch/?v=352773739111906	October 15, 2020	Zee News	472K	6.5K
6	#CAA NRC Protests	Watch: Anti-CAA and NRC protests in Lucknow have led to the UP government announcing cash reward for the arrest of eight absconding protestors किसान बिल वापस हो की जिद इसीलिए ताकि	https://www.facebook.com/watch/?v=373106743742754	November 6, 2020	Zee News English	135K	3.7K

7	#CAA NRC	<p>370, CAA, NRC, तीन तलाक के भी वापिस होने का रास्ता खुल जाये साजिश से सावधान हो जायें</p> <p>Translation: The demand for taking back the Farm Bill is so that the path to repeal [section] 370, CAA, NRC, and Triple Talaq [Act] also clears up. Beware of the conspiracy</p>	<p>https://www.facebook.com/groups/1855870747892234/posts/2467920940020542/</p>	December 17, 2020	Member on Population Control Act Support Group	3.2K
---	-------------	---	--	-------------------	--	------

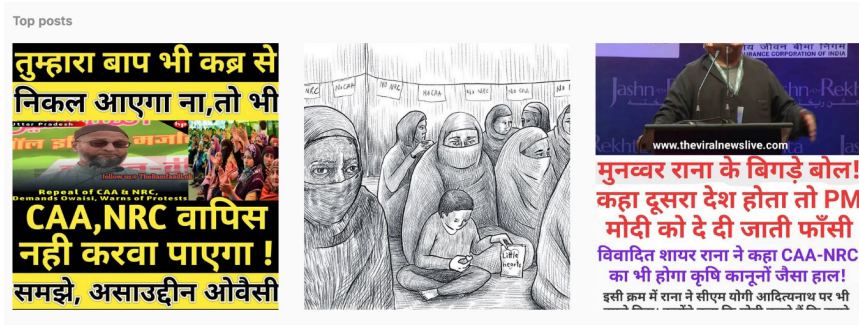
8	#CAA	<p>CAA कानून पर एक इंच भी पीछे नहीं हटेंगे नरेंद्र मोदी यह सुनकर रु 15 लाख आ गए मेरे खाते में जय हिंद। 🇮🇳</p> <p>Translation: Won't go back an inch on CAA law: Narendra Modi, 15 lakhs came into my account on hearing this, Jai Hind</p>	<p>https://www.facebook.com/groups/1855870747892234/posts/2095153503963956/</p>	February 16, 2020	Member on Population Control Act Support Group	-	2.5K
---	------	--	--	-------------------	--	---	------

These posts were accessed on December 20, 2021 and January 11, 2022. The number of views and likes have been recorded on the above-mentioned dates.

ANNEXURE 3: POSTS ON ANTI-CAA NRC PROTESTS OBSERVED ON INSTAGRAM

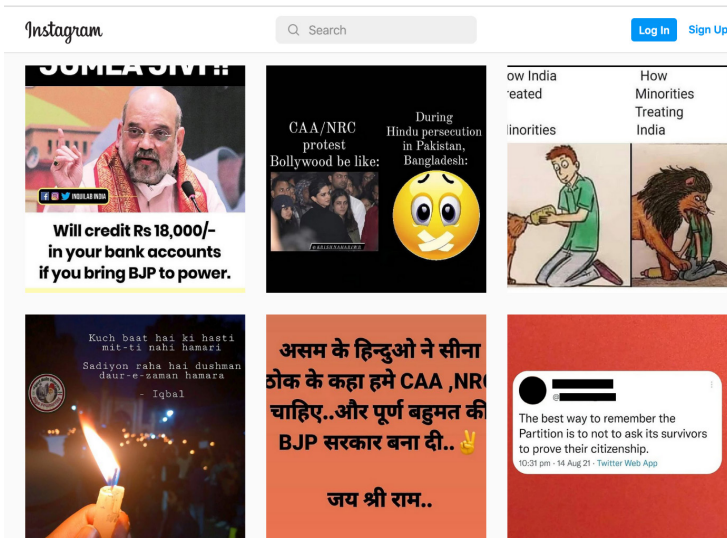
Following are the search queries on Instagram using different hashtags and their corresponding screenshots accessed on January 11, 2022. Instagram does not allow access to view posts without having signed in. Hence, the posts were observed through these search results.

#CAANRC: <https://www.instagram.com/explore/tags/caanrc/?hl=en>



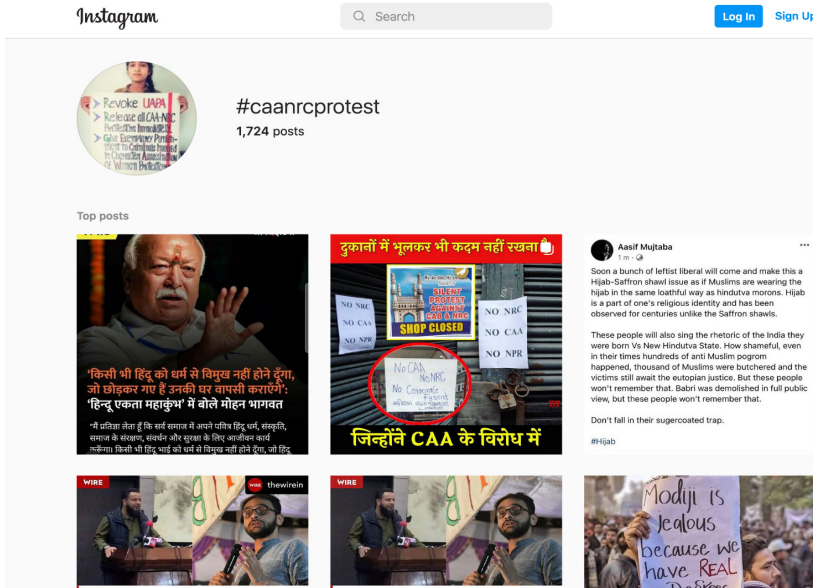
Translation (left to right): “CAA, NRC will not be repealed even if your ancestors come alive from their graves, got it Asaduddin Owaisi!”

“Bad words from Munawwar Rana! Says that if it were any other nation, PM Modi would have been hanged. Controversial Urdu poet said that CAA-NRC will face the same fate as the Farm Bill!”



Translation: “The Hindus in Assam have declared that they want CAA, NRC.. and have formed the BJP government by absolute majority.. Jai Shri Ram..”

#CAANRCProtest: <https://www.instagram.com/explore/tags/caanrcprotest/?hl=en>

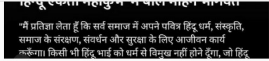


Translation (left to right): “Will never let Hindus turn away from religion, those who have left will return home: Mohan Bhagwat said in the ‘Hindu Ekta Mahakumbh’”


“Do not step into the shops of those who opposed CAA”

Instagram

Q Search Log In Sign Up




जिन्होंने CAA के विरोध में



Court Dismisses Delhi Police's Plea Seeking Handcuffs for Umar Khalid, Khalid Saifi During Trial


The applications were moved by Delhi Police contending that Umar and Khalid are 'high-risk prisoners'. However, Umar and Khalid were already granted bail in the Khajuri Khas riots case.




Court Dismisses Delhi Police's Plea Seeking Handcuffs for Umar Khalid, Khalid Saifi During Trial

The applications were moved by Delhi Police contending that Umar and Khalid are 'high-risk prisoners'. However, Umar and Khalid were already granted bail in the Khajuri Khas riots case.

Don't fall in their sugarcoated trap.
#Hijab



Modiji is Jealous because we have REAL Degrees




Umar Khalid
17 Dec 2019 · 🌐


gime and it's policies like CAB are anti-Muslim, and y so. Nothing to be shocked about it anymore. But is dus and for people of another faith? Will the NRC nt ut the other communities? To avail citizenship thro ter being excluded from NRC, requires a person to p has faced religious persecution in Pakistan, Bangla ghanistan. How will a Tamil Hindu, a Kannada Jain, t ashtrian Christian, a Sikh from Andhra be ever able t hat he came to India from Afghanistan or Pakistan c desh. It is impossible.

1s are the direct targets of CAB/NRC/NPR. The othe unities would be the collateral damage. The poor, the as, the displaced would be the worst sufferers!

JATT DA MUQABLA



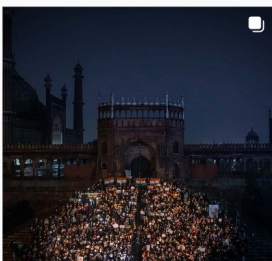


#CAANRCProtests: <https://www.instagram.com/explore/tags/caanrcprotests/?hl=en>

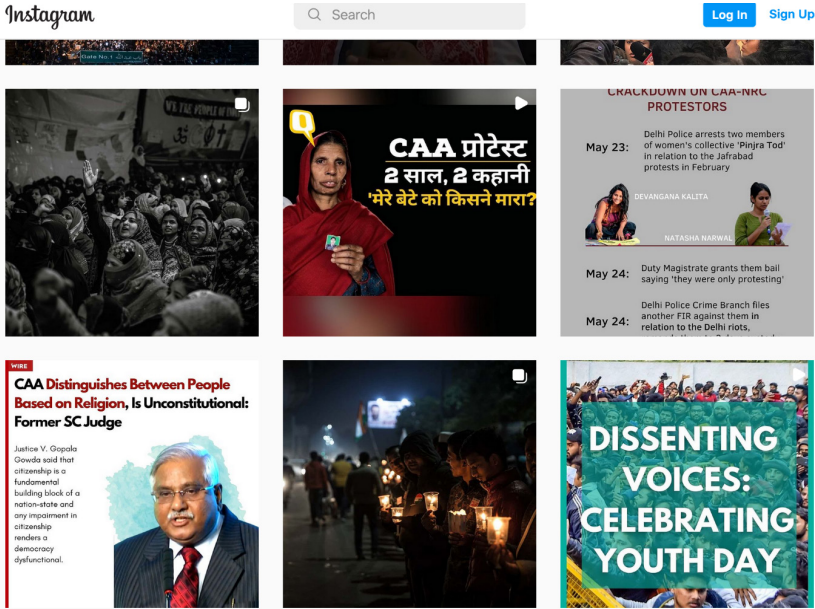


#caanrcprotests

545 posts

Top posts

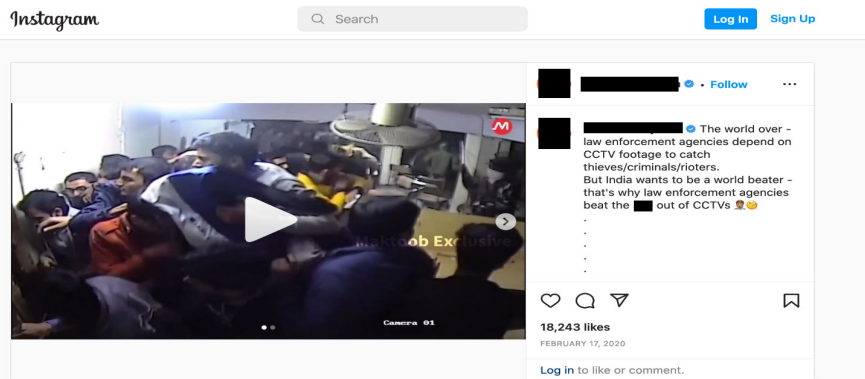






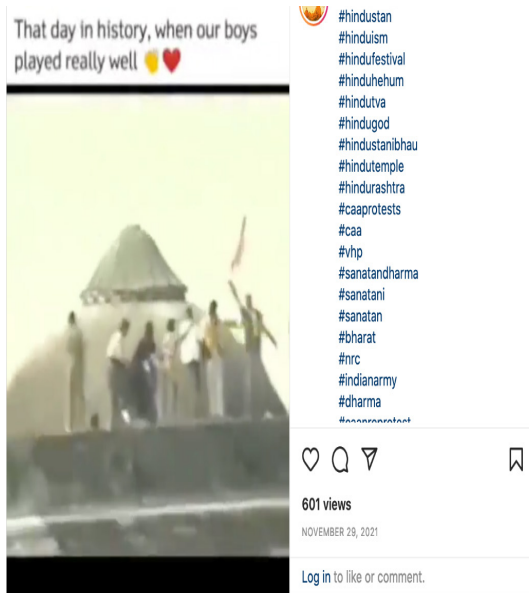
Translation: “CAA Protest: 2 years, 2 stories; ‘Who killed my son?’”

Following are some of the top posts that could be accessed on Instagram.

Screenshot of the video showing students being beaten up by Delhi police; URL: https://www.instagram.com/p/B8qWr_clZzd/; accessed on January 11, 2022



Screenshot of the video showing demolition of Babri Masjid in 1992;
URL: https://www.instagram.com/p/CW2yBzgD-_h/; accessed on January 11, 2022



ANNEXURE 4: POSTS ON ANTI-CAA NRC PROTESTS OBSERVED ON TWITTER

The following tweets were identified as some of the top posts on Twitter using a specific set of hashtags and engagement metrics. These have been listed in order of their reach based on Retweets. These tweets include videos, images, and textual content.

Hashtags used for the search query: #caanrcprotests #caanrc #caa #nrc


Engagement metrics: Minimum Faves: 3000, Minimum Retweets: 3000

Date of Tweet: Between December 2019 to December 2021

S. No.	Hashtag	Content of Tweet	Link	Date of Tweet	Author	Re tweets	Faves
1	#CAA #NRC	#CAA + #NRC + more this Sunday on @patriotact	https://twitter.com/hasanminhaj/status/1208083503721656320	December 20, 2019	Hasan Minhaj	15.2K	38.4K
2	#CAA	During #COVID19 crisis, there are reports #India govt is arresting Muslim activists protesting the #CAA, including Safoora Zargar who is pregnant. At this time, #India should be releasing prisoners of	https://twitter.com/USCIRF/status/1260926337063292928	May 14, 2020	USCIRF	12.6K	25.7K

3	#CAA	<p>conscience, not targeting those practicing their democratic right to protest.</p>	<p>बड़ी संख्या में लोग पूछ रहे हैं जो लोग #CAA के विरोध में हैं वो सब सड़कों पर दिख रहे है लेकिन #CAA का समर्थन करने वाले अपनी आवाज़ देश तक कैसे पहुंचाए? अब @Zee News बनेगा आपकी आवाज़। 7836 800 500 पर missed call करें। अपने दोस्तों और परिवार के साथ भी शेयर करें।</p> <p>Translation: A large number of people are asking – those who are against #CAA are all visible on the streets but how can those who support #CAA reach their voices to the country? Now अब @Zee News will become your voice. Give a missed call on 7836 800 500. Share with your friends and family also.</p>	<p>https://twitter.com/sudhirchaudhary/status/1208663008156770304</p>	December 22, 2019	Sudhir Chaud hary	8K	33.7K
---	------	--	--	---	-------------------	-------------------	----	-------

4	#CAA, #CAA_ NPR_वापस लो	India Muslim women protesting #CAA threatens: “Jis din Musalman Hinduon se zyada hogaya, patak patakke marrege.” (“The day we Muslims exceed the number of Hindus [in India] we will smash them one by one.”) #CAA_NPR_वापस-लो	https://twitter.com/TarekFatah/status/1222163703824445442	January 28, 2020	Tarek Fatah	8K	12.5K
5	#CAA, #Anti CAA Protests	Bangladesh Mullahs spill venom against PM @NarendraModi on streets of Dhaka. They r protesting India's new#CAA law. As I said earlier, the entire #Anti CAA Protests is anger at not being able to turn West Bengal into a Muslim majority state like J&K. https:// twitter.com/ Sakibul Hoque8/	https://twitter.com/TarekFatah/status/1236268848309047298	March 7, 2020	Tarek Fatah	7K	16K

6	#CAA	<p>पारस 11 बजे फोन पर मुझे जान से मारने की धमकी दी गयी फोन करके कहा गया कि #CAA के समर्थन में बोलना बंद करो वरना मार डालेंगे। कॉल +4044 और +5065 नंबर से आया हत्या की धमकियां फेसबुक मैसेंजर पर भी दी जा रही है #CAA के समर्थन में डंके की चोट पर बोलूंगा</p> <p>Translation: Yesterday at 11 o'clock I was threatened with death on the phone. The call came from +4044 and +5065 numbers Murder threats are also being given on Facebook Messenger I am not afraid and will speak in support of #CAA on sting</p>	<p>https://twitter.com/KapilMishra_IND/status/1209312904035463168</p>	December 24, 2019	Kapil Mishra	7K	27.5K
7	#CAA	<p>So this is what's the actual agenda? What's  the sacred symbol of the Hindus got to do with the #CAA ?</p>	<p>https://twitter.com/sambitswaraj/status/1208230275014111233</p>	December 21, 2019	Sambit Patra	6K	18.7K

8	#CAA	<p>And as expected @INCIndia President Sonia Gandhi supports this! ॐ is the eternal,ever present “अनहदनाद” ..try as hard ..you will never ever succeed in erasing my ॐ शक्ति 🙏</p>	<p>देश में लौफ पैदा करने वाली नक्सलवादियों और जिहादियों की संयुक्त सायिशा कर दमन करने में दिल्ली पुलिस के हर प्रयास में भारत का हर नागरिक साथ खड़ा है। देश द्रोही तत्वों की जल्दी से जल्दी पहचानकर उनके विरुद्ध संवैद पानिक कार्यवाही की जायेगी, ऐसा देश का हर नागरिक विश्वास रखता है। #CAA Translation: Every citizen of India stands together in every effort of Delhi Police in suppressing the joint conspiracy of Naxalites and Jihadis to create fear in the country. Called and told to stop speaking in support of #CAA or else you will kill me</p>	<p>https://twitter.com/smittal_ips/status/1206286046524104704</p>	December 16, 2019	Dr. Sandeep Mittal, IPS	5K	10K
---	------	--	--	--	-------------------	-------------------------	----	-----

		The anti-national elements will be identified as soon as possible and constitutional action will be taken against them, every citizen of the country believes. #CAA (Poll) Yes: 96%; No: 4% 51,819 votes					

These tweets were accessed on January 11, 2022. The number of Retweets and Likes have been recorded on the above-mentioned date.

ANNEXURE 5: POSTS ON ANTI-FARM BILL PROTESTS OBSERVED ON YOUTUBE

The following posts were identified as some of the top posts on YouTube using different keywords. These have been listed in order of their reach based on Views.

S. No.	Keywords	Title of Post	Link	Date of Publication	Author	Views	Likes
1	Farmers Protest	Kisaan Anthem Mankirt Nishawn Jass Jordan Fazilpurial Dilpreet Flow Shreel Afsana Bobby	https://www.youtube.com/watch?v=oNjiYuPmh9A	December 8, 2020	Shree Brar	52M	1.2M

2	Farmers Protest, Farm Laws, Farm Bill	Agriculture Reform Bill 2020 MSP APMC Aadti Kisan Andolan One India One Agri Market	https://www.youtube.com/watch?v=3EUL_f8vGJ0	September 20, 2020	Khan GS Research Centre	21M	764K
3	Farm Laws, Farm Bill	Farm Bills : Myth vs Reality - Dr. Vikas Divyakirti : Concept Talk Drishti IAS	https://www.youtube.com/watch?v=YcqvWFZXYaE	December 10, 2020	Drishti IAS	10M	238K
4	Farmers Protest	Farmers Protest Kisan Andolan PM Modi Baba Ramdev Rakesh Tikait Prime Time Godi Media	https://www.youtube.com/watch?v=gDrE123daSo	February 22, 2021	Public Reaction Bank	8M	79K
5	Farm Laws, Farm Bill	DNA: Farmers Protest के शुरुआत PM Modi ने सराया PM Modi on new farm laws New agricultural laws Translation: Farmers Protest's Lies Faced With PM Modi	https://www.youtube.com/watch?v=SZUlapdJ5SM	December 18, 2020	Zee News	6M	37K
6	Farm Laws, Farm Bill	Asaduddin Owaisi, Rakesh Tikait on PM Modi repealing Farm Laws FULL Coverage	https://www.youtube.com/watch?v=Nfqx8atZdSE	November 19, 2021	ABP NEWS	5M	47K

7	Khalistani	DNA: खालिस्तान बनाने का बेमिसाल आइडिया Sudhir Chaudhary Khalistan Canada Analysis Formula Translation: Unique idea to make Khalistan	https://www.youtube.com/watch?v=NNw8SuJAyIM	February 9, 2021	Zee News	640K	15K
8	Khalistani	DNA: किसान आंदोलन में खालिस्तानी शक्ति का नया खुलासा Sudhir Chaudhary Khalistan Analysis Khalistan Translation: New disclosure of Khalistani conspiracy in farmers' movement	https://www.youtube.com/watch?v=8y1a-i7Lbq0	December 10, 2020	Zee News	483K	12K

These posts were accessed on January 20, 2022. The number of views and likes have been recorded on the above mentioned dates.”

ANNEXURE 6: POSTS ON ANTI-FARM BILL PROTESTS OBSERVED ON FACEBOOK

The following posts were identified as some of the top posts on Facebook using varying hashtags. These have been listed in order of their popularity based on Likes. These posts include videos, images, and textual content.

S. No.	Hashtag	Title of Post	Link	Date of Publication	Author	Views	Likes
1	#farmers protests	<p>हल किसानों की हिमालय</p> <p>ਜਦੋਂ ਕਿਸਾਨਾਂ ਦੀ ਹਿਮਾਲੀ</p> <p>ਜਦੋਂ ਕਿਸਾਨਾਂ ਦੀ ਹਿਮਾਲੀ</p> <p>Translation: This is how the Muslim community gave support to farmers</p> <p>#FarmersBill #FarmersProtests #FarmLaws2020 #FarmersProtest News #KisanBills2020 #Farmersprotest #SinghuBorder #GhaziपुरBorder</p>	https://www.facebook.com/ptcnews/online/posts/3906291426057564	February 2, 2021	PTC News	-	297K

2	#farm laws	<p>ਖੇਤੀਬਾੜੀ ਨੂੰ ਚੰਗੇ ਢੰਗ ਨਾਲ ਚਲਾਉਣ ਲਈ ਯੋਗੀ ਯੋਗੀ Adityanath ਨੇ ਕਿਸਾਨਾਂ ਨੂੰ ਸਮਝਾਉਣ ਲਈ ਮੀਂਸ ਫਿਲਮਾਂ ਨੂੰ ਨਰੇਂਦਰਾ ਮੋਦੀ ਨੇ ਬਹੁਤ ਵਧੀਆ ਫ਼ੈਸਲੇ ਲਿਆ Translation: M Yogi Adityanath described the decision to repeal the agriculture law as historic, “We failed to convince the farmers, PM Narendra Modi took a very good decision”</p>	<p>https://www.facebook.com/watch/?v=4632242785223616</p>	November 19, 2021	Kirsani - Farming	1.5M	111K
3	#farmers protests	<p>Ready to purchase crops at cheaper rate than MSP: Naresh Tikait #TikaitExposed #RakeshTikait #FarmersProtests</p>	<p>https://www.facebook.com/watch/?v=379089130607603</p>	September 28, 2021	DNA India	1.1M	19K

4	#farmers protests	टिकैत साहब के सबसे करीबी पत्र का रनेयूं खोला हिंसा का राज छ न्यवाद अजीत अंजुम #FarmersProtests #RedFortAttack Translation: Journalist closest to Tikait opened the secret of violence like this, thanks Ajit Anjum	https://www.facebook.com/watch/?v=262965158515728	January 28, 2021	Individual	2M	18K
5	#Khalistani	खालिस्तान आतंकवादियों पर सबसे बड़ी कार्यवाही की तैयारी में सरकार #Khalistani #FarmersProtests Translation: Government preparing for the biggest action against Khalistani terrorists	https://www.facebook.com/ZeeNews/posts/4511531925577999	December 17, 2020	Zee News	-	10K

6	#Khalistani	<p>खालिस्तान और पाकिस्तानी शक्तियों के मसूबों को बड़ा झटका</p> <p>#FarmLaws #Khalistani Translation: Big blow to the plans of Khalistani and Pakistani powers</p>	<p>https://www.facebook.com/ZeeNews/posts/5660196650711515</p>	November 19, 2021	Zee News	-	5.3K
7	#farmlaws	<p>पहले कहते थे मंडिया खत्म हो जाएगी, अब उसी में किसान जला रहे 100 किलो लहसुन: कृषि कानून होते तो नहीं आती ये नौबत, जानिए कैसे #Mandsaur #FarmLaws</p> <p>Translation: Earlier they used to say that markets will be finished, now farmers are burning 100 kg garlic in the same: If there were agricultural laws, then this trouble would not come, know how</p>	<p>https://www.facebook.com/opindia.in/posts/1666938353658668</p>	December 19, 2021	OpIndia Hindi	-	2.3K

8	#Khalistani	Please note that people like #DishaRavi are not arrested for spreading lies about govt but they are arrested when the link was established between fake activists and #khalistani elements	https://www.facebook.com/watch/?v=412454966717889	February 15, 2021	PMO India: Report Card	-	1.8K
---	-------------	--	---	-------------------	------------------------	---	------

These posts were accessed on January 21, 2022. The number of views and likes have been recorded on the above mentioned dates.

ANNEXURE 7: POSTS ON ANTI-FARM BILL PROTESTS OBSERVED ON INSTAGRAM

Following are some of the top posts that could be accessed on Instagram under different hashtags.

#farmbill: Repeal of Farm Laws announcement; URL: <https://www.instagram.com/p/CWcbNoEhdva/>; accessed on January 11, 2022



Translation: “Modi governments’ big announcement for the country’s food provider (farmers). The government has rolled back the three farm laws. Modi took the decision on the occasion of Guru Purab (birth anniversary of the first Sikh Guru)”

#farmbill: Comparison with Indira Gandhi; URL: <https://www.instagram.com/p/CWcwpmGNauI/>; accessed on January 11, 2022

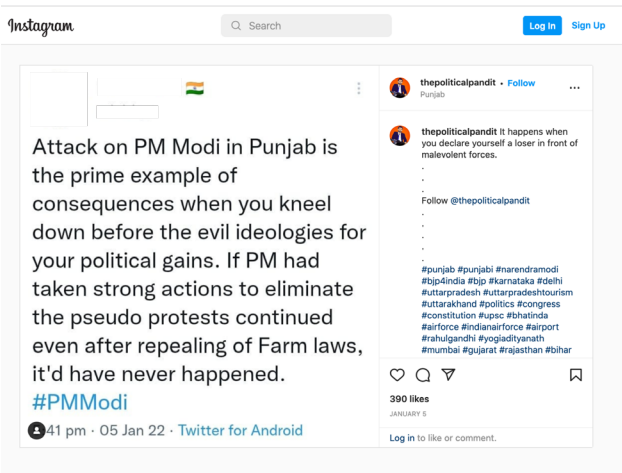


Translation: “This is the difference. Dictator’s government (referring to Indira Gandhi’s image) in interest of power; Democratic government (referring to Narendra Modi’s image) in interest of the nation.”

#farmersprotest: Image of Punjabi artists at the protest; URL: <https://www.instagram.com/p/CYiG8KFFMRB/>; accessed on January 11, 2022



#farmersprotest: Claims of protests being inauthentic or ill-intended; URL: <https://www.instagram.com/p/CYWRw3rPwSw/>; accessed on January 11, 2022



#farmbill: Claims of repeal being for national interest; URL: <https://www.instagram.com/p/CWdu0DgP9FJ/>; accessed on January 11, 2022



Translation: “Whatever I did was for the farmers, what I am doing now is for the benefit of this nation”

ANNEXURE 8: POSTS ON ANTI-FARM BILL PROTESTS OBSERVED ON TWITTER

The following tweets were identified as some of the top posts on Twitter using a specific set of hashtags and engagement metrics. These have been listed in order of their reach based on Retweets. These tweets include videos, images, and textual content.

Hashtags used for the search query: #farmersprotests #farmersprotest #farmlaws #farmbill #khalistani

Engagement metrics: Minimum Faves: 3000, Minimum Retweets: 5000

Date of Tweet: Between December 2019 to December 2021

Another search was conducted using the keyword “Khalistani”

Engagement metrics: Minimum Faves: 1000, Minimum Retweets: 1000

Date of Tweet: Between December 2019 to December 2021

S. No.	Hashtag	Content of Tweet	Link	Date of Tweet	Author	Retweets	Faves
1	#farmers protests	There has been much social media coverage around the #FarmersProtest in #India. Very useful guide to the legislation and the impact on farmers.	https://twitter.com/BobBlackman/status/1357755699162398720	February 5, 2021	Bob Blackman	18K	39.5K
2	#farmers protests	#WATCH Delhi: Protestors attacked Police at Red Fort, earlier today. #FarmersProtest	https://twitter.com/ANI/status/1354088807424028673	January 26, 2021	ANI	11.3K	25.1K
3	#Khalistani	BIG EXPOSE ON @GretaThunberg @miakhalifa @rihanna FUNDING CONNECTION FROM KHALISTAN SUPPORTER ORG.	https://twitter.com/TajinderBagga/status/1357072379084595200	February 4, 2021	Tajinder Pal Singh Bagga	10.1K	20.8K

4	#Khalistani	100s of people in a rally in Punjab's Gurdaspur raised Azadi & Khalistan slogans. This is in India. Home Minister Amit Shah should wake up. Situation in Punjab is getting worse now	https://twitter.com/Ask-Anshul/status/1455808023926960129	November 3, 2021	Anshul Saxena	5K	14K
5	#Khalistani	Who is the man in farmer protest video, lying about 'govt snatching farmland': Profile of an actor and Khalistan supporter	https://twitter.com/OpIndia_com/status/1332633524822626304	November 8, 2020	OpIndia.com	4K	15K
6	#Khalistani	Meet Mo Dhaliwal, the creator of the toolkit. "The repeal of the farm bills is the beginning of this battle, not the end. You're not separate from the Khalistan movement. We're here for the independence of Punjab." If this isn't a secessionist conspiracy, what is?	https://twitter.com/sudhirchaudhary/status/1357674016115286016	February 5, 2021	Sudhir Chaudhary	4K	10.5K

7	#Khalistani	Congress Organised Protesters are Raising Khalistan Jindabad Slogans. I always said they are not Kisans, they are Congress workers, Farmers are Nationalists, they can't say Khalistan Jindabad	https://twitter.com/TajinderBagga/status/1309514020269981696	September 25, 2020	Tajinder Pal Singh Bagga	4K	11K
8	#Khalistani	Skyrocket, a PR firm owned by Mo Dhaliwal paid \$2.5 million to Rihanna for her tweet on Farm protests. Dhaliwal is a Khalistan supporter who is also close to Canadian leader Jagmeet Singh Now connect the dots	https://twitter.com/TrulyMonical/status/1357577804703911937	February 5, 2021	Monica	2K	6K

9	#Khalistani	Rihanna was paid \$2.5 million (Rs 18 crore) by PR firm with Khalistani Links to tweet in support of farm protests. How much were Greta Thunberg and Mia Khalifa paid to be farmers?	https://twitter.com/abhijitmajumder/status/1480980424180453377	January 12, 2022	Abhijit Majumder	1K	4K
---	-------------	---	---	------------------	------------------	----	----

These tweets were accessed on January 11, 2022. The number of Retweets and Likes have been recorded on the above-mentioned date.

DATA PRIVACY AND ELECTIONS IN INDIA: MICROTARGETING THE UNSEEN COLLECTIVE:

*Sayantana Chanda**

ABSTRACT *In India, the usage of social media to reach hundreds of millions of active online users is common across political parties. With revelations regarding data mining being undertaken by political parties across the world, there is a need for robust data privacy not only to protect individuals, but also to ensure free and fair elections. In this context, the importance of the data collected lies in the inferences it allows a data fiduciary to draw about the person whose data is collected. Access to private details, through mining of online data from social networks and other sources, allows individuals to be aggregated into unseen collectives, purely on the basis of specific data points, and for them to be given targeted and even false messages. Most importantly, this is a problem on a societal scale, as micro-targeting occurs across large groups of people and not merely at the individual level. Thus, the individual centric focus of data privacy law is insufficient when the target of manipulation is not one individual, but entire groups or collectives of people.*

This paper will highlight how both the Data Privacy Bills as introduced by the Indian Government in 2019 and 2022, fail to account for the collective privacy of citizens and how the rights provided do not address the problem of inferences. To that end, a move away from individual privacy and toward collective privacy will be proposed which can protect individuals who are assimilated unknowingly into collectives that are based on mined data.

* Judicial Law Clerk-cum-Legal Researcher at the Supreme Court of India. Undergraduate law degree from O.P. Jindal Global Law School. Views are personal. Feedback is welcome at: sayantan122194@gmail.com. The author would like to acknowledge the efforts and assistance of the peer-reviewer and the editorial team at the NLS Indian Journal of Law and Technology, whose comments were invaluable in refining this work. The author would additionally like to acknowledge Muskan Tibrewala (Advocate at the Delhi HC & Supreme Court), Aiswarya Murali (Judicial Law Clerk-cum-Legal Researcher at the Supreme Court) and Ashish Matthew (former Analyst at a political consultancy) for their advice/assistance on this project.

I Introduction	273	Redundancy of the Notification Requirement for Inferences	296
II. Elections in a Digital India	277	Sensitive Personal Data	299
III. Drawbacks of Data Analytics in Elections	281	Fairness	301
IV. Data Privacy in Elections and Indian Election Laws.	283	Privacy as a Balancing Act	302
V. Details of the Data Protection Bill	285	VII. The Need for Collective Privacy	303
VI. Inferences, Elections, and the Pdp Bill.	289	Alternative Approaches to Protecting Privacy of Groups	303
Status of Inferences under the GDPR and PDP Bill.	289	Group Privacy	306
Application of Data Principals' Data Rights to Inferences	292	Collective Privacy	307
Inferences and Rights of the Data Fiduciary.	294	Enforcement of Collective Privacy Rights	310
		VIII. Conclusion	314

I. INTRODUCTION

The Personal Data Protection Bill, 2019 ('PDP Bill' or 'Bill') went through various revisions over the past 3 years. It was the subject of much discussion among privacy activists, industry heads, government departments, and consumers. The discussions led to a second draft being issued in 2021, however, this also proved inconclusive. It seemingly did not address the entire ambit of concerns that were raised regarding some of the potential drawbacks of the Bill. Hence, on August 3, 2022, the PDP Bill, was withdrawn and it was announced that a new bill would be tabled soon with substantial alterations.¹ It is disappointing that after 3 years of deliberations, the PDP Bill has now returned to the drawing board. However, this turn of events presents an opportunity as well to highlight certain issues with the Bill. The revised Personal Data Protection Bill, 2022 ("2022 Bill" or "PDP Bill, 2022"), was duly introduced which cut out various excessive measures such as data residency requirements within the country and criminal penalties.² However, these changes are primarily targeted toward easing the privacy related compliance requirements for commercial actors.³ In other contexts, various loopholes remain that require addressing. Specifically with regard to

¹ The Hindu Bureau, 'Union Government Rolls Back Data Protection Bill' *The Hindu* (New Delhi, 3 August 2022), <<https://www.thehindu.com/news/national/union-government-rolls-back-data-protection-bill/article65721160.ece>> accessed 8 August 2022.

² Sourabh Lele, 'Nasscom Hails Draft Data Protection Bill for Dropping Contentious Rules' *The Business Standard* (New Delhi, 5 December 2022), <https://www.business-standard.com/article/economy-policy/industry-body-nasscom-welcomes-draft-digital-personal-data-protection-bill-122120501098_1.html> accessed 9 December 2022.

³ Hemant Kashyap, 'Data Protection Bill: From Deemed Consent to Exemptions, Lack of Clarity May Hurt the Cause' *Inc42* (New Delhi, 5 December 2022), <<https://inc42.com/buzz/data-protection-bill-deemed-consent-exemptions-lack-clarity-hurt-cause/>> accessed 8 December 2022.

microtargeting, the 2022 Bill, in fact, constitutes a step in the wrong direction.

The importance of data privacy rights has increased with the progress of technology and the increasing digitization of society. The fact that almost all forms of economic activity and human interaction have shifted online has raised several concerns regarding the security of peoples' personal data. Not just protestors, but consumers, researchers, academics, and governments themselves, have taken a keen interest in regulating privacy rights. The interests of these stakeholders are often at odds. While members of civil society desire greater privacy coverage, law enforcement would like access to as much information as possible. While consumers browse the products available to them on Amazon and eBay, they worry about the amount of personal data these tech giants are accumulating. Moreover, while governments take a dim view of their own citizens' privacy rights, they themselves wish to maintain utmost secrecy regarding their own activities with such data.

These complex inter-relationships between stakeholders lead to significant legal and policy implications. One relationship which requires particular scrutiny is that between political parties and the electorate. An example of why this is relevant may be drawn from the Cambridge Analytica scandal associated with the 2016 United States Presidential Elections.⁴ The culpability of Facebook in failing to protect private information led to widespread condemnation of the social media giant.⁵ Cambridge Analytica took advantage of Facebook's Open Graph platform to harvest information about millions of users.⁶ Having created profiles of these individuals based on this information which included their social background, the posts they 'liked', the comments they made and put on their respective Facebook Wall etc., this data was then sold to different political campaigns, including Donald Trump's and was then exploited by these Presidential candidates to target these individuals with targeted messages.⁷ Consequently, having this infor-

⁴ Scott Detrow, 'What Did Cambridge Analytica Do During the 2016 Election?' *NPR* (20 March 2018) <<https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election>> accessed 28 October 2022.

⁵ Emma Graham-Harrison & Carole Cadwalladr, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach', *The Guardian* (London, 17 March 2018) <<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>> accessed 24 September 2021.

⁶ David Ingram, 'Zuckerberg Apologizes for Facebook Mistakes with User Data, Vows Curbs' *Reuters* (21 March 2018) <<https://www.reuters.com/article/us-facebook-cambridge-analytica-idUSKBN1GX0OG>> accessed 24 September 2021.

⁷ Nicholas Confessore, 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far', *New York Times* (New York, 4 April 2018) <<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>> accessed 26 September 2021; Allan Smith, 'There's an Open Secret about Cambridge Analytica in the Political World: It

mation at hand, gives a prospective party/candidate, an advantage over competitors. This allows the campaigner in question to target each individual with the kind of messaging and advertising that is most persuasive to them.⁸ This process is known as ‘Micro-Targeting’.⁹

The use of personal data for political campaigning has not received the scrutiny that it deserves, in India. For example, the state assembly elections in Bihar featured mass usage of online platforms for campaigning.¹⁰ The importance of this in the electoral space is such that almost every political party now requires a comprehensive database of personal information regarding voters in order to be effective on election day.¹¹ One may even say that now personal data is the primary commodity for those wishing to contest elections.

Therefore, the legal framework for privacy is of great importance for regulating the use of data in elections. While the PDP Bill, 2019 is no more, it is necessary to identify the potential loopholes in the Bill that could have allowed parties to collect data *enmasse* (in large numbers) for their campaigns. Further, it is even more important to highlight the advantages the 2019 Bill had over the current 2022 iteration. The inception of the analysis will focus upon how the 2019 Bill, though not without its shortcomings, remains a far better standard for data privacy laws and its ability to address issues such as microtargeting. However, while noting the primacy of the 2019 Bill over the 2022 Bill in this context, the primary argument is that it would have also been necessary to examine the gaps in the former that required redressal from the perspective of microtargeting and political manipulation.

There has been limited investigation of this in an Indian legal context,¹² even though the conversation on this topic has reached an advanced stage

Doesn't have the "Secret Sauce" it Claims' (*Business Insider*, 21 March 2018) <<https://www.businessinsider.in/tech/theres-an-open-secret-about-cambridge-analytica-in-the-political-world-that-sheds-new-light-on-the-facebook-data-scandal/articleshow/63402917.cms>> accessed 26 September 2021.

⁸ Sandra C Matz and others, 'Psychological Targeting as an Effective Approach to Digital Mass Persuasion' (*Proceedings of the National Academy of Sciences* 2017) <<https://www.pnas.org/content/114/48/12714>> accessed 25 September 2021.

⁹ Ira Rubinstein, 'Voter Privacy in the Age of Big Data' (2014) 5 *Wisconsin Law Review* 861, 882.

¹⁰ Amita Tagore, 'The Digital Campaign', *Indian Express* (New Delhi, 27 October 2020) <<https://indianexpress.com/article/opinion/the-digital-campaign-bihar-assembly-election-6901647/>> accessed 23 September 2021.

¹¹ Nikhil Pahwa, 'The Election Commission of India Needs to Restrict Political Usage of Data' (*Medianama*, 20 June 2019) <<https://www.medianama.com/2019/06/223-the-election-commission-of-india-needs-to-restrict-political-usage-of-data/>> accessed 20 September 2020.

¹² *ibid.*

in other parts of the world.¹³ It is necessary for the Indian legal sphere to address this issue with greater urgency, given the hundreds of millions of Indians who lead active lives online. The question that this paper will seek to address is whether the PDP Bill, 2019, and to a lesser extent the newer version introduced in 2022, provide sufficient protection against mass collection of personal data by political parties and how privacy rights may be shaped to protect against microtargeting. The utility of this exercise is to highlight deficiencies in the now withdrawn Bill that may, hopefully, be addressed in the scheme and provisions of the future data privacy bill that is currently being considered. However, in order to do so, it is also necessary, as touched upon, to point out the numerous ways that the PDP Bill, 2022 is a regression from the earlier model of the Bill.

This paper will attempt to address this question by first providing an overview of the level of digital penetration in Indian society. It will also focus on the increasing usage of data analytics for the purpose of refining campaign advertising by political parties in the country. In this first part, it will conclude with looking at the both the promises and drawbacks of microtargeting in the context of elections.

The second part will go on to examine the state of the law vis-à-vis data privacy in the electoral sphere, in other jurisdictions before examining the problem that inferences pose to proper data regulation and enforcement of data rights in India. In doing so, it will elaborate on how the PDP Bill in 2019 did not sufficiently address the issue of inferences and merely including it under the ambit of personal data in Clause 3(28) of the PDP Bill is insufficient. Clause 3(28) refers to the different forms of data that come under the ambit of ‘personal data’ and lists inferences under it. The protection for such inferences under the 2022 Bill has been negated completely. Clause 2(13) of the PDP Bill, 2022,¹⁴ makes no reference to inferences specifically and reduces personal data to only those forms of data which make a person identifiable. Hence, though flawed, Clause 3(28) of the PDP Bill, 2019, still provided a form of recognition to inferences which has now been done away with entirely.

The third and final part will propose the steps that can be taken, both by the Data Protection Authority that was to be set up under the PDP Bill, and the Election Commission (“EC”), to properly deal with the threat of data collection and political microtargeting. Fundamental to this, will be the

¹³ Normann Witzleb, Moira Paterson and Janice Richardson, *Big Data, Political Campaigning and the Law* (Taylor & Francis 2018) Part 3.

¹⁴ Digital Personal Data Protection Bill 2022, cl 2(13) (“Personal Data Bill 2022”).

need for the DPA to lay out codes of good practice, and for the recognition of the concept of ‘collective privacy’. This part will show that the recognition of “collective privacy” is the most appropriate way to protect constituents and that collective privacy should be incorporated into the revised PDP Bill which is currently being considered.

For undertaking this evaluation, there will be a focus upon the 2019 and 2022 versions of the PDP Bill. These two draft legislations, being drafted and tabled by the Government of India itself, are the most appropriate for analysing the evolution of the focus and thought process behind data privacy law in India. The critiques of the 2019 Bill led to the unveiling of the more recent 2022 iteration. However, as will be elaborated upon, the latest incarnation of the PDP Bill constitutes a decline in the level of protection that is necessary to appropriately address the problem of microtargeting. Conversely, the earlier 2019 Bill, even with its drawbacks, was preferable. Before proceeding, an acknowledgement of the 2018 Draft by Justice B.N. Srikrishna and the Committee of Experts on a Data Protection Framework in India, and the Joint Parliamentary Report in 2021 on the 2019 version of the PDP Bill, is necessary. However, this paper will not discuss these, given that these suggestions while valuable, were never endorsed by the government of India and did not directly address the specific problems of data privacy in the context of elections. In fact, it appears that this particular danger with regard to microtargeting and manipulation of voters during elections has largely evaded attention so far. Consequently, to maintain focus on this specific subject matter, the actual Bills which have been officially tabled and considered by the Government of India, will remain the centre of attention in this paper.

PART I

II. ELECTIONS IN A DIGITAL INDIA

India’s digital presence is significant. Over 400million people are estimated to be owners of smartphones. WhatsApp recorded 487.5 million active users in India as of June 2021,¹⁵ with Facebook recording 329.65 million profiles as of 2022.¹⁶ Comparatively, Twitter has a fairly limited following in India

¹⁵ Statista, ‘Number of WhatsApp Users in Selected Countries Worldwide as of June 2021’ (*Statista*, October 2021) <<https://www.statista.com/statistics/289778/countries-with-the-most-facebook-users/>> accessed 5 November 2022.

¹⁶ Statista, ‘Leading Countries Based on Facebook Audience Size as of January 2022’ (*Statista*, January 2022) <<https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/>> accessed 5 November 2022.

with approximately 23.6 million users in 2022.¹⁷ A large amount of online campaigning utilizes the two former services for information collection and advertising. In the aftermath of the Cambridge Analytica scandal, multiple accusations were made by political parties in India against each other for having exploited Cambridge and similar services.¹⁸ The ability to engage with voters in the online sphere has been shown to play a major role in a party's success.

The COVID-19 pandemic further compelled parties to grow their digital footprint due to restrictions on physical campaigning.¹⁹ Parties which had invested in building their online infrastructure were in a position to take advantage of this. The Bihar election demonstrated the strength of the Bharatiya Janata Party (BJP) in this sphere, where high ranking party members were attuned to online campaigning, unlike their Mahagathbandhan ("MGB") opponents which included the Indian National Congress, Rashtriya Dal, and various Left Parties.²⁰ The MGB moved the ("EC") to restrict the amount that parties could spend on their online campaigns.²¹ This demonstrated the MGB's apprehension regarding the BJP and Janata Dal's expertise in the digital sphere in terms of the resources they had available to harvest data on voters and indulge in micro-targeting.

However, the act of campaigning through microtargeting is merely the final stage of an elaborate process whereby data is harvested and utilised. The important work that is done in the background is obtaining the information regarding voters. The raw data allows analysts to make inferences/predictions regarding the biases and opinions of each voter. The ability to discern the most effective message to sway voters and then send such messages via social media is the object of this exercise. Shivam Shankar Singh, a data analyst who worked directly on a number of political campaigns, went

¹⁷ Statista, 'Leading Countries Based on Number of Twitter Users as of January 2022' (Statista, January (2022) <<https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/>> accessed 5 November 2022.

¹⁸ Yahoo News, 'Congress was Caught in Alliance with Cambridge Analytica, Facebook to Weaponise Data: RS Prasad', *Yahoo News* (New Delhi, 16 August 2020) <<https://in.news.yahoo.com/congress-caught-alliance-cambridge-analytica-115007570.html>> accessed 23 September 2021.

¹⁹ Vijai Laxmi, 'Bihar Elections: Parties Go Full Throttle on Online Prachar for Victory Amid Coronavirus Pandemic', *India TV News* (5 July 2020) <<https://www.indiatvnews.com/politics/national-bihar-elections-2020-congress-bjp-online-campaign-ljp-rjd-631841>> accessed 21 October 2021.

²⁰ Tushar Dhara, 'BJP's Social-Media Dominance is Shaping Mainstream Media Narratives Ahead of Bihar Polls', *Caravan Magazine* (Patna, 3 October 2020), <<https://caravanmagazine.in/politics/bjps-social-media-dominance-is-shaping-mainstream-media-narratives-ahead-of-bihar-polls>> accessed 21 September 2021.

²¹ Amita Tagore (n 10).

as far as claiming that even “Cambridge Analytica...couldn’t dream of this level of targeted advertising.”²²

There are multiple forms of information regarding people. Some may be considered intrinsic to people, such as their gender, sex, religion, and financial status. These kinds of information would have fallen under the definition of ‘sensitive personal data’ under the PDP Bill, 2019. However, even innocuous information which would not be considered ‘personal data’ under the 2019 Bill, are important data points for drawing inferences. In the context of both sensitive personal data and seemingly innocuous non-personal data, the PDP Bill, 2022, takes two significant steps backward. The former, sensitive personal data, no longer finds any place in the newly proposed Bill.²³ Further, Clause 2(13) of the new Bill is inadequate for addressing the dangers that even harvesting of non-personal data pose, given that it classifies personal data as only those kinds of data that can lead to identification of the data principal.

Singh elaborates on how data like electricity bills help determine the overall economic profile of different areas.²⁴ A household with high electricity bills would lead to an inference of high economic status with its attendant social attitudes and tastes. In this manner, evaluations can be made regarding the type of online advertising is most visible to such individuals, and what issues are of greatest importance to them. This is a stark example of exactly the kind of data that Clause 2(13) of the new PDP Bill, 2022, fails to engage with. Such forms of data, whether they can lead directly to identification of an individual or not, can still be sufficient to draw inferences about them and subject them to microtargeting.

In this manner, effective data collection teams can allocate individuals into different groups and infer the political preferences of each group. Singh uses the example of non-Yadav Other Backward Classes (‘OBC’) voters in Uttar Pradesh.²⁵ Through gathering both personal data like their age, sex, and education level, along with other innocuous bits of data such as electricity bills, a highly personalized profile can be created for each non-Yadav OBC. In this manner, a seemingly amorphous and diverse collection of

²² Shivam Shankar Singh, *How to Win an Indian Election: What Political Parties Don’t Want you to Know* (Penguin Books 2019) 76.

²³ Nivedita Krishna, ‘Digital Personal Data Protection Bill 2022: How it has Left Both Civil Society and Industry Body Shell Shocked’ *The Times of India* (29 November 2022) <<https://timesofindia.indiatimes.com/blogs/niveditas-musings-on-tech-policy/digital-personal-data-protection-bill-2022-how-it-has-left-both-civil-society-and-industry-body-shell-shocked/>> accessed on 3 December 2022.

²⁴ Shankar Singh (n 22) 64, 74.

²⁵ Shankar Singh (n 22) 75.

people can be allocated into a group for campaigning purposes.²⁶ A highly targeted message can be communicated to only these individuals, through social media and online advertising, regarding the issues that matter to them the most.

Apart from the fact that parties are able to advertise their messages this way, the other important aspect of online campaigning is that not every party can effectively use this resource. Singh elaborates on how the BJP used data collection and targeted campaigning in the Tripura Assembly elections of 2018.²⁷ He notes that the incumbent Communist Party of India (Marxist) [‘CPI(M)’], did not have the resources to make the kind of promises the BJP was able to during the election campaign. More importantly, the CPI(M) did not possess the vast amounts of data regarding their constituents that the BJP did. This example demonstrates how even a relatively significant political party such as the CPI(M) lags behind in terms of adoption of technologically supported methods of campaigning. As significant and major parties become more attuned to the advantages of this approach, the importance of regulating their activities will increase.

The sources from which data was collected is also worth noting. The PDP Bill, 2019 created an exception to the notification requirement when the information is already public under Clause 14(2)(g)²⁸, which implies that such information may be harvested freely and without any accompanying disclosure or attainment of consent. An example of information that is already public is the rolls of the EC.²⁹ Further, the BJP developed mobile applications, independently or in conjunction with private parties, which required information such as name, sex, religion, and so on, from those who downloaded them.³⁰ Importantly, Singh notes that none of these actions undertaken by the BJP were illegal.³¹ The lack of any legal regulation accentuates the need for a governing law that addresses these activities. Under the new 2022 Bill, various forms of data may not even qualify as personal data to begin with, given the truncated nature of Clause 2(13) of the Bill. Hence, the question of notification would likely not arise at all. As already noted above, data which does not cross the threshold of Clause 2(13) would be sufficient to create a profile of large swathes of people for targeted advertising.

²⁶ *ibid*; William A Gorton ‘Manipulating Citizens: How Political Campaigns use of Behavioural Social Science Harms Democracy’ (2016) 38(1) *New Political Science* 61.

²⁷ *ibid*.

²⁸ Personal Data Protection Bill 2019, cl 14(2)(g) (“Personal Data Bill”).

²⁹ Pahwa (n 11).

³⁰ Shankar Singh (n 22) 127, 140-146.

³¹ *ibid*.

III. DRAWBACKS OF DATA ANALYTICS IN ELECTIONS

Modern data analytics has made online political microtargeting into a form of behavioural advertising. Behavioural advertising, used in large part by commercial entities like Big Tech companies, tracks users' online activity to market specific ads.³² This form of advertising has its own benefits and drawbacks. The question of balancing the two is difficult, however, considering the dynamic way in which microtargeting keeps evolving and because the new ways in which data is harvested from different sources opens up further possibilities of the kinds of targeted messages that could be sent to consumers.

There are certain advantage/benefits to microtargeting. It is often useful to mobilize a portion of the electorate which may not be politically active by sending them direct and targeted messages,³³ and is also advantageous for nascent and up-coming political parties, given it is a cheap and easy way to broadcast their message to compete with more established parties in the initial stages of its existence at the local level.³⁴ However, this requires sufficient technological prowess and efficiency, as well as a basic amount of data regarding the social and economic make-up of the constituency in question. As may be evident, when elections transition from the local level to a larger stage, the expenses related to undertaking this become more onerous. Hence, this potential benefit of microtargeting for smaller parties is, in any case, swiftly eroded. Regardless, of the possible benefits of microtargeting, the dangers of such online advertising have been demonstrated amply in recent times. The Cambridge Analytica scandal was the highest profile of these, but by no means the only one. The threats of microtargeting can be roughly allocated under two headings: a) manipulation of voters; and b) violations of privacy.

In the context of manipulation, parties can maximise the turnout of constituents who are in favour of their stand. Conversely, they can use ads to dissuade constituents who prefer their opponents through 'dark campaigning'. Dark campaigning is a form of campaigning that informs voters about the negative aspects of their opposing parties, rather than providing positive

³² Joseph Turow, *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth* (YUP 2011); Frederik Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer 2015).

³³ Holt Kristoffer and others, 'Age and the Effects of News Media Attention and Social Media Use on Political Interest and Participation: Do Social Media Function as Leveller?' (2013) *European Journal of Communication* 19, 19-20.

³⁴ European Parliamentary Research Service, *Social Media in Election Campaigning* (Briefing, 21 March 2014, <[https://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140709/LDM_BRI\(2014\)140709_REV1_EN.pdf](https://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140709/LDM_BRI(2014)140709_REV1_EN.pdf)> accessed 15 October 2021).

messages regarding policies.³⁵ This can also include disinformation or half-truths to distort the image of opposing parties. The Donald Trump campaign in the 2016 US Elections was accused of using this strategy among African Americans. Using targeted ads, the Trump campaign was alleged to have shown African Americans ads about Hillary Clinton where she refers to them as “super predators” and “serial sexual harassers”.³⁶ This discouraged African American turnout at the elections. Even if these constituents would not have voted for Trump, the objective was to ensure they did not vote for Clinton either, thus reducing her vote share.

Parties could also purport to prioritise the singular issue that is most important to each individual voter. This may even be entirely contradictory issues.³⁷ Taking the example of tribal people in Tripura, a party may target them with messaging that claims the economic and social upliftment of them as being their most important issue. At the same time, it could target other portions of the population by stating that development of forest and tribal areas for industry is the focus of the party. Clearly, these two stances are in conflict, as using the forest for industrial purposes is against the interests of the tribal population. Considering that the ads are only being shown in a targeted manner, they are hidden from the constituency which has received the directly contradictory promise.

This also misleads the electorate regarding how important an issue is to a political party.³⁸ Microtargeting creates an illusion that a particular party is completely devoted to a specific issue because that class of voters receives information and advertising that is targeted. These multiple promises to multiple people create a dissonance for both the electorate and the parties themselves. As different pledges have been made to different groups, a party might then struggle to determine which issue is of greatest importance.³⁹ Additionally, even though the marketplace of ideas benefits in some ways from this form of campaigning, it also creates significant fragmentation in the public conversation. The marketplace becomes multiple markets where

³⁵ Gorton (n 26).

³⁶ Joshua Green & Sasha Issenberg, ‘Inside the Trump Bunker, With Days to Go’ *Bloomberg* (27 October 2016) <www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go> accessed 18 October 2021; McKenzie Funk, ‘The Secret Agenda of a Facebook Quiz’ *New York Times* (New York, 19 November 2016) <www.nytimes.com/2016/11/20/opinion/the-secret-agenda-of-a-facebook-quiz.html?_r=0> accessed 21 October 2021.

³⁷ Borgesius (n 32) 87.

³⁸ D Sunshine Hillygus and Todd Shields, *The Persuadable Voter: Wedge Issues in Presidential Campaigns* (YUP 2008) 14.

³⁹ Borgesius (n 32) 88.

individuals do not visit other markets as the information that matters to them is provided directly to them through microtargeting.⁴⁰

In terms of the privacy violations that occur as a result of this, the actual collection of data has already been elaborated upon.⁴¹ But the other primary issue is the passing on of data to third parties by an otherwise reputed fiduciary. The argument used by most individuals regarding not bothering with their privacy in the context of Facebook and other such companies is based on trust. People believe that giving their personal data to reputed companies is acceptable as it will not be misused. However, the indirect collection of data by other malicious third parties like Cambridge Analytica or others, is a risk that should be given greater consideration. This is especially a risk when multiple private parties are entrusted with doing different aspects of data collection.⁴²

Microtargeting can, therefore, expose the political process to both good and bad. As a result, its regulation cannot merely be confined to data privacy law, though it must be of primary importance. Election laws must also take cognizance of data privacy issues and work in tandem with privacy regulations to ensure the greatest degree of protection. The next part of the paper will look into election and data privacy laws across the world, before commenting on how the Representation of Peoples Act, 1951 can incorporate privacy concerns into its ambit.

PART II

IV. DATA PRIVACY IN ELECTIONS AND INDIAN ELECTION LAWS

The dangers related to lack of regulation of data mining in the context of political campaigns and elections has witnessed increased recognition.⁴³ This new found awareness had led to an acknowledgment that there must be specific guidelines in place for political parties rather than reliance on general data privacy law. As Clause 50 of the PDP Bill, 2019, allowed the DPA to frame such guidelines for different industries, this responsibility must be taken up, as will be elaborated upon later. Under the 2022 Bill, however, the power to frame such guidelines seemingly does not vest with the DPA

⁴⁰ *ibid.*

⁴¹ Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (OUP 2015).

⁴² *Borgesius* (n 32) 87.

⁴³ *Normann Witzleb* (n 13).

any more. Clause 20, which lists the powers of the DPA does not include the framing of guidelines⁴⁴, and instead, grants the discretion to issue Rules under the Bill to the Central Government under Clause 26.⁴⁵ Further, data privacy laws must be synthesized with election laws to ensure they complement each other in addressing the specific challenges that arise. The responsibility to protect data and electoral integrity must be apportioned between both the EC and the DPA.

The EC under Section 123(2) of the Representation of Peoples Act, 1951, permits restriction of corrupt practices, which includes multiple forms of speech. While there is, obviously, no jurisprudence whatsoever on the point of whether data mining can be considered a corrupt practice, a case could be made for its inclusion. The Supreme Court had termed “undue influence” as being anything which reduces the free will of the electorate to the extent that the individuals have almost no choice.⁴⁶ However, the standard has subsequently been expanded wherein covering up important details such as criminal antecedents of a candidate amount to unduly influencing constituents.⁴⁷ Importantly, the Supreme Court has also maintained that the threat of violence is not necessary for Section 123(2) to be violated.⁴⁸

On this basis, microtargeting could be considered a form of undue influence. The most effective usage of this provision would be to tally it with data privacy. Thus, a breach of data privacy laws would create a presumption that there had been violations of privacy which give rise to undue influence. This is because of the difficulty associated with conclusively proving that microtargeting has had a particular threshold level of influence on constituents. If such an inference is drawn, the determination of undue influence would not be a purely subjective determination but rather be premised on whether the party has adhered to data privacy requirements. Thus, breaches of data privacy law, and the practice of microtargeting using this data, may cumulatively create a presumption that the practice of a party has been acted in a manner that has unduly influenced the voters in an upcoming election. The fact that the Supreme Court departed from the “no free choice” standard and classified certain actions or omissions as automatically amounting to undue influence, allows for this. This would form a strong deterrent against parties attempting to skirt data privacy laws.

⁴⁴ Personal Data Bill 2022, cl 20.

⁴⁵ *ibid*, cl 26.

⁴⁶ *Shiv Kirpal Singh v V.V. Giri* (1970) 2 SCC 567.

⁴⁷ *Krishnamoorthy v Sivakumar* (2015) 3 SCC 467.

⁴⁸ *ibid*.

What is more important, however, is to now examine the PDP Bills, both 2019 and 2022, and its relevance to elections. While election laws may play an important role at deterring microtargeting, the stage at which the manipulation of voters begins is via mining and usage of data to profile constituents. The preliminary conclusion that is evident from this, as will be elaborated upon subsequently, is that no single statute or authority will be able to adequately address the entire spectrum of issues that arise in the context of data collection and microtargeting. This paper will now turn to the analysis of this dilemma by starting with an examination of the provisions of both PDP Bills.

V. DETAILS OF THE DATA PROTECTION BILL

The withdrawn PDP Bill, 2019, was based largely from the most comprehensive data privacy legislation in the world at present, the General Data Protection Regulation (“GDPR”). Thus, several provisions mirror the contents of the GDPR.⁴⁹ For example the definition of “Personal Data” provided under Clause 3(28) of the PDP Bill contains the same wording as the GDPR equivalent, with one important distinction.⁵⁰ The PDP Bill includes “inferences” under the ambit of personal information, unlike the GDPR. This is a lacuna in the GDPR which has been commented on negatively by scholars.⁵¹ The importance of inferences is that the raw data which is accumulated is often of less importance than the inference derived from it as a result. On the face of it, classifying inferences as personal data is valuable, as it provided individuals with the full ambit of rights associated with personal data under the PDP Bill, 2019. However, this lacuna which had correctly been addressed in the 2019 Bill has now been removed in the 2022 Bill. Rather than a helpful step, this is a significant regressive move in the development of the Bill.

Clause 3(13) of the PDP Bill, 2019 defined Data Fiduciaries as individuals, the state, or juristic entities (which includes political parties) that accumulate personal data.⁵² Chapter II of the 2019 Bill outlined the obligations of Data Fiduciaries. Clause 4 restricts the collection of personal data except for

⁴⁹ Anirudh Burman, ‘Will a GDPR-Style Data Protection Law Work for India’ (*Carnegie India* 15 May 2019) <<https://carnegieindia.org/2019/05/15/will-gdpr-style-data-protection-law-work-for-india-pub-79113>> accessed 25 September 2021.

⁵⁰ Personal Data Protection Bill, cl 3(28).

⁵¹ Sooraj Shah, ‘This Lawyer Believes GDPR is Failing to Protect You – Here’s What She Would Change’ *Forbes* (30 January 2019) <<https://www.forbes.com/sites/soorajshah/2019/01/30/this-lawyer-believes-gdpr-is-failing-to-protect-you-heres-what-she-would-change/>> accessed 24 September 2021.

⁵² Personal Data Bill cl 3(13).

lawful purposes.⁵³ While there are no laws which restrict political parties from collecting personal data, they would still abide by the restrictions under the PDP Bill, alongside respecting the rights of Data Principals. Clause 5 restricts the usage of collected data for stated purposes. However, Clause 5(b) truncates this protection by allowing the data to also be used for which “...is incidental to or connected with such purpose, and which the data principal would reasonably expect...”.⁵⁴ The party which is in power may have access to far more data than its competitors, given that it processes data for various purposes related to administration of government. Clauses such as 5(b), and Clause 12 which grants the ability to process data without consent, could be misused by a ruling party to gain an advantage.

In the 2022 Bill, there are various troubling provisions in respect of how Data Fiduciaries can now collect data. Clause 8 which deals with “deemed consent” forgoes the consent of the data principal entirely.⁵⁵ While not all the sub-clauses are unusual or potentially harmful, there exists the possibility of abuse in respect to certain instances of deemed consent, such as with sub-clause (2).⁵⁶ Further, instead of an exemption from notification, Clause 8(8) (f) now merely presumes consent in the case of publicly available data about an individual, such as information from electoral rolls that parties can easily access.⁵⁷ Further, Clause 8(9) outlines a vague notion of deemed consent for any “fair and reasonable” purpose as may be prescribed, after consideration of certain conditions within the sub-clause.⁵⁸ All these provisions, in the background of the overall watering down of the definition of “personal data” under Clause 2(13), provide significant leeway for collection of data from which to draw inferences.

With regard to the DPA which was constituted under Clause 41(1) of the PDP Bill, 2019 it is entrusted with carrying out a number of functions.⁵⁹ The most important of these functions in the context of elections is the power to lay down codes of best practice for different industries under Clause 50.⁶⁰ As already mentioned, this power seemingly no longer vests with the DPA at all. Regardless, even if the 2019 Bill was taken as the benchmark, one preliminary issue associated with the DPA’s functions is that it seems to clearly be aimed toward commercial entities. The penalties under Chapter X seem to

⁵³ *ibid*, cl 4.

⁵⁴ *ibid*, cl 5(b).

⁵⁵ Personal Data Bill, 2022, cl 8.

⁵⁶ *ibid*, cl 8(2).

⁵⁷ *ibid*, cl 8(8)(f).

⁵⁸ *ibid*, cl 8(9).

⁵⁹ PDP Bill 2019 cl 41(1).

⁶⁰ *ibid*, cl 50.

be aimed at the turnover of commercial entities, presumably, because that is the primary objective of such Data Fiduciaries.⁶¹ While, as mentioned already, the definition of a Fiduciary could *prima facie* apply to parties, the reliefs provided seem to be oriented more toward commercial entities.

The 2022 Bill under Clause 19 refers to setting up the DPA.⁶² While the Chapter on criminal penalties has been excluded in the 2022 Bill, the civil penalties provided under Clause 25 read with Schedule 1 remain seemingly focused on commercial entities.⁶³ Hence, this overall approach of the Bills, no matter which version, appears to remain fixated with the dangers of collection and processing of data by commercial entities, but not by political actors. This facet appears to have been overlooked.

Clause 7 of the 2019 Bill outlined the obligation of Data Fiduciaries to inform the Data Principals about the collection of their data, along with other forms of information collected, in the notification, that must be issued as mandated by the Clause. However, a caveat in this provision exists in the form of data collected from a source other than the Data Principal itself. If the data is accrued from a third-party source, the notification needs to only be done “...as soon as reasonably practicable...”.⁶⁴ There is no indication of what this “reasonable” period might be. Also of note, is Clause 7(b) requires only the “nature and categories” of data be notified to the Principals, and not necessarily the exact content of said data.⁶⁵ Hence, a category of data may include credit or financial information regarding the Data Principal, but would not necessarily include what kind of information in this category, such as outstanding loans or scheduled payments, have been harvested. The processing of personal data can be done without consent for reasons provided under Chapter III, such as under Clause 12 which exempts notification for effectuating laws or orders of a Court⁶⁶, or under Clause 13 which provides the same exemption when it comes to information required for employment purposes.⁶⁷ In Clause 14(2)(g), data which is publicly available may be collected and processed without seeking permission from the Data Principal.⁶⁸

The 2022 Bill refers to roughly the same obligations that existed for Data Fiduciaries under the 2019 Bill. Chapter 2, from Clauses 5 to 11, outlines the

⁶¹ *ibid*, ch X.

⁶² Personal Data Bill 2022, cl 19.

⁶³ *ibid*, cl 25; Sch 1.

⁶⁴ PDP Bill 2019 cl 7.

⁶⁵ *ibid*, cl 7(b).

⁶⁶ *ibid*, cl 12.

⁶⁷ *ibid*, cl 13.

⁶⁸ *ibid*, cl 14(2)(g).

various requirements that Data Fiduciaries and Significant Data Fiduciaries must adhere to while carrying out their activities.⁶⁹ Within these provisions, various implicit exceptions to the requirement of consent from Data Principals have been incorporated. Clause 9(9) of the 2022 Bill allows Data Fiduciaries to transmit data to each other when it has been obtained via consent from the Data Principal already.⁷⁰ The notice requirements have become somewhat vaguer than they had been under the first iteration of the Bill in 2019. Clause 6(1) refers to providing an “itemised list” of data that is sought to be obtained from the Data Principal, without any indication as to how specific these “items” need to be.⁷¹ The discretion that appears to be vested in a Data Fiduciary may be misused.

The rights of the Data Principals are located under Chapter V. These rights include the Right to Access data collected by the Fiduciary⁷², the Right to Correction⁷³ and the Right to be Forgotten.⁷⁴ Clause 21 directs the Data Principal to request a Data Fiduciary to comply with any of the rights provided under Chapter V, in case they find that there is a breach of the rights provided. However, Clause 21(4) allows a Data Fiduciary to refuse compliance, with reasons provided in writing. The Data Principal may then appeal to the DPA.⁷⁵ Several of the same rights are transposed onto the PDP Bill, 2022, however, certain anomalous additions have also been made in Clause 16, which deals with duties of Data Principals. These inclusions abrogate the rights under Chapter 3. Specifically, Clause 16(2) states that a Data Principal “shall not register a false or frivolous claim” against a Data Fiduciary.⁷⁶ It is entirely unclear what counts as a “false or frivolous” claim, and the need to include such wording in the Bill itself is questionable. Undoubtedly, had the claim been false or frivolous, it would have been dismissed via the judicial process. Instead, the inclusion of an explicit duty under Clause 16 is likely to have a chilling effect on Data Principals exercising their data rights. In the alternative, it could even lead to counter claims made by the Data Fiduciary against the Data Principal on the ground that the objections raised by the latter, come under the category of “false and frivolous”.

There are other exemptions which are of importance in the context of data collection by political parties or their agents. An example of such an

⁶⁹ Personal Data Bill 2022, ch 2.

⁷⁰ *ibid*, cl 9(9).

⁷¹ *ibid*, cl 6(1).

⁷² PDP Bill 2019, cl 17.

⁷³ *ibid*, cl 18.

⁷⁴ *ibid*, cl 20.

⁷⁵ *ibid*, cl 21(4).

⁷⁶ Personal Data Bill 2022, cl 16(2).

exemption that could be exploited is Clause 38 of the PDP Bill, 2019, which allowed processing of Personal Data for statistical and/or research purposes. An entity may process this data, claiming that it falls under Clause 38, but then use the research that it does to engage in micro-targeting.⁷⁷ This problem is accentuated by the fact that there is no requirement for these actors to specify what type of statistical work or research they are undertaking. A similar provision, Clause 18(2)(b), has been retained in the 2022 Bill.⁷⁸ The Central Government also has power to exempt Data Fiduciaries from the entire ambit of Chapter 2 of the PDP Bill, 2022, based on “volume and nature of personal data processed”. What this implies is not clarified and the threshold in terms of “volume” and genus of personal data in terms of “nature”, which could lead to such wide-ranging exemptions, is not even hinted at. Many of these provisions, both in the 2019 and 2022 versions of the PDP Bill, are relevant for the question that will be addressed now which is how effectively each of the Bills deals with inferences. It will be argued that even under the more favourable regime of the 2019 Bill, categorizing inferences as personal data does little to address the specific issues that such inferences pose for data privacy in an electoral context.

VI. INFERENCE, ELECTIONS, AND THE PDP BILL

The regulations of inferences have increasingly been seen as crucial for ensuring adequate protection of data. Inferences as the subject of data protection presents a unique set of issues which are different to other types of data. The reasons for this, and the consequences that this has for guaranteeing data rights, will now be elaborated upon, in the context of multiple provisions of the PDP Bill, 2019, as it was. Considering the similarities between the GDPR and PDP Bill, 2019, the jurisprudence and experiences under the former will be used to analyse the potential problems that may arise in India. This will also be helpful, to an extent, in the context of the 2022 Bill given some of its provisions remain similar to those that existed under the 2019 Bill.

Status of Inferences under the GDPR and PDP Bill

One of the acknowledged flaws in the GDPR was its failure to include inferences under the ambit of personal data.⁷⁹ In Europe, there has been an

⁷⁷ PDP Bill 2019, cl 38.

⁷⁸ Personal Data Bill 2022, cl 18(2)(b).

⁷⁹ Sandra Wachter and Brent Mittelstadt, ‘A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI’ 20192 Columbia Business Law Review 494; Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN WP136 (20 June 2007).

increasing recognition in legal policy circles that inferences should also be addressed in the GDPR. For example, the Article 29 Working Party, an advisory body comprised of representatives from the data protection authorities of each EU Member State, the European Data Protection Supervisor, and the European Commission, has noted that inferential analytics, the process by which inferences are drawn from data, do the actual harm to individuals in the context of privacy breaches.⁸⁰ The focus of data privacy law is usually at the stage of inputs or when the data is collected. Of equal importance, is the output generated as a result of those inputs. These outputs are the basis for actions taken in the real world regarding that person. The outputs, which are inferences, require greater regulation under the law.⁸¹

The PDP Bill, 2019, *prima facie* addressed this concern by including inferences under personal data in Clause 3(28). This is similar to the California Consumer Privacy Act, which also classifies inferences as part of “personal information” under Title 1798.140, and is then accorded protection of various forms under the Act.⁸² However, in the context of the PDP Bill, 2019, in actuality, the inclusion of inferences under personal data in Clause 3(28) did little to address the issues associated with inferences. The difference between inferences and other data points is the subjectiveness and non-verifiable nature of the former.⁸³ What this means is that inferences, although based on objective facts about a Data Principal, are subjective to the extent that an evaluator draws their own subjective conclusions based on those facts. Inferences, by their nature, are derived from objective facts or data that is accumulated about the Data Principal. This inference is, essentially, an opinion that must be subjective and based on the evaluator’s personal metrics of judgment.⁸⁴ Such inferences are non-verifiable in nature given this subjectivity. This presents problems in terms of the ambit of rights that can be enforced regarding non-verifiable inferences.⁸⁵ Such non-verifiable inferences are inherently based on the judgment of the individual or entity making the evaluation of the Data Principal. It is not possible to test such subjective inferences or establish their “correctness” given that the discretion of the evaluator is built into the inference and final decision that is made.

The act of making an inference from raw data presents two separate issues for data privacy law. The first is the metric by which the inference is made.

⁸⁰ Art 29 Data Protection Working Party (n 79).

⁸¹ Wachter and Mittelstadt (n 79) 4-6.

⁸² Title 1798.40, Title 1.81.5 California Consumer Privacy Act of 2018.

⁸³ Art 29 Data Protection Working Party (n 79).

⁸⁴ *ibid.*

⁸⁵ *ibid* 8.

The process, criteria, or algorithm in the case of automated decision making, is the metric used by the Data Fiduciary to make an evaluation. This process is what leads to the conclusion. For example, banks use multiple criteria to determine to determine if an individual has a satisfactory credit score and is eligible to receive a loan.⁸⁶ The raw data about the applicant is put into the system to reach the final inference.

This metric has an important effect on the final inference. The Article 29 Working Group has advocated the inclusion of both inferences and the underlying metric used to reach the inference under the ambit of “personal data” under the GDPR. European case law shows that this interpretation has been partially taken into account. Even though the GDPR does not categorize inferences as personal data⁸⁷, the ECJ has included it regardless. It noted that the assessments or evaluations of individual will lead to a decision being made that affects him/her. Therefore, it is appropriate to include this under “personal data” and afford it the protections in the GDPR.⁸⁸

However, the second issue that arises is that for an inference to be considered personal data, it must be a “verifiable” inference. While India had already crossed the initial threshold of defining inferences as personal data by including it in the PDP Bill, 2019, the verifiability question has further implications. An inference that is based primarily on a subjective metric or criteria would be difficult to “correct” under Clause 18.⁸⁹ A subjective opinion regarding a person’s credit score, for example, cannot logically be open to “correction”. Ultimately, it is within the bank’s own subjective determination whether an applicant has demonstrated reliability in terms of paying back a prospective loan.

Thus, there is essentially no difference between the position in Europe and under the PDP Bill, 2019. The 2019 Bill included inferences under personal data, and the ECJ has also extended the definition of personal data to include inferences, depending on verifiability of the inference. While verifiability did not matter under the 2019 Bill, other attendant issues with inferences as personal data will still apply, such as accuracy of the decision-making process and the fact that certain rights, such as the aforementioned Right to Correction under Clause 18, may not even be available for inferences. These issues will now be expanded upon.

⁸⁶ *ibid.*

⁸⁷ Joined Cases C-141 and 372/12 *YS, M and S v Minister voor Immigratie, Integratie en Asiel* [2014] ECR I- 2081 para 40 (Cases preceding the GDPR also follow this principle).

⁸⁸ Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECR I-994 para 60.

⁸⁹ *ibid* 34, 42-44.

In this context, while there were improvements that may have been brought to the treatment of inferences under the 2019 Bill, the fact that they were explicitly mentioned as “personal data” was a positive step. This entire discussion is now negated by the latest 2022 Bill, which ignores inferences entirely. The removal of inference from the umbrella of “personal data” constitutes a regrettable omission and the 2019 Bill remains a better starting point on this aspect than the latest version which is being considered.

Application of Data Principals’ Data Rights to Inferences

The reasons or the criteria on which a subjective inference is drawn regarding a Data Principal is also not included as personal data under the PDP Bill, 2019, nor under the 2022 Bill given its shrunken definition of personal data. After objective facts and data are collected about a Data Principal, there will often be a set of guidelines or criteria which will be applied to those facts, and which will give rise to final inference made about the Data Principal. Under the GDPR, there have been arguments made to include these criteria/guidelines under the ambit of “Personal Data”. However, there are indications from the interpretation of the GDPR that it may be left out.⁹⁰ For this exercise, we may take the assistance of how the GDPR, in the same context, has been interpreted. This is, evidently, because the GDPR and PDP Bill, 2019 had significant similarities and there is no jurisprudence under the latter. While this does not, of course, mean the PDP Bills, 2019 or 2022, would have been interpreted by Indian Courts in the same manner, this similarity may assist in providing us with important indicators in this regard. Further, as already mentioned, the lack of any interpretation of the provisions of the Bill, due to it having not come into force, would make any consideration of alternatives purely speculative. For carrying out this comparison and estimation of how data privacy rights may develop, the provisions of the 2019 Bill will be utilized.

The ECJ while interpreting the GDPR has made clear that, in its view, the purpose of data privacy law is not to provide transparency in the decision-making process by which an inference is made.⁹¹ The end result i.e., the inference may be personal data under certain circumstances but not the rationale or analysis behind the inference. The drawback of this is that it removes an avenue of inquiry for a Data Principal. In the context of an unverifiable or subjective inference, one of the means of challenging it or seeking a correction could have been that the criteria of evaluation is flawed.

⁹⁰ *ibid* 57.

⁹¹ Joined Cases C-141/12 & 372/12 (n 86) paras 45–47; Case C-28/08 *P European Comm’n v Bavarian Lager* [2010] ECR I-06055 para 49.

A similar problem is faced in the context of the Right to Access under Clause 17 of the PDP Bill, 2019. If the ECJ's interpretation of the ambit of personal data is taken as a proxy for what it could be under the PDP Bill, the process/criteria for making the inference cannot be accessed by the Data Principal. The Article 29 Working Group has disagreed with this approach and included the method of evaluation under the ambit of the GDPR.

What is evident from this is that the rights under the PDP Bill, 2019, would not have been applied equally across all scenarios. Wachter & Mittelstadt note that the *telos* (end term of a goal-directed process) of different spheres of activity will shape the way data privacy rights are applied.⁹² In certain scenarios, such as the bank's credit score, certain rights may not be available at all, such as the Right of Correction.⁹³ This is because, in the context of giving an individual a credit score, the individual is asking to be evaluated. Therefore, the individual would not have the right to correct that evaluation, unless it is shown that there was a mistake in recording the data points or inputs. This also falls in the category of a "non-verifiable" inference, as already alluded to earlier.

In regard to a non-verifiable inference, the 2022 Bill takes yet another turn for the worse. Clause 16(4), which lists out the mandatory duties of a Data Principal, explicitly precludes a Principal from even asking for Correction or Erasure of their data under Clause 13, unless the data is "verifiably authentic".⁹⁴ The ambit of this phrase is nebulous and leaves much to imagination. A "non-verifiable" inference in this context, may arguably have been excluded entirely from the scope of the rights of a Data Principal under Clause 13 of the PDP Bill, 2022. As the analysis earlier shows, this is particularly dangerous in the context of inferences given that many are, by nature, "unverifiable". However, under the PDP Bill, 2019, there had not been any explicit bar on seeking a correction or erasure of an inference, as difficult as actually doing so may have been in practical terms. This was further enabled by the fact that inferences were recognized out rightly as Personal Data under Clause 3(28). However, even that limited scope for interference has been completely closed off by the PDP Bill, 2022.

Regardless, even if we were to take the 2019 Bill as the benchmark, certain issues would persist. When looked at in this teleological context, the way by which rights under the PDP Bill, 2019, may have been applied to

⁹² *Peter Nowak v Data Prot. Comm'r* [2017] ECR I-994, Case C-434/16, Opinion of Advocate General Kokott, paras 35, 53.

⁹³ Wachter and Mittelstadt (n 79).

⁹⁴ Personal Data Bill 2022, cl 16(4).

micro-targeting and election campaigning would have been curbed. To begin with, the Right to Correction may not be available as parties are making their own determination of what they need to say to a particular electorate. Looking back to the example of non-Yadav OBC's, the party in question determines what is most effective to build support for itself. Considering this touches on the freedom of a party to conduct its election campaign and decide strategy for itself, a Data Principal may not have the Right to Correct an inference made about himself.⁹⁵

Further, the inferences made may be unflattering or embarrassing to a Data Principal, but may still in fact be the best way to win their vote. A Data Principal may consider himself to be liberal or left-leaning, but his data may indicate policy leanings which are more associated with conservative positions. Positions taken by any individual are complex and often overlap onto both sides of the political spectrum in terms of both Right- and Left-Wing parties. The inferential analytics of a political party may lead to the conclusion that appealing to the individual's conservative positions is more effective. This might contradict the way the Data Principal self-identifies but self-identification often depends on social pressure and peer groups. For getting the Principal to vote for it, a party is unconcerned with such technicalities.

This goes back to the problem with inferences and the reason why a simplistic inclusion of it under Clause 3(28) would not have solved the problem. The PDP Bill, 2019 was ill-suited to determine whether the inference reached about a Data Principal is accurate or not. One cannot use the standard of what the Data Principal itself determines to be accurate. The consequence of this would be that all individuals would always flag any unflattering inference about them as "inaccurate", and demand its correction. In the context of powerful individuals in society, this problem is especially pronounced. It would be unbecoming of data privacy law to allow individuals to alter all negative inferences made about them.

Inferences and Rights of the Data Fiduciary

The Data Fiduciary may have itself have rights which conflict with the rights provided under the PDP Bills, both 2019 and 2022. The method or criteria of assessment may be part of the Data Fiduciary's own right to privacy as the metrics may be unique. In different contexts, the privacy rights of companies and juristic entities has been acknowledged in India, though the full ambit

⁹⁵ Opinion of Advocate General Kokott (n 92) para 56.

of rights under *Puttaswamy* do not seem to have been extended to them.⁹⁶ The Data Fiduciary, understandably, would not want to reveal the criteria which was used to make the decision as it would then be open to scrutiny by competitors. Another possible restriction may be other laws in the country itself. It has been increasingly understood that information and data form a commodity in and of itself. A private company which is entrusted with doing the collection for a party, may use Intellectual Property Laws to protect against needing to make disclosures.⁹⁷ Trade Secrets under Intellectual Property could be a ground taken by a private company to claim that revealing data would prejudice their competitive position vis-à-vis other companies offering the same services.⁹⁸ While data has not been explicitly recognized as a commodity, capable of protection under Intellectual property or competition law, other jurisdictions have recognized this possibility and included data protection under Trade Secrets within the ambit of IP.⁹⁹

This applies in an electoral context, and not just in a commercial setting between two business competitors. The BJP's methods of categorizing different people into groups which is the basis of inferences made about them, may be of great importance for campaigning. The competitive advantage of any party in this sphere would, undoubtedly, be something they wish to maintain. The Right of Correction is similarly impacted. It can be argued that a party has a right to make its own evaluation regarding the tastes and preferences of voters. This could especially be the case if, as the ECJ stated, the purpose of data protection law is not to evaluate the "correctness" of decisions except in limited scenarios.

Thus, the balancing of the rights of Data Principals with the rights of Data Fiduciaries is necessary. The former is detailed in both the PDP Bills,

⁹⁶ Lomesh Nidumuri and Tejas Shetty, 'India: Right to Privacy of Companies Vis-à-Vis the Powers of the Central Government under Section 206(5) of the Companies Act, 2013 – Has the Balance Been Lost?' (*Mondaq*, 15 May 2020) <<https://www.mondaq.com/india/privilege/934460/right-to-privacy-of-companies-vis-a-vis-the-powers-of-the-central-government-under-section-2065-of-the-companies-act-2013--has-the-balance-been-lost-#:~:text=INDIAN%20LAW%20ON%20THE%20INTER,AND%20DOCUMENTS%20OF%20A%20COMPANY&text=The%20recent%20judgment%20of%20the,of%20the%20Constitution%20of%20India>> accessed 7 October 2021.

⁹⁷ Wachter and Mittelstadt (n 79) 55.

⁹⁸ *John Richard Brady v Chemical Process Equipments (P) Ltd* 1987 SCC OnLine Del 236; AIR 1987 Del 372; *Ambiance India (P) Ltd v Naveen Jain* 2005 SCC OnLine Del 367; (2005) 122 DLT 421.

⁹⁹ Gianclaudio Malgieri, 'Trade Secrets v. Personal Data: A Possible Solution for Balancing Rights' [2016(6)] Int'l Data Privacy L. 102, 115; 'Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure', 2016 OJ (L 157) 1.

but the possible defences that can be raised by the latter seem to have been overlooked in the 2019 and 2022 frameworks. Undoubtedly, such conflict between rights would inevitably arise as the law develops and would likely have to be dealt with on a case-to-case basis. The jurisdiction of the DPA to determine whether an inference by a political party is legitimate or not is also unclear.

Considering the DPA is not conditioned for this purpose, its own *telos* is not shaped to be able to address the specificities of election advertising.¹⁰⁰ Therefore, a clear demarcation between the roles to be played by both the DPA and the EC will need to be created, as will be elaborated upon further. At present, it is sufficient to say that the DPA should, in principle, examine the entire process of data collection and generation of inferences through which categorization of voters takes place, while the EC should evaluate the exact effects of microtargeting itself and whether it amounts to a breach of Section 123(2) of the RPA. In the latter evaluation, the findings of the DPA regarding legality of the data collection, should be a relevant factor.

Redundancy of the Notification Requirement for Inferences

The PDP Bills largely try to protect data by providing transparency regarding its processing. The notification requirements under the respective Clauses of the 2019 and 2022 Bills, as already detailed before, strengthen the ability of Data Principals to track what kind of data is being collected from them. However, in the context of inferences, these provisions are lacking. For instance, Clauses 7 and 8 of the 2019 Bill cannot assist with Data Principals being aware of inferences about them, as the notification requirements are for personal data that is directly taken from them. By their very nature, inferences are not taken from the Data Principals but are derived from the data which is collected. Thus, the raw data collected is subject to the requirement of explicit consent from the Data Principal. However, there is little incentive to inform Data Principals about the inferences based on this data. This problem persists in the 2022 Bill as well, over and above the various additional problems in it which had not existed under the 2019 Bill.

Clause 7 of the 2019 Bill contains an additional problem in that it allows for data to be used for purposes that are reasonably related to the purpose that the Data Principal consents to. Even if it could have been argued that

¹⁰⁰ For further reading, Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Wash LRev 119; Jeroen Van Den Hoven, *Information Technology, Privacy and the Protection of Personal Data* (CUP 2008).

the consent requirement mandated a clear indication regarding the possible inference to be made from the data, this is undermined by the words “reasonably related”. A Data Fiduciary may simply state that the inference falls within this safe harbour without providing details about its specifics. They would not have to include this under the notice of consent at all. There is no direct mirror provision to this in the PDP Bill, 2022, which on the face of it is one of the few aspects on which the newer Bill improves on the 2019 iteration.

Alternatively, it could be that a separate entity from the political party processes the data and creates the inference.¹⁰¹ Singh notes that multiple private parties assisted the BJP in their data accumulation exercise.¹⁰² Thus, if the inferences are made by this entity and transferred to the BJP, a notification would have to be provided. Even this requirement was hollowed out by Clause 7 of the 2019 Bill stating that the transferee only needs to notify the Data Principal “as soon as reasonably practicable”. There is no indication of what this entails and could be abused by the Data Fiduciary to delay revealing the inference that it received from the third party. This is particularly problematic, given the corresponding provision in the GDPR, Clause 14, mandates that the notification be provided within one month. Thus, a clear intention can be discerned in the shelved PDP Bill, 2019, to make the notification requirement more lenient. This aspect has been left unaddressed completely in the 2022 Bill. Whether a notice is required to be provided to the Data Principal when their data is transferred by a Data Fiduciary to a third-party entity, is not answered. Clause 9(9) allows for such transfers to take place provided a valid contract exists between two entities, but does not mention notice being sent to the Data Principal. This leaves open the possibility that the data of Principals may be shipped around from one party to another, after the initial grant of consent to a specific Data Fiduciary to process personal data.

Finally, the notification requirement in the 2019 Bill only mandated that categories of data be provided, and not the actual data itself.¹⁰³ This creates an unnecessary layer of confusion for the Data Principal. The category does little to inform Principals about whether the data that has been collected is potentially harmful or particularly invasive of their privacy. Another question

¹⁰¹ Wachter and Mittelstadt (n 79) 52.

¹⁰² Shankar Singh (n 22) 140-150.

¹⁰³ Similar to the position in the EU, *EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, OJ 2016 L 119/1, art 13.

that is left unaddressed is whether the notification is necessary if the original Data Fiduciary had informed the Data Principals of the possible sharing of their data with a list of third parties. Substantively, the Data Fiduciaries could argue that the pre-emptive notification is sufficient, in substance, to satisfy the requirements of Clauses 7 and 8. The PDP Bill, 2022, makes the notification requirement even less definitive, by merely requiring an “itemised” list of data that is collected to be provided to the Data Principal. How detailed, or broad, this list can be is not mentioned in the Bill.

The lacunae in the notification requirements mean that Data Principals cannot rely on it to remain up to date regarding inferences. The possible solution to this is the Right to Access. Principals may seek information regarding the inferences made by the Data Fiduciary at any point in time. However, this right also cannot be deemed to be absolute. The Right to Access provides the option to the Data Fiduciary to restrict the disclosure to merely the categories of data that are collected. This gives significant leeway to the Data Fiduciary to keep the crux of the data collection a secret.

Furthermore, as already alluded to above, the Right to Access can become hollow in several other scenarios.¹⁰⁴ Data Fiduciaries may raise their own rights under other laws as a defence against complying with a data request by a Data Principal. This reduces the oversight and transparency that is possible for inferences. The Right to Access the data of Data Principals by the Principals themselves is primarily meant to provide this transparency, in conjunction with consent requirements and notification. However, as described above, there are multiple ways to keep this information opaque due to loopholes in the PDP Bills, both 2019 and 2022, as well as potential rights that Data Fiduciaries may have that guard against a need for full disclosure.

In the electoral context, this is problematic given the sources of information for parties may not be apparent. Further, the most important piece of data which is the inference made about a voter will be difficult to identify. Having access to this information would make a Data Principal more aware of the kind of targeting he/she might be exposed to. Political messaging and advertising might be easier to identify if the individual knows that he/she is being targeted in a certain way. Without this transparency, it is possible for Data Principals to be implicitly influenced without even realising that it is occurring.

Further, the specific provision to object to decisions made via automated or algorithmic processing in the GDPR had not been reproduced in the PDP

¹⁰⁴ Text to n 92.

Bill, 2019, and predictably finds no place in the 2022 Bill given its significantly reduced scope. Thus, keeping in mind these issues, the inclusion of inferences under the definition of “personal data” had been made somewhat redundant even within the 2019 Bill by the many barriers to the exercise of the rights provided for Data Principals.

Sensitive Personal Data

In the 2019 iteration of the PDP Bill, the category of “sensitive personal data” does not include inferences under the PDP Bill and the standards provided under Clause 15 for the inclusion of new forms of sensitive personal data would have meant that their subsequent incorporation would have been unlikely. Sensitive personal data had been subject to certain additional protections under the PDP Bill, 2019 such as being exempt from processing under Clause 13, and a need for Significant Data Fiduciaries to undertake Data Protection Impact Assessments under Clause 27 of the 2019 Bill which mandates the Assessment to happen when using data that has a risk of harm to the Data Principal.¹⁰⁵ Sensitive personal data is no longer protected under the 2022 Bill, but the requirement for Significant Data Fiduciaries to conduct Data Protection Impact Assessments has been retained under Clause 11(2).¹⁰⁶

Under the 2019 Bill, it would have been very difficult to include data under this category given the high procedural and substantive barriers to doing so under Clause 15. Wachter & Mittelstadt have designated a category of inferences as “high-risk inferences”.¹⁰⁷ This refers to inferences which are accumulated through data collection, and which are the basis for decisions made regarding the Data Principal. In their definition, such inferences include the following characteristics: a) privacy invasive; b) damaging to reputation; c) have low verifiability.¹⁰⁸

While the GDPR contains provisions for protecting sensitive personal data under Clause 9, the PDP Bill, 2019, contained a poor mirror provision. Clause 15 allowed the Central Government to designate certain categories of personal data as “sensitive”. Thus, the designation of new forms of “sensitive personal data”, outside of those already included under Clause 2(36) was at the discretion of the Central Government. Importantly, under Clause 15 the DPA and authorities in the relevant sector do not make the categorization

¹⁰⁵ PDP Bill 2019, cl 27.

¹⁰⁶ Personal Data Bill 2022, cl 11(2).

¹⁰⁷ Wachter and Mittelstadt (n 79) 10-17,

¹⁰⁸ *ibid*; Sandra Wachter, ‘Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR’ (2017) 34(3) *Computer Law & Security Review* 436.

but are merely part of the consultation process. From the wording of the clause, it would seem the Government is not bound by the advice received from the DPA and other relevant authorities. It is often in the interests of the Government to define this category of data in a restrictive way. A sitting government would wish to keep “sensitive personal data” narrow and confined to Clause 2(36) as provided, to prevent additional barriers to collecting data. One further point to note is that the rationale behind including or excluding a certain form of data under the “sensitive” category did not need to be provided as per the PDP Bill, 2019.

Apart from this procedural hurdle, there were substantive hurdles in place as well. Clause 15(a) & (c) both use the term “significant harm” as the threshold for data to be classified as “sensitive”. This standard seems unnecessarily high. A clear intention exists, therefore, to make the categorization of “sensitive personal data” as limited as possible. Clause 15(d) gives the Central Government the final word on determining whether existing privacy laws are sufficient for ensuring data protection. Finally, Clause 15(b) refers to the “expectation of confidentiality” among Data Principals, but the ability of the Government to make this determination undermines this. No consultation procedure for the Data Principals is mentioned, and as already discussed, no third-party opinion is binding on the Government’s final decision.

This reduces the utility of inferences being included under Clause 3(28). An inference in the context of an election is unlikely to fall under Clause 15. The most detrimental effect of micro-targeting is the manipulation of voters and their opinions. Whether this qualifies as “significant harm” is questionable. Regardless, the overarching issue with this Clause remains the Central Government’s prominent role in classification, and the minor importance of the DPA and other stakeholders.

This is problematic considering the indirect, but genuine harms caused by data analytics and micro-targeting. However, it is not always simple to demonstrate these harms and to show they fulfil the standard of “significant harm”. One of the important advantages of including inferences under personal data would have been the ability to classify inferences used for micro-targeting as “sensitive”. Under the GDPR, such inferences could have been afforded a much greater degree of protection. However, this possibility was remote under the PDP Bill given the wording of Clause 15.

The GDPR which has a broad definition of such data had been largely ignored under the PDP Bill, 2019. For example, data regarding political opinions, of paramount importance in an election context, falls under “Sensitive”

data under the GDPR.¹⁰⁹ In the 2022 PDP Bill, the concept of sensitive personal data itself has been removed, thus, completely negating the potential of greater protection for such data along the lines of the safeguards under the GDPR. This is emblematic of the fact that while the 2019 Bill required improvements, it was still preferable to the 2022 Bill that has subsequently been put forward.

Fairness

While these legal loopholes may be found in the rights under the PDP Bill, one could argue that Clause 5 of the 2019 Bill still imposed an obligation upon Data Fiduciaries to process personal data in a “fair” manner. However, the ambit of this requirement is unclear and no guidance was provided under the PDP Bill, 2019 itself. Once again, we may refer to the GDPR’s experience with “fairness” requirements in this regard as a similar provision exists within it which has been interpreted by scholars. Eskens has stated that “fairness” as under the GDPR equates to the Data Fiduciary being transparent in its activities. She interprets fairness as being synonymous with concepts such as lawful and transparent. In this iteration, fairness has a fairly limited utility.¹¹⁰

An opposing interpretation has been put forward by the European Data Protection Board. The Board’s approach to fairness is as a purpose limitation to data collection. Data Fiduciaries would, in this school of thought, be restricted from expanding the scope of what they could use collected data for. Additionally, fairness must also take into account the expectations of Data Principals and the actions of Data Fiduciaries must be in consonance with these expectations.¹¹¹ Wachter & Mittelstadt note that one use of the fairness provision could have been to prevent Data Fiduciaries from providing vague and overtly broad purpose uses in their terms and conditions. This practice tends to encapsulate any and all possible uses, which erodes the consent protections that Data Principals are meant to have. However, the prevailing view at present is that the GDPR’s “fairness” requirement is nothing more than a transparency tool.¹¹² Thus, it contains procedural

¹⁰⁹ GDPR 2016, art 9.

¹¹⁰ Sarah Johanna Eskens, ‘Profiling the European Consumer in the Internet of Things: How Will the General Data Protection Regulation Apply to This Form of Personal Data Processing, and How Should it?’ (*Thesis Research Master Information Law 2016*) <<https://www.saraheskens.eu/publications/Eskens-2016-iot.pdf>> accessed 14 September 2022; Lee Bygrave, ‘Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making’ in Karen Yeung and Martin Lodge (eds) *Algorithmic Regulation* (OUP 2019).

¹¹¹ *The European Data Protection Board*, Endorsement 1/2018 (25 May 2018) 5, 9.

¹¹² Wachter and Mittelstadt (n 79) 93-94.

obligations only, and not substantive ones which could help with the question of inferences and their correctness. In light of this, it is unclear how substantive obligations could be derived from the requirement under Clause 5 of the PDP Bill, 2019, especially in the context of inferences given the earlier discussion on the various difficulties associated with applying data rights to them. The point on non-verifiable inferences once again poses a challenge in this regard.

As with several other regressive steps, the requirement for “fairness” in processing of data has been done away with in the PDP Bill, 2022. It is important to recognize the drawbacks that undoubtedly underlined the 2019 Bill in order to improve them. However, the solution was not to truncate the Bill even further as has been done in the 2022 version. The critique provided in this section regarding the various shortcomings in the PDP Bill, 2019, is by no means an implicit approval of the subsequent version of the law that has been proposed. Rather, the subsequent legislation undoes many of the beneficial, albeit flawed, steps that the PDP Bill, 2019 had attempted to take toward a robust protection of online data. What we must contend with now is a 2022 Bill that sacrifices several of even those basic safeguards.

Privacy as a Balancing Act

What should be clear from the discussion outlined above, is that the determination of rights under the PDP Bills is a balancing act. The degree to which Data Fiduciaries may exercise their own rights to keep data collection and the metrics used for creating inferences confidential will have to be set off against the rights of Data Principals. However, this balancing could not be appropriately done unless certain additional regulations are put in place to deal with the gaps in both the PDP Bills that have been pointed out above. These deficiencies will require the DPA to step in and lay down codes of practice, or to be addressed directly in the wording of the revamped 2022 Bill. Given the state of the Bill at present, it seems unlikely that such substantive guidelines will be included before it is finalized.

Additionally, a progressive legal approach toward privacy will be necessary. Given the very nature of data analytics which operates at a massive scale, exemplified by Singh’s own accounts, simply looking at privacy as an individual right is insufficient. Moreover, group privacy cannot apply to the kinds of categories of individuals created through inferential analytics. Therefore, a completely different notion of privacy will be proposed in the next part of this paper, which is better equipped to deal with the realities of inferential analytics.

PART III

VII. THE NEED FOR COLLECTIVE PRIVACY

Having noted the deficiencies in both the 2019 and 2022 PDP Bills vis-à-vis proper regulation of inferences, we can now turn to what the more appropriate means of analysing the competing interests under the Bill would have been. Undoubtedly, whenever a Data Principal raises a grievance regarding a particular practice, some weighing of the different stakes involved will take place to determine whether the data collection practice and usage of said data are permissible. The correct means of doing so should not merely be to look at the rights of each individual Data Principal, but rather the entire collective or category of Data Principals who are placed similarly. Looking at data rights in only an individual way does little to curb the effects of data analytics and micro-targeting. A single Data Principal may bring a claim to protect their rights, but in the context of entire populations or groups of people exposed to such data harvesting, this is merely a drop in the bucket. To effectively place fetters on this practice, the collective requires protection, not just single individuals. Before elaborating on the notion of Collective Privacy, it is important to highlight the deficiencies in two alternative approaches that are generally invoked for dealing with the issue of data mining and drawing of inferences regarding groups of people.

Alternative Approaches to Protecting Privacy of Groups

The general tack followed for addressing such an issue is to refine the already existing provisions in the statute. In the context of the PDP Bills, this may have involved strengthening the provisions on inferences through any number of ways. This is especially the case for the PDP Bill, 2019, given that it accorded explicit recognition to inferences, unlike the 2022 Bill. Thus, our starting point for this examination remains the 2019 Bill, given that the objective is to demonstrate how it could have been improved and protection of inferences made more robust, from the basic platform that the earlier Bill provided. The 2022 Bill, as has been made clear, is a significantly poorer position from which to begin.

The two primary approaches that may be adopted will be addressed to demonstrate why a collective privacy approach is necessary. The first would be to attack the issue at its source i.e., greater restrictions on the collection and processing of data. The second is to make changes to the provisions on

inferences, such as the suggestion provided by Wachter & Mittelstadt to incorporate a “Right to Reasonable Inferences”.¹¹³

With regard to the first issue, a focus on the actual collection of data overlooks the manner in which collectives of people are aggregated using data analytics. The generic practice of classifying groups of people together is on the basis of sensitive personal data. This is because sensitive personal data is, by definition, information that individuals wish to keep private, such as their religious affiliation, ethnicity, and various other immutable characteristics. Aggregations of people via such criteria are used often by law enforcement to identify areas and communities that require special attention. Enhanced policing, surveillance and specialized tactics are then employed in these regions to ensure the suppression of threats. Similarly in an electoral scenario, one would consider that some voters would want such information to remain secret.

Even in a hypothetical world where provisions are introduced which perfectly protect one’s sensitive data, such provisions would be unable to address the fact that even completely innocuous and non-personal data which is publicly available will be sufficient for the purpose of creating agglomerations of people for the purposes of micro-targeting. It may take a draconian level of data processing restrictions to prevent even the minutest forms of non-personal data from being accumulated. No legislation in any surveyed jurisdiction contains restrictions of that degree upon non-sensitive personal data. As Singh shows, electricity bills, which do not fall anywhere remotely within the definition of sensitive data, are enough to begin creating a profile of an individual.¹¹⁴ Combining similarly non-personal data points will be sufficient to determine the exact manner in which to micro-target any collective of individuals.

The second approach could be to make provisions on inferences more stringent. Thus, even if it is difficult to prevent the collection and categorisation of people based on their data, one can try to restrict the drawing of inferences and consequently the actions taken on the basis of those inferences qua that person. However, there are practical difficulties associated with tracking and detecting when an inference has been drawn about individuals. The Snowden disclosures in 2013 revealed that most people are oblivious to the number of ways in which they are being influenced on a daily basis and

¹¹³ Wachter & Mittelstadt (n 79).

¹¹⁴ Shankar Singh (n 22).

how decisions are being taken based on inferences drawn about them.¹¹⁵ The tracking en-masse of peoples' behaviour online, as well as programs such as X-Keyscore and trackers within online applications, led to a wealth of information being mined about millions of people, making it possible to then carry out surveillance. It is significant that until the initial story surrounding the existence of such programs was published, there was almost no knowledge in the public domain about these illicit activities and no recognition of the consequences. Thus, this presents an enforcement problem whereby a restriction on inferences cannot be properly implemented.

Regardless of these shortcomings, the primary issue with using the tactic of tweaking provisions of the PDP Bill, 2019, is that it remains focused on an individual-centric approach toward data privacy. The objective in big data analytics, and for political parties, is to target entire collectives of people. In a hypothetical scenario, if a sharp and technologically aware individual is able to discern that they are being microtargeted, they can only raise an objection with the relevant authorities in terms of himself/herself. The difficulty of this has already been commented upon above in the context of the Snowden revelations, and has been elaborated upon at length by scholars.¹¹⁶ In any case, in the hypothetical scenario, though this individual is able to avoid being targeted it does not in any way stop a party from achieving its primary purpose which is to target the larger collective. When the objective of microtargeting is to influence the collective, individual-centric data privacy rights are insufficient.

Addressing this issue from the standpoint of the privacy of entire collectives of people is in consonance with how parties in elections view their target audience. Logically, the objective is not to influence specific individuals but to provide a broad message that can appeal to the largest number. Hence, the manner in which the data privacy rights of people are protected must necessarily reflect that reality rather than remain focused on purely individual rights.

¹¹⁵ European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2014) <<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230>> accessed 5 May 2022.

¹¹⁶ Lee Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002).

Group Privacy

The Right to Privacy largely follows an individual rights model. The implication of this is that the right attaches primarily to an individual rather than a collective or group entity. Bygrave notes that this holds true for both European and American law, two places where privacy law has developed more than others.¹¹⁷ There has been a slow evolution of this position with the Article 29 Working Group recognizing the concept of a collective interest in privacy rights.¹¹⁸ This has largely been seen as an agglomeration of multiple individual grievances and not as a separate and independent legal right in and of itself. Mantelero notes that this interpretation has meant that relief granted is usually premised on protection of individuals within the agglomerations, rather than collective relief.¹¹⁹ Therefore, the development of data privacy law has only come to the stage of group privacy, rather than collective privacy.

Contemporaneous data privacy scholars have identified two primary concepts of group privacy. The first, concerns the privacy of individuals within the group's settings.¹²⁰ The second concerns an entity which is recognized as a body of individuals in law with that entity itself having privacy rights.¹²¹ Neither of these concepts are useful in the context of elections. The peculiar situation in political microtargeting is that the individuals so targeted do not necessarily identify as a group. They are disparate and non-aggregated individuals whose only commonality is the inferences that political parties draw about them. This restrictive idea of group privacy has been recognized and Bygrave has posited a more suitable alternative. He proposes that individual privacy rights in statutes be transposed to such collectives which do not self-identify as such.¹²²

¹¹⁷ Lee Bygrave, 'Privacy Protection in a Global Context—A Comparative Overview' (2004) 47 *Scandinavian Studies in Law* 319; Article 29 Data Protection Working Party 'Letter to Mr. Larry Page, Chief Executive Officer' (2013) <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130618_letter_to_google_glass_en.pdf> accessed on 18 October 2021.

¹¹⁸ Article 29 Data Protection Working Party, 'Letter to Mr. Larry Page, Chief Executive Officer' (2013) <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130618_letter_to_google_glass_en.pdf> Accessed 18 October 2021.

¹¹⁹ Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor, Luciano Floridi and Bart Van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer Link 2017).

¹²⁰ Edward Bloustein, 'Group Privacy: The Right to Huddle' in Edward J Bloustein, Nathaniel J Pallone (eds), *Individual and Group Privacy* (Routledge 2018).

¹²¹ Alan Westin, *Privacy and Freedom* (Ig Publishing 1970).

¹²² Bygrave (n 110).

Collective Privacy

Mantelero has built on this to elaborate how the subject of data privacy law must shift away from individuals/recognized group entities, toward clusters of individuals who do not identify as a collective but are grouped as collectives on the basis of the inferences made about them.¹²³ Individual privacy rights must be suitably modified in such situations to provide adequate relief to such disaggregated collectives.¹²⁴ This conception of “collective” is consistent with the manner in which micro-targeting occurs. Singh’s elaboration of how data gathering targeted tribals in Tripura and non-Yadav OBC’s in Uttar Pradesh, demonstrates how these individuals are implicitly classified together without them knowing that they are part of a collective at all. They are not recognized as a group or juristic entity in law and their grouping occurs only in the context of inferential data analytics.¹²⁵ Recall how certain people were categorized together on the basis of their electricity bills. These people would not even think of themselves as a collective, given most of them would not even know of each other.

These categories are created based on data analytics and recognizing certain clusters of information from the data collected. All individuals with high electricity bills are formed into a cluster, based on their bills. While these individuals remain oblivious to what is happening, for the analyst they are an autonomous category, primed for a particular form of election advertising.¹²⁶ This form of categorization has become increasingly common, especially in the context of elections and for law enforcement.¹²⁷ However, these collectives do not currently have recognition in data privacy law in any jurisdiction.

What is important about such collectives is that the way the individuals are affected is not based on their individual data, but rather on the collective data regarding their respective clusters.¹²⁸ Thus, the decisions made regarding micro-targeting are based on the overall inferences drawn about the group to which they belong. This issue is further complicated by the fact

¹²³ Mantelero (n 119) 143.

¹²⁴ Mantelero (n 119) 144.

¹²⁵ Shivam Shankar Singh (n 22) 75.

¹²⁶ *ibid* 64, 75.

¹²⁷ Oskar Josef Gstrein, Gerard Jan Ritsema van Eck, ‘Mobile Devices as Stigmatizing Security Sensors: The GDPR and a Future of Crowdsourced “Broken Windows”’, (2018) 8(1) *International Data Privacy Law* 69.

¹²⁸ David Bollier, *The Promise and Perils of Big Data* (Aspen Institute, Communications and Society Program, Washington, DC, 2010) <https://www.aspeninstitute.org/wp-content/uploads/files/content/docs/pubs/The_Promise_and_Peril_of_Big_Data.pdf> accessed 8 September 2022.

that individuals will belong to multiple such clusters in big data analytics. Specific individuals will be subject to different types of advertising or treatment, depending on the different clusters they are grouped into. Due to the fact that they do not identify as a “group”, and thus, group rights cannot be transposed onto them¹²⁹ Mantelero enunciates a “collective privacy” principle, which looks at clusters of individuals who do not identify as groups.¹³⁰

This approach to privacy is far more effective than looking at individual interests. The reason for this is that through data analytics a group norm is culled out, rather than the individual norms.¹³¹ For instance, a particular part of a city may be deemed to have one primary concern or a particular political leaning due to demographic factors such as predominant religion and average income. Based on data collected about the majority of individuals in that area, only certain kinds of advertising and information will be provided to them. Those individuals who may not fall into the majority category may be exposed to certain kinds of advertising based on the collective into which they have been placed due to their residence in that part of the city. These individuals may have different opinions regarding this kind of collective electoral profiling i.e., not all of them may find it to be problematic.¹³² Thus, if an individual-centric approach is taken, some of these individuals who are targeted may not, for various reasons, care for the collective interest of the electorate to not be targeted in such a manner. One such cause could be that the individual supports the targeted messaging as the party undertaking it conforms to the specific political outlook and ideology of that voter. Hence, the individual believes that society would benefit from these messages being sent directly to them without a thought for how this may be part of a strategy of manipulation and implicit coercion.

Parties are unconcerned with providing the electorate with all the necessary information regarding any particular issue. Their focus is to only elaborate on those points that they determine will encourage people to vote in their favour. The ability of parties to do this in a sophisticated and precise manner is accentuated by data analytics. The question that then arises is how best to protect the collective from undue influence. Newman proposes that the collective interest should be what governs the decision regarding whether such collective profiling is detrimental or not.¹³³ Depending on the

¹²⁹ Luciano Floridi, *The Ethics of Information* (OUP 2013).

¹³⁰ Mantelero (n 119).

¹³¹ Pam Dixon and Robert Gellman, ‘The Scoring of America: How Secret Consumer Scores Threaten your Privacy and your Future’ (World Privacy Forum, 2014).

¹³² Mantelero (n 119) 148.

¹³³ Dwight G Newman, ‘Collective Interests and Collective Rights’ (2004) 49(1) *American Journal of Jurisprudence* 6.

context, different collectives may arise. For elections, the freedom of the vote and collective interest against disinformation or half-truths is of relevance.¹³⁴ This interest would not be dependent upon the individual voter, as highlighted above, but rather centre around a general principle that underpins the objective of free, fair, and legal elections. Thus, in line with Newman's suggestion, inferences and microtargeting which go against the collective interest of having free and fair elections must be ceased.

This has also been recognized by Koss and Perry who advocate a shift away from purely individual rights and toward rights against the inferences made as a result of clustering people in this manner.¹³⁵ Disaggregated people being made into a collective have an interest in their privacy and ownership over personal information at an individual level.¹³⁶ However, over and above those individual concerns, the issues at a collective level would involve possible negative consequences of inferences made regarding them as a collective rather than as individuals.¹³⁷ This is the crucial distinction that the recognition of collective privacy allows us to address.

Thus, the special concern of data privacy law in the context of elections needs to be inferences made about disaggregated collectives of people.¹³⁸ Both of these aspects were insufficiently addressed in the PDP Bill, 2019, which followed the typical and standard individual-centric approach. In any case, inferences are inadequately protected under the PDP Bill and the rights provided under Chapter V had several barriers to their applicability. The question of collective privacy is completely missing from the PDP Bill, 2019, and there is no indication of how it is supposed to be dealt with. The 2022 Bill, as has been elaborately detailed, is even more deficient in significant and profound ways on this point. Thus, the legal framework was lacking in terms of its ability to deal with inferences in the context of collective privacy and

¹³⁴ Snigdha Poonam and Samarth Bansal, 'Misinformation is Endangering India's Election' *The Atlantic* (1 April 2019) <<https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/>> accessed 25 September 2021.

¹³⁵ Walter Perry and others, 'Predictive policing: The Role of Crime Forecasting in Law Enforcement Operations', (Rand Corporation 2013) <http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf> accessed 2 October 2021; Kelly K. Koss, 'Leveraging Predictive Policing Algorithms to Restore Fourth Amendment Protections in High-Crime Areas in a Post-Wardlow World' (2015) 90 *Chicago-Kent Law Review* 301.

¹³⁶ Fred Cate and Viktor Mayer-Schönberger, *Data Sue and Impact (The Centre for Information Policy Research and The Centre for Applied Cybersecurity Research, Indiana University 2013)* <http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf> accessed 25 September 2021.

¹³⁷ John Finnish, 'The Authority of Law in the Predicament of Contemporary Social Theory' (1984) 1(1) *Notre Dame Journal of Law, Ethics & Public Policy* 115.

¹³⁸ Edward Bloustein, *Individual and Group Privacy* (Routledge 1978).

is required to be comprehensively addressed in the revamped Bill that is currently being contemplated. The current rendition of the 2022 Bill, however, leaves even more to be desired than the PDP Bill, 2019.

Enforcement of Collective Privacy Rights

Now that the specific purpose and importance of collective privacy have been detailed, the issue of how to enforce such a collective privacy right must be addressed. Mantelero proposes that the respective Data Privacy Authorities of different countries make the risk assessment of these inferences.¹³⁹ However, the issue with this has already been elaborated upon where there is a specialized agency such as the EC already in place to address election-related concerns. An intriguing solution is put forward by Kammourieh who relates the Right to Privacy of a group/collective to several human rights principles.¹⁴⁰

The Right to Privacy of a group may be related to the Right to Dignity, specifically the right to Self-Determination. The right is rooted in Article 1 of the International Covenant on Civil and Political Rights (“ICCPR”).¹⁴¹ The original interpretation of Article 1 was confined to external self-determination which legally allowed colonized peoples to declare independence.¹⁴² The evolution of the right has now encapsulated an internal right to self-determination. This allows groups within groups to demand constant social and political rights. In this way, the notion of self-determination has expanded to include rights such as “informational self-determination” which may be directly relevant to data analytics and collective privacy rights.¹⁴³ However, Paton recognizes that the ICCPR contemplates the exercise of these rights by recognized entities or groups. In this context, there is no recognized group but merely passive clusters that are created due to them being clubbed together by data analytics. Such passive clusters or collectives cannot exercise rights under the ICCPR.¹⁴⁴ Due to this, Kammourieh falls back on policy recommendations and changes to help such passive collectives better regulate the collection and usage of their data.

¹³⁹ Mantelero (n 119) 150.

¹⁴⁰ Lannah Kammourieh, ‘Group Privacy in the Age of Big Data’ in Linnet Taylor, Luciano Floridi and Bart Van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer Link 2017) 54.

¹⁴¹ International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 1; Antonio Cassese, *Self-Determination of Peoples: A Legal Reappraisal* (CUP 1995) 11.

¹⁴² Jonathan Charney, ‘Self-Determination: Chechnya, Kosovo, and East Timor’ (2001) 34 *Vanderbilt J of Tech L* 455; UNGA Res 1803 (1962) GOAR 17th Session Supp 17, 15.

¹⁴³ Kammourieh (n 140) 54.

¹⁴⁴ George Whitecross Paton, *A Textbook of Jurisprudence* (4th edn, Clarendon Press 1972).

Additionally, Mantelero correctly notes that one cannot protect collective rights the same way one would protect corporate group rights. Corporate rights can be enforced by the central authority of the organization or entity. Collectives of the kind described here, do not have any central authority at all and are atomistic in nature.¹⁴⁵ For collective privacy to fulfil its purpose, a method to enforce it is necessary.¹⁴⁶ To achieve this outcome, it is possible to look at collective or general interests that are protected by centralized authorities. Examples of this include financial regulators and consumer redressal bodies which seek to ensure the basic and general protection of consumers and investors.¹⁴⁷ Similarly, the DPA could focus on the general interest of the collective in ensuring that it is not manipulated and its right to a free vote is not hindered.

However, a return to the DPA would once again mean dependence on centralized authority. If this were seen as the only viable solution, it would remain a problematic one as a centralized authority remains more susceptible to political influence and bias. Mantelero's suggestion of having such a centralized authority act as gatekeeper seems feasible at face value but he acknowledges one of the greatest concerns with this would be the impartiality of the authority.¹⁴⁸ In India, this role could be fulfilled by the combination of both the DPA and the EC. The scrutinization of data collection, especially that of inferences and the metrics on which such inferences are reached, and their utilisation for microtargeting can be apportioned between both authorities depending on various factors.

The determination of the potential detriments of such collection from the perspective of its consequences for political disinformation, classification of constituents and microtargeting, and undue influence of voters, requires the expertise of both the DPA and EC. Such considerations must be looked at in terms of the consequences for the individual as well as the disaggregated collective to which that individual belongs.¹⁴⁹ The interests of this collective,¹⁵⁰ which is created by the Data Fiduciary through inferential analytics, must be analysed both from the perspective of unfair means of collecting the data and the criteria provided for the inferences drawn about voters as collectives.

¹⁴⁵ Bygrave (n 110).

¹⁴⁶ *ibid*; Mantelero (n 119) 150.

¹⁴⁷ Mantelero (n 119) 150.

¹⁴⁸ *ibid* 152.

¹⁴⁹ Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89(1) *Washington Law Review* 1.

¹⁵⁰ Alessandro Mantelero, 'The Future of Consumer Data Protection in the EU Rethinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30 *Computer Law & Security Review* 643.

This would, hypothetically, be the province of the DPA. Simultaneously, the EC may investigate the potentially detrimental effects such a practice may have on elections and whether it amounts to a violation under Section 123(2) of the RPA.

Another possible method would be for the DPA, in conjunction with the EC, to carry out Data Protection Impact Assessments.¹⁵¹ Such Assessments have been proposed in various jurisdictions across the world in different contexts and can provide a benchmark for determining what activities may pose a risk to collective privacy. DPAs are often best placed to identify technological innovations and practices which could pose a risk to collective privacy. Thus, it may examine the various methods by which parties collect constituents' data and act accordingly. This is a form of predictive analytics which makes a presumption about potential dangers from specific activities of data collection and inference drawing. As Cohen and Floridi point out, such predictive analytics requires a proper understanding of the social or political consequences of the specific data practice in question.¹⁵² This cannot be done by the DPA in a vacuum and must involve the EC and its expertise and knowledge of the way that elections function and how voters can be influenced. This goes back once again to Mantelero's suggestion that a multi-department collaboration is necessary to effectively enforce collective privacy rights.

The specifics of how these two institutions may work together to frame rules for the conduct of parties must necessarily be context specific. Wright correctly notes that general guidance in this realm is difficult to lay down.¹⁵³ Rather, criteria for governing the mining of data, drawing of inferences, and then using such inferences to aggregate people for the purpose of microtargeting, will necessarily depend on the specific legal framework and social context. This would involve a far more in-depth analysis of how to balance different interests and the specifics are not the subject of this paper.

While this may be a rough demarcation in terms of the responsibilities undertaken by the DPA and EC respectively, it is unclear whether there can be a guarantee of their independence from the Central Government in power

¹⁵¹ Mantelero (n 119).

¹⁵² Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press 2014); Julie Cohen, 'What Privacy is for' (2013) 126 *Harvard Law Review* 1933.

¹⁵³ David Wright, 'A Framework for the Ethical Impact Assessment of Information Technology' (2011) 13(3) *Ethics and Information Technology* 199; Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010) 231; Mantelero (n 119) 150.

at the relevant time. The DPA has not, of course, even been formed yet. The EC is routinely accused of bias and failure to ensure completely free and fair elections.¹⁵⁴ The appointment of the DPA is to be determined by the Cabinet of the Central Government, which could create issues of independence as well as individuals sympathetic to whichever ruling government exists could be appointed to the DPA.¹⁵⁵ Regardless, it is necessary to recognize the concept of Collective privacy and to take whatever steps are feasible to ensure the greatest amount of impartiality and rigour on the part of regulators.

In the current scenario of data protection and elections in India, a collaboration between the EC and DPA seems to be the most appropriate means by which to enforce Collective Privacy. Various scholars have noted that this solution lies in the realm of policy where balancing must be done between different interests and components within society.¹⁵⁶ Data Protection Authorities do not normally concern themselves with the impact of the use of data (influence and manipulation of voters), but rather, focus on the collection of data itself. However, as exhaustively elaborated upon above, it is necessary to incorporate enforcement that looks at the negative effects of data mining and drawing inferences on a collective scale. This is the stage where the EC, which focuses on the actual impact of inferences drawn about collectives of voters, would be needed.

To this extent, Mantelero's proposed solution involves having multiple agencies or departments involved in order to ensure that different stakeholders and interests are adequately addressed.¹⁵⁷ Examples of this have been seen in consumer protection and labour law.¹⁵⁸ In the former, it is in the collective interest of all consumers to ensure product security and prevent unfair commercial practices, however, consumers are atomized and not connected to each other. In order to enforce these general interests, institutions must take the lead in setting policy. These steps would not be taken in isolation by the DPA. In the electoral context, the implementation of safeguards on data protection and inferences would be of minimal assistance without the expertise of the EC in addressing the actual manner in which such data

¹⁵⁴ 'Election Commission Biased, Poll Schedule Made to Benefit PM Narendra Modi: Rahul Gandhi' *India Today* (17 May 2019) <<https://www.indiatoday.in/elections/lok-sabha-2019/story/election-commission-partial-poll-schedule-made-for-pm-modi-s-campaigns-rahul-gandhi-1527525-2019-05-17>> accessed 15 October 2021.

¹⁵⁵ Personal Data Bill, cl 42.

¹⁵⁶ Wright (n 156).

¹⁵⁷ Mantelero (n 119).

¹⁵⁸ European Commission, *Second stage consultation of social partners on the protection of workers personal data* 7, 10, 16–17 <<http://ec.europa.eu/social/main.jsp?catId=708>> accessed 3 March 2022.

and inferences are used to influence elections. Thus, a collaborative effort between both institutions would be required in order to appropriately protect the collective privacy of large groupings of people who are ill-equipped and poorly placed to ensure their rights are not violated.

PART IV

VIII. CONCLUSION

For data privacy law, the collective matters as much as the individual. If the subject of the law was merely the individual, it could serve to protect him/her but do little to deter the drawing of inferences about, and profiling of, the entire collective. In modern data analytics, the profiling of a single individual is of relatively little importance. The targets of data collectors and those interested in targeted advertising are entire collectives of people.

The logic is a fairly straightforward one i.e., through data analytics about large factions of people, the greatest number of them may be implicitly manipulated. For a commercial entity, that can mean persuading sufficient people to choose their product over those of competitors. For social media and other websites, it is to market that data to advertisers for revenue. And for States and political parties, it is to persuade voters during elections or to convince them regarding the wisdom of their respective policies while in office. Privacy law, therefore, must keep pace with the ways in which data collection takes place and how it is used. As the Edward Snowden disclosures revealed, at the best of times, individuals are mostly unaware of the number of ways in which their activities are being monitored and how their behaviour is being shaped implicitly.

One of the greatest threats that arise from these practices is the possibility for entities to manipulate elections. While this is usually thought of in the context of external manipulation by foreign enemies, internal actors could just as easily influence politics and society. The news that the PDP Bill, 2019, was withdrawn, after 3 years of waiting, was disappointing and shows that recognition of data privacy is still at its most nascent stage in India. However, it also provides an opportunity, in that the gaps identified in the PDP Bill can be addressed more holistically in a reworked legislation. This hope has not been crystallized in the PDP Bill, 2022. The revised Bill has gone in the opposite direction in many ways, including removing the explicit recognition accorded to inferences as being personal data, the removal of sensitive personal data and the obligations that are imposed on Data Principals under Clause 16 which have a chilling effect on the enforcement of rights under

Chapter 2 of the 2022 Bill. Thus, the only appropriate course of action is an about turn on various steps taken in the 2022 Bill that aggravate the issues associated with inferences and microtargeting. The PDPD Bill, 2019, is a better starting point from which to gauge the improvements that must be brought about in our data privacy laws.

Thus, a restoration of the recognition of inferences as personal data is a *sine qua non* for bringing the PDP Bill in tune with modern methods of microtargeting. The PDP Bill, 2019, which started from the position that inferences fall under the ambit of personal data, is more attuned to this reality than the 2022 version. Further, the corpus of laws as contained in the 2019 Bill must be complemented by a recognition of collective data privacy and provisions for conducting Data Protection Impact Assessments, regardless of the type of Fiduciary. Any Fiduciary, regardless of whether it is significant or not, should be required to conduct such Assessments given the significant impact that data privacy in this area has on politics and social engineering via microtargeting. In order to ensure enforcement of collective privacy in this context, the DPA and EC must coordinate with each other and implement an improved PDP Bill which includes a recognition of this approach to data privacy, in tandem with electoral laws. This a modern reality of data privacy that the law must equip itself to address.

BRINGING SHADOW LIBRARIES OUT OF LEGAL SHADOWS: AN OPPORTUNITY FOR THE DELHI HIGH COURT

*Rahul Bajaj and Anchal Bhateja**

ABSTRACT *At the heart of the copyright bargain is the need to strike a balance between fostering creativity, by incentivizing producers of intellectual property and promoting the interests of the public at large. These two are often in tension with each other. Some cases bring this tension into sharp focus. The ongoing litigation in the Delhi high Court, on the legality of shadow libraries - Libgen and Sci Hub - is one such case. The case has seminal importance for ensuring that the right to education is duly respected and fulfilled.*

In this paper, we argue that this litigation offers the Delhi High Court an opportunity to build on its progressive jurisprudence on the educational exception embodied in Indian Copyright Law and to further push its frontiers, by regarding these shadow libraries as falling within the ambit of the fair dealing exceptions, and holding their access to be a facet of the Constitutionally guaranteed right to education. We hope that our contribution will assist stakeholders involved in the litigation and others to work towards fashioning a solution to the litigation that enables continued access to these shadow libraries, as that is what the public interest in this case demands.

I. Introduction	317	D. Affixing the Liability on the State	327
II. Setting the Scene	318	V. Comparative Experience	329
III. Recalibrating the Debate	320	VI. Copyright Law Analysis	331
IV. Constitutional Justification	323	A. Basic Purpose of Copyright Law	331
A. The Historical Background	323	B. Section 52[1][a] of the Copyright Act	332
B. Expansion by the Courts:	325	C. Educational Exception	334
C. RTE as Justification for the Continued Existence of Shadow Libraries.	327	VII. Conclusion.	341

* Rahul Bajaj is an academic and practitioner in the fields of intellectual property law and constitutional law. Views are strictly personal and must not be attributed to any entity. Anchal Bhateja is a final year student at the National Law School of India University, Bangalore.

I. INTRODUCTION

In December 2020, three libraries, Elsevier Ltd, Wiley India Pvt. Ltd. and the American Chemical Society ('ACS') filed a lawsuit in the Delhi High Court, alleging that the copyright of their paywalled material is being breached by 'Sci-Hub' and 'LibGen'. These are open-access online repositories which provide, among other things, free access to various journal articles and books which are paywalled by publishers and are popularly called 'Shadow Libraries'.¹ The lawsuit has brought into sharp relief the appropriate scope of copyright law and the determination of its boundaries.

The petitioners in the case claim that:

“Pirate sites like Sci-Hub threaten the integrity of the scientific record, and the safety of university and personal data. They compromise the security of libraries and higher-education institutions, to gain unauthorized access to scientific databases and other proprietary intellectual property, and illegally harvest journal articles and e-books.”

The petitioners further allege that Sci-Hub uses stolen user credentials and phishing attacks to extract copyrighted articles.² The petitioners have sought a dynamic injunction against these platforms.³

The legality of these platforms has been challenged in close to eleven jurisdictions up till now and ex-parte decisions have been handed down in a few of these cases. The consequences in these cases range from blocking of access to these platforms in Austria, Belgium, Denmark, France, Germany, Italy, Portugal, Russia, Spain and Sweden, amongst others, up to the potential arrest of the founder of these platforms. In the USA, the founder has been already held liable for wilful copyright infringement and has also been directed to pay a statutory compensation of USD 15 million.⁴ On similar lines, the platform has been brought before the Delhi High Court on the charges of copyright infringement.

¹ Joe Karaganis J, *Shadow Libraries: Access to Knowledge in Global Higher Education* (The MIT Press 2018).

² Holly Else, 'What Sci-Hub's Latest Court Battle Means for Research' (2021) 600 *Nature* 370.

³ Kashish Khandelwal, 'The Sci-Hub Case & the Unique Remedy of a Dynamic Injunction' (*Law School Policy Review & Kautilya Society*, 1 March 2021) <<https://lawschoolpolicyreview.com/2021/03/01/the-sci-hub-case-the-unique-remedy-of-a-dynamic-injunction/>> accessed 19 June 2022.

⁴ Sukrita Baruah, 'Hardlook: Copyright vs wrong—the Sci-Hub case being fought in Delhi' *The Indian Express* (29 September 2021) <<https://indianexpress.com/article/cities/delhi/delhi-high-court-academicians-scientists-researchers-7536252/>> accessed 29 January 2023.

In what follows, we will begin by providing a descriptive account of the lawsuit pending in the Delhi High Court. We will then seek to recalibrate the focal point of the general framing of the debate around this issue to the effect that the dispute is actually between the interests of the publishers and the readers with limited resources and the authors' interests do not lie at the core of this debate. This will not be a commentary on this specific case but on the broader questions as to access to research materials that this case gives rise to. Thereafter, we will provide a constitutional justification for affixing liability on the state to secure the interests of the authors and the publication houses while ensuring that students and researchers have affordable access to knowledge formally secured through the right to education. We will then argue that, owing to the state's failure to secure such access, shadow libraries remain the most effective channel to secure the enjoyment of the right to education in terms of adequate access to research materials. We then argue how the use of such shadow libraries has been dealt with by courts in other jurisdictions. We conclude by arguing that the conduct of the shadow libraries at issue falls within the ambit of the fair dealing provisions in Indian copyright law that pertain to research and education.

II. SETTING THE SCENE

Four plaintiffs, Elsevier, Wiley India, Wiley periodicals and American Chemical Society, have filed a lawsuit against LibGen and Sci-Hub. In their lawsuit, the plaintiffs describe themselves as comprising of entities 'within 3 top-tier, global publishing houses in the field of scientific and academic publications.'⁵ They contend that they have expended enormous energy and effort in 'distribution/issuing copies, reproduction, storage, adaptation, communication and/or making available' their materials which are protected as literary works.⁶ They contend that they are the exclusive owners of the rights to reproduce, distribute and communicate the works to which this lawsuit relates.⁷

The plaintiffs contend that Sci-Hub and LibGen 'substantially indulge in online piracy by making available for viewing and download, providing access to, and communicating to the public' their copyrighted material. They contend that the defendant websites have the primary purpose/effect of infringing, facilitating or inducing infringement and are also liable for

⁵ Plaintiff in *Elsevier Ltd v Alexandra Elbakyan* 2022 SCC OnLine Del 3677 (Delhi High Court) [on file with the author], [6].

⁶ *ibid* [16].

⁷ *ibid* [19].

contributory infringement. This is because the two websites ‘actively encourage viewing/downloading of original literary works for which the Plaintiffs have exclusive rights.’ Defendant Nos. 3-11 are Internet/Telecom Service Providers who have been arraigned as defendants for the effective implementation of the court’s directions. Defendants 12 and 13 are the Department of Telecom and the Union Ministry of Electronics and Information Technology, whose assistance the plaintiff seeks in ensuring compliance with any orders of injunction and for the protection of their rights.

On the first date of listing, after recording the contentions of the parties, the Court took on record Defendant No. 1’s undertaking that no new articles or publications, in which the plaintiffs have copyright, will be uploaded or made available, via the internet, till the next date of hearing.⁸ This understanding has continued to hold good to date, as reflected by the order dated May 13, 2022. Pertinently, on February 10, 2022, the Court rejected an intervention application filed by three researchers who sought to intervene in the case. They argued that the works in question are of use to researchers like them and that taking them off the Internet would have a deleterious impact on public interest.⁹

The Court rejected this application on the ground that the mere fact of the researchers being adversely impacted cannot be a valid basis for allowing the intervention.¹⁰ It seemed to be concerned about the ‘slippery-slope’ effect of allowing the intervention, reasoning that doing so would ‘seriously impact the prosecution of the proceedings in the Court.’¹¹

With respect, the Court clearly failed to grasp the significance of these proceedings for access to research and academic material. It failed to acknowledge that these infringement proceedings are not ‘run-of-the-mill’. Hearing the interveners would have helped it to understand the full consequences of stopping the defendants’ activities. This understanding could have fed into an evaluation of whether their activity is fair. The Court’s myopic approach does not augur well for its final determination, from the standpoint of promoting access to education and research. For the sake of completion, it bears mention that, vide order dated 03.11.2022, the Court rejected an application by Defendant No. 1, Alexandra Elbakyan, to amend her written statement. Elbakyan sought to change her stance on the admission of the plaintiff’s copyright. The Court held that she had admitted in the written

⁸ *Elsevier Ltd v Alexandra Elbakyan* 2022 SCC OnLine Del 3677 (Delhi High Court) [6.2].

⁹ *ibid* [6].

¹⁰ *ibid* [7].

¹¹ *ibid* [10].

statement that the plaintiffs were the copyright owners with respect to the material on their platform and that she could not go back on this admission vide an amendment. The last order in the case is dated 09.02.2023. In this order, the Court rejected Elbakyan's plea that the plaint should be rejected under Order 7, Rule 11 of the Civil Procedure Code, on the basis that the assignment agreements between the plaintiffs and authors lacked monetary consideration. The Court held that Elbakyan had categorically admitted the plaintiff's copyrights over the works in question, and therefore the issue as to the proper construction to be placed on the assignment agreements, is not a pure question of law. It further held that the issue as to whether these agreements embody adequate and sufficient consideration is a factual question that cannot be determined at this stage. The volume of such agreements placed on record by the plaintiffs prima facie demonstrated their ownership of copyright over the works in question. It finally held that the assignment agreements form the basis for the plaintiff's copyright ownerships over the works that Elbakyan has allegedly infringed and hence rejected Elbakyan's argument that the agreements are not relevant to the plaintiff's case against Elbakyan.¹² The court decided to proceed *ex parte* against Lib Gen as they were not represented by counsel and had not filed written statement despite service of summons¹³ and listed the matter next on 12th July.¹⁴

III. RECALIBRATING THE DEBATE

The publishing market is a 10-million-dollar market. The publishers have one of the highest profit margins of around 40%. The reason for these high-profit margins is not the price of publishing but the monopoly that these publishers enjoy in this market.¹⁵ Not only lesser affluent countries like India, but even richer universities like Harvard University have expressed concerns over the high prices that can go up to 40,000 Dollars.¹⁶ Resultantly, readers are unable to procure the subscriptions to these journals and are generally dependent on well-resourced institutions for the same.¹⁷ Many authors

¹² *ibid* [5].

¹³ *ibid* [7].

¹⁴ *ibid* [8].

¹⁵ 'Are Royalties Fair? A Publisher Weighs In' (*The Passive Voice*, 8 June 2021) <<https://www.thepassivevoice.com/are-royalties-fair-a-publisher-weighs-in/>> accessed 29 January 2023.

¹⁶ Suzanne Day and others, 'Open to the Public: Paywalls and the Public Rationale for Open Access Medical Research Publishing' (2020) 6 *Research Involvement and Engagement* <<https://researchinvolvement.biomedcentral.com/articles/10.1186/s40900-020-0182-y>> accessed 29 January 2023.

¹⁷ Theres Sudeep, Copyright Case Sparks Debate on Access to Academic Journals (Deccan Herald, 15 January 2021) <<https://www.deccanherald.com/metrolife/metrolife-your-bond->

including Philip Pullman, the president of the society of authors, have repeatedly raised concerns over the increasing turnovers of the publishers and the falling revenues that are eventually shared with the authors.¹⁸

Even though the authors hold the copyright over literary works, they can assign it to the publisher. As per the 2015 amendment to Section 18 of the Copyright Act, the authors cannot wave off their right to receive royalty. The provision mandates that the authors are entitled a minimum of 50% of royalties. Despite the utopia imagined in this provision, the reality of the industry is very different. Authors often allege that royalty contracts are drafted in legalese, publication houses do not share the sale statements with the authors, they do not respond to correspondences for months, they do not make payments despite reminders and sometimes cite reasons like austerity and charity to evade their legal responsibility to share royalties with the authors. Just besides the opaqueness of the process, the unequal bargaining power between the authors and the publishers compounds the vulnerability of the authors. Given that authors are dependent on the publication houses for printing, marketing, distribution and promotion of their works, they do not raise objections even when the royalty agreements are not fair. This shows that the inequality of bargaining power between the authors and the publication houses is stark.

Further, the authors cannot engage in the business of issuing or granting of copyright licenses except through copyright societies as per Section 33 of the Copyright Act. However, authors still engage in third party licensing under Section 18 and Section 30 of the Copyright Act which enables the authors to assign their copyright to third parties. The conflict between Section 18 and Section 33 has been muddled by various high courts as some say that absolutely no transfer of copyright can take place without the involvement of copyright societies.¹⁹ While others say that the authors can assign their copyright to third parties.²⁰ Further, even if authors stop third party licensing altogether, copyright societies still have lesser clout as compared to publication houses, as the copyright society can have as less as 7 members. Given the financial capital and power capital held by authors, it is unlikely for these

with-bengaluru/copyright-case-sparks-debate-on-access-to-academic-journals-939283.html> accessed 29 January 2023.

¹⁸ Alison Flood, 'Philip Pullman Calls for Authors to Get Fairer Share of Publisher Profits' (The Guardian, 5 March 2018) <<https://www.theguardian.com/books/2018/mar/05/philip-pullman-calls-for-authors-to-get-fairer-share-of-publisher-profits>> accessed 29 January 2023.

¹⁹ Writ proceedings in *Event and Entertainment Management Assn v Union of India* 2017 SCC OnLine Del 12740.

²⁰ *Leopold Cafe & Stores v Novex Communications (P) Ltd* (2014) SCC OnLine Bom 4801.

smaller copyright societies to have much bargaining power. This shows that even copyright societies are unable to bridge the unequal bargaining power between the authors and publication houses.

The above discussion shows that the high selling prices of these books and journal articles are attributable to the publishers and not the authors. In fact, authors are not even decisive voices in the process of pricing. Rather, they are rather in a disadvantageous position as against the big publication houses. When readers are made to pay high prices, they are not benefitting the authors as much as they are benefitting the publishers. Acknowledging the key stakeholders in the Sci-Hub dispute, who are the publishers and readers, instead of framing it in the language of authors versus readers will help us in realising that the contestation is between the commercial interests of the publishers and the reader's right to access knowledge and academic material, and not between the author's right to be fairly compensated and the right of the readers to access academic material. That said, the interests and role of authors cannot be ignored altogether in this equation. Authors have to work with big publishing houses for the reputational capital, editing services, and marketing power that this brings. It is therefore imperative to find middle paths to resolve this issue that also accounts for the interests and concerns of authors, without foregrounding them.

As shown above, publishers hold immense bargaining power and their monopoly hurts the rights of both authors and readers. While legal regulation is doubtless an important step in levelling the playing field, as we have indicated with reference to the royalty example, legal regulation alone is inadequate to achieve this objective. In this paper, we look at the role that the state can play in this situation.

There is a need to have a player who is better placed than the authors and the readers to balance out this unequal bargaining power. For all practical purposes, the state clearly has more financial capacity to bear this liability. We are cognizant of the risks to free speech that flow from the state wielding the power to control access to materials. A detailed discussion of this issue is beyond the scope of this paper. However, we submit that with the requisite accountability from academicians and civil society, the state can provide much-needed financial cushion to universities to access paywalled material. While at the same time ensuring that the freedom of speech and expression is not curtailed.

Beyond its ability, there is also a strong constitutional justification for affixing the liability on the state. In the next section, we will delineate this constitutional justification. We will do so by laying down the broad contours

of the Right to Education ('RTE') and will then contextualize it within the debate around shadow libraries.

IV. CONSTITUTIONAL JUSTIFICATION

A. The Historical Background

Before independence, the British government did not show much interest in sponsoring the educational institutions in India.²¹ The constituent assembly, however, acknowledged that education was a vital factor in the progress of the nation. In fact, the Sub Committee on Fundamental Rights of the Constituent Assembly had also recommended that an enforceable right to education ('RTE') should be included in the fundamental rights chapter. However, various members of the constituent assembly including Sir Alladi Krishnaswamy Aiyar, Sardar K.M. Panikkar and Sir Govind Ballabh Pant believed that an overarching RTE could open a floodgate of claims that the state could not have handled.²² Pursuant to their opposition, RTE was included in Part IV of the constitution which speaks of the Directive Principles of State Policy ('DPSPs').²³ Resultantly, at the time of the adoption of the constitution, RTE was not an enforceable fundamental right and was a merely an unenforceable principle to guide the state's policies.

In Part IV of the Constitution, the RTE enjoyed an elevated position. Specifically, Article 36 of the draft constitution guaranteed RTE [which was analogous to article 45 in the final draft] started with 'every citizen is entitled to' even when other DPSPs started with the 'state shall endeavour to' language. Various members like Pandit Lakshmi Kante and Rd. B. R. Ambedkar objected to the same noticing the anomaly in the phrasing of the article and stating that such a phrasing could lead to a conflation of DPSPs and fundamental rights.²⁴ Resultantly, the article was amended and it was rephrased as: "The State shall endeavour to provide, within a period of ten years from the commencement of this Constitution, for free and compulsory education for all children until they complete the age of fourteen years."

²¹ Manas Chutia, 'Growth and Development of Education in India During British Period in a Historical Perspective' (2020) 11(9) *International Journal of Management* 1464.

²² Nalini Juneja, 'Is Blocked Chimney Impeding Access to Secondary Education in Some Cities and Inducing Dropout in Municipal Primary Schools' (2005) 35 *Niepa Occasional Paper* <<http://niepa.ac.in/new/download/Publications/Occasional%20Paper%20No.%2035.pdf>> accessed on 29 January 2023.

²³ Jai S Singh, 'Expanding Horizons of Human Right to Education: Perspective on Indian and International Vision' (2010) 52(1) *Journal of the Indian Law Institute* 34.

²⁴ PP Rao, 'Fundamental Right to Education' (2008) 50(4) *Journal of the Indian Law Institute* 585.

Interestingly, despite being unenforceable, it was the only DPSP to provide a time frame for the government to fulfil its obligation.

The status of this DPSP underwent gradual transformation into a fundamental right. In the case of *Mohini Jain v State of Karnataka* ('*Mohini Jain*'), the Supreme Court recognized that RTE was a multiplier that enabled an individual to enjoy other rights.²⁵ It further noted that 'It is primarily [sic] the education which brings forth the dignity of a man . . . An individual cannot be assured of human dignity unless his personality is developed and the only way to do that is to educate him.' While recognizing the centrality of education in the advancement of an individual, it observed that 'We hold that every citizen has a 'right to education' under the Constitution. The State is under an obligation to establish educational institutions to enable citizens to enjoy the said right.' It categorically read RTE into article 14 and 21 of the Constitution.

Further, in the case of *Unni Krishnan, J.P. v State of A.P.*,²⁶ the Supreme Court clarified that the judicially crafted obligation to provide free and compulsory education extended only to children below the age of 14 years. In this case, the court also took an opportunity to reprimand the government institutions for the lackadaisical enforcement of article 45. It concretized the enforceability of this DPSP by categorically remarking that every child who was denied RTE, could seek the issuance of the writ of mandamus against the appropriate authority, for the enforcement of the right.

These judicial interventions fostered a movement outside courts. various non-government and civil society organizations coordinated their efforts which culminated establishment of the National Alliance for the Fundamental Right to Education ('NAFRE'). Other collectives that were committed to the abolition of child labour including the South Asian Coalition on Child Servitude ('SACCS') and Campaign Against Child Labour ('CACL') also joined the NAFRE.²⁷ In response to this growing movement, the government sort to translate article 45 into a justiciable right via the 83rd Amendment Bill in 1997.

RTE finally translated into a fundamental right through the 86th Constitution Amendment Act, 2002. Pursuant to the same, article 21A was added and it states: "21A. The State shall provide free and compulsory

²⁵ *Mohini Jain v State of Karnataka* (1992) 3 SCC 666.

²⁶ (1993) 1 SCC 645; 1993 AIR 2178.

²⁷ John Harriss, 'Universalizing elementary education in India: Achievements and challenges' (2017) 3 UNRISD <<https://www.econstor.eu/bitstream/10419/186098/1/1010306782.pdf>> accessed 29 January 2023.

education to all children of the age of six to fourteen years in such manner as the State may, by law, determine.”

This is how the RTE became a justiciable right. The statutory manifestation of this constitutional provision can be seen in the Right to Education Act, 2009 which provides the legal framework and the roadmap for materializing this RTE.

B. Expansion by the Courts:

In the following section, we will trace the evolution of the RTE in the courtrooms, to show how it has acquired the shape and colour of a justiciable right for the citizens and a positive obligation for the state. The Supreme Court has held, in the context of fundamental rights in general²⁸ and the RTE in particular²⁹, that the realization of such rights, and the RTE in particular, must be pursued, notwithstanding the existence of resource constraints. The state, therefore, cannot deny fundamental rights to citizens on the ground of austerity. For instance, to draw on an example unrelated to the RTE, in the case of *Municipal Council, Ratlam v Shri Vardichan*,³⁰ the inhabitants of Ratlam brought a suit against the municipality on the ground that it had failed to provide for appropriate sanitary facilities, despite the orders from the magistrate under Section 133 CRPC. The municipality argued that it could not comply with the orders of the magistrate due to lack of financial resources. The court held that “The right of the people to live in a clean and healthy environment is a basic human right, fundamental to live a decent life, the violation of which will be considered a violation of basic right to life.” It further noted that the municipality could not cite financial difficulties as a reason for denying the right to life to the inhabitants. This general principle is also applicable to the right to education.

More specifically on the question of RTE and resource constraints, the pre-RTE act judgement rendered in *Unni Krishnan, J.P.*, introduced a qualifier to the judicially crafted RTE by stating that the obligation of the state was contingent on capacity constraints.

But besides this judgement, the supreme court has taken a pro-RTE stance in a catena of judgements. For instance, In *State of Bihar v Bihar Secondary Teachers Struggle Committee*³¹, it was held that the interpretation placed on the right must be one that helps make its realization a reality.

²⁸ *Municipal Council, Ratlam v Vardichan* (1980) 4 SCC 162: AIR 1980 SC 1622.

²⁹ *Avimash Mehrotra v Union of India* (2009) 6 SCC 398.

³⁰ *Municipal Council, Ratlam v Shri Vardichan* (1980) 4 SCC 162.

³¹ (2019) 18 SCC 301.

In *State of H.P. v H.P. State Recognised and Aided Schools Managing Committee*³², it was held that lack of financial capacity could not be cited as an excuse for denial of the RTE to children under the age of 14 years. Further in the case of *Avinash Mehrotra v Union of India*³³, the Court observed that a RTE placed an affirmative burden on all participants in our civil society for its meaningful realization. Its enforcement was not dependent on the cost involved and capacity constraints of the state.³⁴ In a similar vein, the supreme court in the case of *Ashoka Kumar Thakur v Union of India*³⁵, re-affirmed the judgement in *Mohini Jain* by stating that RTE enabled the realization of other rights. The Court must supervise the government spending on free and compulsory education as RTE plays an important role in unleashing the potential of the individual and the progress of the nation.³⁶ Further, in *Anuradha Bhasin v Union of India*³⁷, the Supreme Court held that RTE was unique amongst all other fundamental rights. This is because, while the latter are negatively worded, the RTE is positively worded, encompassing an obligation on the state to ensure that children between the age of 6-14 have access to education.

More recently during the pandemic when education shifted online, the Supreme Court heard a plea by the managements of unaided recognized schools in Delhi for exempting them from bearing the cost of providing equipment' and internet packages to students from economically weaker Sections. They further claimed reimbursement from the state for the costs that would be incurred in providing the technological equipment' and internet facilities. The state cited lack of resources and pushed back against the plea. The court recognized that students from economically weaker sections/disadvantaged groups were unable to realize their RTE in a meaningful manner due to the stark inequalities. It further noted "The State cannot wash its hands of the obligation imposed particularly by Article 21 A of the Constitution.' It also held that the 'needs of children from the underprivileged sections to receive adequate access to online education cannot be denied.'³⁸

Two conclusions emerge from the above survey of case laws. First, the Supreme Court has placed an affirmative duty on the state to realize RTE which puts this right on an elevated footing vis-a-vis other fundamental right

³² (1995) 4 SCC 507.

³³ (2009) 6 SCC 398.

³⁴ *ibid.*

³⁵ (2008) 6 SCC 1.

³⁶ *ibid* [466].

³⁷ (2020) 3 SCC 637.

³⁸ *Action Committee Unaided Recognized (P) Schools v Justice for All 2021 SCC OnLine SC 3301* [4].

(which are all negatively worded). Second, that resource constraints cannot be cited as a valid justification for a failure to realize the RTE.

C. RTE as Justification for the Continued Existence of Shadow Libraries

These conclusions are extremely relevant for recalibrating the debate around the shadow library case. Even though article 21A provides for free and compulsory education only to children aged between 6-14 years, the recognition of a facet of education as a fundamental right has positively influenced the judiciary's approach to cases involving educational access. To illustrate, in a case concerning the denial of admission to a medical college, the Supreme Court noted:

We would like to take this opportunity to underscore the importance of creating an enabling environment to make it possible for students, such as the petitioners, to pursue professional education. While the right to pursue higher (professional) education has not been spelt out as a fundamental right in Part III of the Constitution, it bears emphasis that access to professional education is not a governmental largesse.³⁹

The Court noted that the government has an affirmative obligation to facilitate access to education, at all levels.⁴⁰ It traced the recognition of the right to professional education in international human rights law. Further it noted that a key area where government intervention is mandated is 'economic accessibility' so as to ensure that 'financial constraints do not come in the way of accessing education.'⁴¹

Consequently, there is a credible basis to obligate state intervention to facilitate access to educational content, even at the professional level.

D. Affixing the Liability on the State

As things stand now, books and articles which can facilitate learning, research and creation of academic works are mostly paywalled by publishers.⁴² As the survey of the case law in the above two segments makes clear, the interpretation of the RTE adopted by the Supreme Court [and its impact on the right to access professional education as well] can be interpreted as an

³⁹ *Farzana Batool v Union of India* 2021 SCC OnLine SC 3433 [9].

⁴⁰ *ibid.*

⁴¹ *ibid* [11].

⁴² Isabella Liu, 'Opinion: It's Time for the Academic Paywall to Fall' (The Varsity, 13 March 2022) <<https://thevarsity.ca/2022/03/13/opinion-no-more-academic-paywall/>> accessed 29 January 2023.

entitlement to access research material that is paywalled or otherwise unaffordable/inaccessible to a majority of students. Given that users themselves are unable to afford access to this paywalled material, the obvious course of action is to affix the liability for the realization of the RTE on the institutions they are affiliated to. Since Article 21-A is only enforceable against the state, the only viable alternative is to obligate the state to enable these institutions to provide access to this academic material, to students and researchers. In a scenario where the full realization of the RTE is contingent on accessing this copyrighted material, it is natural that the state takes up the job of negotiating with the publishers and databases, buying subscriptions and securing licenses. This is not just useful from a rights perspective; but is also likely to yield more efficient results. These macro contracts between the state and the publishers can be far more uniform and certain. This can reduce the transaction cost for both the publishers as well as the government and private universities as one entity that is the state will get involve in these negotiations. Lastly, it can also address the problem of unequal bargaining power between the universities and the publishers where the former is dependent on the latter for facilitating educational research and writing while the latter enjoys immense control and monopoly over the publication and distribution of academic material.

In order to play a more active role in this equation, the government has launched the ‘one nation, one subscription’ project to buy a bulk subscription to multiple journals.⁴³ Inspiration can be drawn from the program launched by the European Commission and the European Research Council which aims at providing full and immediate open access to research publications. It focuses on ‘Plan S’, which mandates that research funders would have to ensure that research publications generated through grants allocated by them are openly accessible and not monetized in any way.⁴⁴ In view of the above discussion, a constitutionally ideal outcome would be to have the state to facilitate access to paywalled material so that the RTE can be fully realized through state intervention. This would ensure that authors are fairly compensated for their work and that readers have access to academic material without incurring any out-of-pocket costs. However, doctrinal expectations are often divorced from empirical realities.

⁴³ Anubha Sinha, ‘The STI Policy Proposes a Transformative Open Access Approach for India (*Centre for Internet and Society*, 21 January 2021) <<https://cis-india.org/a2k/blogs/the-sti-policy-proposes-a-transformative-open-access-approach-forindia>> accessed 29 January 2023.

⁴⁴ ‘About Plan S’ (*Plan S*) <<https://www.coalition-s.org/>> accessed 29 January 2023.

Specifically, there continues to remain widespread unaffordability to research material in India today.⁴⁵ We shall develop this point further when discussing the fair dealing educational exception in Indian copyright law. For the present discussion, it suffices to state that the existence of the problem of widespread unaffordability provides evidence of the failure of the government to secure access to copyrighted material for all, making access to shadow libraries imperative.

Given this position, the question that arises is whether the state, acting through its judicial wing, should block access to copyrighted material, thereby imperilling the RTE of those who depend on it. Our answer would clearly be in the negative. When the role of shadow libraries in realizing the RTE is acknowledged, it becomes clear that the court should not frustrate the realization of the RTE by finding the operation of shadow libraries to be illegal.

We will now turn to a consideration of how LibGen and Sci-Hub have been dealt with in other jurisdictions, with a view to determine what lessons can be drawn through this comparison for India.

V. COMPARATIVE EXPERIENCE

In France, a complaint was filed in the High Court of Paris by the publishers Elsevier and Springer Nature against, inter alia, LibGen and Sci-Hub. This led to an order to four Internet Service Providers in France to block Sci-Hub and LibGen sites for the year to come. The court reasoned that the two sites ‘clearly claim to be pirate platforms rejecting the principle of copyright and bypassing publishers’ subscription access portals.’⁴⁶

In Sweden, in December 2019, the Swedish Patent and Market Court issued a dynamic blocking injunction on December 9, in case PMT 7262-18 between AB Svensk Film industri and the Swedish digital service provider Telia Sverige AB. The same court further issued a dynamic blocking injunction against the aforesaid DSP. The injunction directed the DSP to block customer access to file sharing services on current domain names and web addresses and artifices designed to circumvent the ban. Claimants were to

⁴⁵ Swaraj Paul Barooah, ‘Time to More Seriously Question the Spectre of Copyright in the Realm of Education’ (*SpicyIP*, 23 December 2022) <<https://spicyip.com/2020/12/time-to-more-seriously-question-the-spectre-of-copyright-in-the-realm-of-education.html>> accessed 29 January 2023.

⁴⁶ Ernesto Van der Sar, ‘French ISPs Ordered to Block Sci-Hub and LibGen’ (*TorrentFreak*, 31 March 2019) <<https://torrentfreak.com/court-orders-french-isps-to-block-sci-hub-and-libgen-190331/>> accessed 3 January 2022.

inform the DSP of infringing access on which the DSP were to act within two to three weeks to block those services.⁴⁷

In the United States, a temporary and permanent injunction was granted against Sci-Hub. A lawsuit was instituted by the American Chemical Society ('ACS') in the Southern District of New York. In an order in October 2015, the judge held that ACS had established a good prima facie case based on the evidence to show Sci-Hub's activities and Alexandra Elbakyan's admission as to Sci-Hub's activities. The court held that, while there is certainly a need to ensure broad access to scientific material, Elbakyan's solution is not in the public interest. This is because it upsets the delicate ecosystem that fosters scientific research. Inadequate protection of copyrighted material might imperil scientific research, it reasoned.⁴⁸ Importantly, the fair dealing exception for research and education in Indian copyright law, it is submitted, make this reasoning in apposite for India. In the US case, the court did briefly consider the fair use exception. However, it held that the exception would only permit the use of Elsevier's articles in certain circumstances and not wholesale infringement.⁴⁹ The fair dealing exceptions that we shall subsequently discuss are encoded into the delicate ecosystem created in India to foster the creation of copyrighted material. The moment a use falls within the ambit of a recognized fair dealing exception, it is legally permissible. We will explain why the finding of the US court as to the application of the fair use exception will not hold good in the Indian context, given the broad language of the relevant fair dealing exceptions and the judicial interpretation that has been placed on them. The way the operation of shadow libraries falls within these two fair dealing exceptions shall be discussed later in this paper.

Reverting to the US case, in October 2017, the court granted ACS a permanent injunction against Sci-Hub. It found that Sci hub had: 'systematically infringed ACS's copyrighted works.'⁵⁰ In Austria, following guidance from the regulator, LibGen and Sci-Hub were blocked.⁵¹

⁴⁷ Neil Wilkof, 'The Swedish Patent and Market Court Issues its First Dynamic Blocking Injunction' (*The IPKat*, 23 January 2020) <<https://ipkitten.blogspot.com/2020/01/the-swedish-patent-and-market-court.html>> accessed 3 January 2022.

⁴⁸ *Elsevier Inc. v www.Sci-Hub.org*, 15 Civ 4282 (RWS).

⁴⁹ *ibid* 16.

⁵⁰ Andrea Widener, 'ACS Prevails over Sci-Hub in copyright suit' (*Chemical & Engineering News*, 7 November 2017) <<https://cen.acs.org/articles/95/i45/ACS-prevails-over-Sci-Hub.html>> accessed 25 January 2023

⁵¹ Glyn Moody Fri, 'Elsevier Gets Sci-Hub and LibGen Blocked in Austria, Thereby Promoting the Use of VPNs and Tor in the Country' (*Techdirt*, 15 November 2019) <<https://www.techdirt.com/articles/20191112/08504743369/elsevier-gets-sci-hub-libgen-blocked-austria-thereby-promoting-use-vpns-tor-country.shtml>> accessed 3 January 2022.

A brief survey of comparative jurisprudence, therefore, makes clear that the operation of shadow libraries has been frowned upon by courts. However, as Elbakyan points out in her written submissions,⁵² none of these jurisdictions had the progressively worded research and educational exceptions that India does and nor were the shadow libraries represented in these cases. This is therefore a unique opportunity for an Indian court to adopt a progressive interpretation of Indian copyright law that is consistent with the constitutional culture around the RTE, the need for accessibility and the socioeconomic realities that prevail in India.

The matter can be looked at through another angle also. The operation of these shadow libraries arguably fits within the ambit of the fair dealing provisions that relate to research and education in Indian copyright law. It is this fair dealing argument that we turn to next.

VI. COPYRIGHT LAW ANALYSIS

A. Basic Purpose of Copyright Law

It would be instructive to commence the analysis of fair dealing provisions by first exploring the purpose of copyright law, emerging from the case law. This understanding of the contextual peculiarities that prevail in India is also critical for making good our argument that the judgments in other countries, referenced above, would not have much persuasive force in India. Two cases in this regard bear emphasis.

First, the Jammu and Kashmir High Court held in *Romesh Chowdhry v Kh. Ali Mohamad Nowsheri*⁵³ ‘it is well settled that under the guise of copyright, authors cannot ask the court to close all the doors of research and scholarship and all frontiers of human knowledge.’ What is crucial in the quoted excerpt for this paper is the Court’s insistence that copyright cannot be weaponized to thwart access to knowledge.

Second, in *Rameshwari Photocopy Services*,⁵⁴ the single judge held that copyright is not a divine right or a natural right, and is a statutory right, which is subject to certain exceptions enumerated within the provisions of the Act. Copyright law is designed rather to stimulate activity and progress in the arts, for the intellectual enrichment of the public, and is intended to

⁵² Written Statement on behalf of Defendant No 1 in *Elsevier Ltd v Alexandra Elbakyan*, 2022 SCC OnLine Del 3677 (Delhi High Court) [on file with author] [81-82].

⁵³ 1965 SCC OnLine J&K 1: AIR 1965 J&K 101.

⁵⁴ *University of Oxford v Rameshwari Photocopy Services* 2016 SCC OnLine Del 6229.

increase, and not to impede, the harvest of knowledge. This finding was not disturbed by the Division Bench which affirmed the single judge's verdict.

As Defendant No. 1's written submission in the shadow library case indicates, the basis of the fair dealing provisions in copyright law can be traced to Article 19(1)(a) of the Constitution.⁵⁵ This sentiment is evident from the Delhi High Court's judgment in the case of *Wiley Eastern Ltd. v Indian Institute of Management*⁵⁶ in which the court held as follows: "the basic purpose of Section 52 is to protect the freedom of expression under Article 19(1) of the Constitution of India- so that research, private study, criticism or review or reporting of current events could be protected." This Constitutional basis for fair dealing provisions assumes significance, as it underscores the importance of having robust exceptions to a well-functioning copyright system. We submit that an Indian court that is called on to interpret whether the operation of shadow libraries falls within the four squares of Section 52(1)(a) and 52(1)(i) ought to foreground the above articulated purpose of copyright law. Having this purpose in mind will enable the court to evaluate the importance of shadow libraries from this vantage point.

B. Section 52(1)(a) of the Copyright Act

The text of the exception embodied in Section 52(1)(a) supports the interpretation being offered by the defendants. Specifically, the exception explicitly states that it is worded as 'including research'. Since it is a settled position that the use of 'including' is meant to give the terms used in a provision a broad interpretation,⁵⁷ the term 'research' has to be given an interpretation that means something. Further, such research envisaged by the provision would not merely be of a private nature. This is because, if the legislature's

⁵⁵ Written Statement (n 52) [9].

⁵⁶ 1995 SCC OnLine Del 784: (1995) 15 PTC 375.

⁵⁷ See, for instance, *CIT v Taj Mahal Hotel* (1971) 3 SCC 550:

The purport of interpretation of the expression 'includes' has to be in the context of the Act. This Court has held thus... The word 'includes' is often used in interpretation clauses in order to enlarge the meaning of the words or phrases occurring in the body of the statute. When it is so used, those words and phrases must be construed as comprehending not only such things as they signify according to their nature and import but also those things which the interpretation clause declares that they shall include.

See also, *S.K. Gupta v K.P. Jain* (1979) 3 SCC 54:

²⁴ The noticeable feature of this definition is that it is an inclusive definition and, where in a definition clause, the word 'include' is used, it is so done in order to enlarge the meaning of the words or phrases occurring in the body of the statute and when it is so used, these words or phrases must be construed as comprehending not only such things which they signify according to their natural import, but also those things which the interpretation clause declares that they shall include... But where the definition is an inclusive definition, the word not only bears its ordinary, popular and natural sense whenever that would be applicable but it also bears its extended statutory meaning.

intent was to merely cover private research, it would have stopped short at referring to ‘private or personal use’. There would have been no need to cover ‘research’ separately.⁵⁸

As Elbakyan points out in her written submissions, the sole purpose for which Sci-Hub makes available material on its website is research.⁵⁹ The use would therefore squarely fall within the ambit of the research exception.

This interpretation of the exception also has Constitutional backing. As MP Ram Mohan and Aditya Gupta point out, the judicial interpretation of Article 19[1][a] and Article 21 indicates that these fundamental rights encompass a right to research.⁶⁰ Specifically, in offering an expanded interpretation of Article 21 in the celebrated Francis Mullen case, the Supreme Court read the right as including facilities for: ‘reading, writing and expressing oneself in diverse forms.’⁶¹

A 1997 Supreme Court judgment read the right to life as including ‘social, cultural and intellectual’ fulfilments.⁶² A Delhi High Court judgment interpreted Article 21 as including ‘a right to acquire useful knowledge.’⁶³ Based on the broad conception of the right to life adopted in these cases, they conclude that Article 21 harbours constitutional protection for the right to research.⁶⁴

In the only Indian judgment that has thus far interpreted Section 52[1][a][i], the facts were as follows. The plaintiff had an exclusive license from the Central Board of Secondary Education to publish and reproduce class 10th and 12th question papers. The defendants published the same question papers for commercial gain.⁶⁵ The Court rejected the defendant’s argument on Section 52[1][a][i] on the ground that the defendant’s publication was for commercial exploitation.⁶⁶ Speaking through Justice Lahoti, the Court held:

“If a publisher publishes a book for commercial exploitation and in doing so infringes a copyright, the defence under Section 52(1)(a)(i)

⁵⁸ Written Statement (n 52) [33].

⁵⁹ *ibid* [31].

⁶⁰ M.P. Ram Mohan and Aditya Gupta, ‘Right to Research and Copyright Law: From Photocopying to Shadow Libraries’ (2022) 11(3) NYU Journal of Intellectual Property and Entertainment Law 249.

⁶¹ *Francis Coralie Mullin v UT of Delhi* (1981) 1 SCC 608 [8].

⁶² *Samatha v State of A.P.* (1997) 8 SCC 191 [247], [248].

⁶³ *Rabinder Nath Malik v The Regional Passport Officer, New Delhi* 1966 SCC OnLine Del 41 [24], [25].

⁶⁴ Mohan and Gupta (n 60). See generally Vandana Mahalwar, ‘On Copyright Protection’ (2015) 56 Economic and Political Weekly 7.

⁶⁵ *Rupendra Kashyap v Javan Publishing House* 1996 SCC OnLine Del 466.

⁶⁶ *ibid* [21].

would not be available.⁶⁷ As Mohan and Gupta note, the critical difference between the instant case and the shadow library case is that shadow libraries do not aim to obtain commercial returns.⁶⁸

An expanded understanding of what constitutes research can also be found in a Canadian Supreme Court judgment. In *Law Society of Upper Canada v CCH Canadian Ltd.*,⁶⁹ the Canadian Supreme Court adopted a broad interpretation of research, holding that activities incidental to research are also covered within the ambit of the term ‘research’. The Court held that users’ rights should not be ‘unduly constrained’ or ‘limited to non-commercial or private contexts.’⁷⁰ The Court held: ‘Although the retrieval and photocopying of legal works are not research in and of themselves, they are necessary conditions of research and thus part of the research process.’

In addition to the research exception, the conduct of the defendants would also fall within the ambit of the educational exception, as discussed below.

C. Educational Exception

Section 52[1][i] of the Copyright Act reads as follows:

- (i) the reproduction of any work-
- (ii) by a teacher or a pupil in the course of instruction; or
- (iii) as part of the questions to be answered in an examination; or
- (iv) in answers to such questions;

This exception fell for the interpretation of the Delhi High Court in the DU photocopy case.⁷¹ The Division Bench began its analysis by foregrounding the importance of education. In particular, the Court’s emphasis on equitable access to education is crucial here. It noted: ‘So fundamental is education to a society - it warrants the promotion of equitable access to knowledge to all segments of the society, irrespective of their caste, creed and financial position. Of course, the more indigent the learner, the greater the responsibility to ensure equitable access.’⁷²

⁶⁷ *ibid.*

⁶⁸ Mohan and Gupta (n 60) 43.

⁶⁹ 2004 SCC OnLine Can SC 13; (2004) 1 SCR 339.

⁷⁰ *ibid* [55].

⁷¹ See generally Lawrence Liang, ‘Paternal and Defiant Access: Copyright and the Politics of Access to Knowledge in the Delhi University Photocopy Case’ (2017) 1 *Indian Law Review* 36, 50.

⁷² *University of Oxford v Rameshwari Photocopy Services* 2016 SCC OnLine Del 6229 [30].

The Division Bench adopted a capacious interpretation of the exception. It held that the phrase ‘course of instruction’ means the entire process or programme of education in a semester and not the process of teaching in the classroom alone. Reliance was placed on the judgment of the High Court of New Zealand in *Longman Group Ltd. v Carrington Technical Institute Board of Governors*⁷³ where it was held that ‘course of instruction’ includes:

“anything in the process of instruction with the process commencing at a time earlier than the time of instruction, at least for a teacher, and ending at a time later, at least for a student. So long as the copying forms part of and arises out of the course of instruction it would normally be in the course of instruction.”

The Division Bench’s interpretation of the exception in the above terms assumes significance in the shadow library case. Education does not take place in silos. Activities including mandatory submission of projects and dissertations, writing of books and scholarly articles for academic accreditation form a part of the super structure of the educational system. Even if one of these activities is halted by paywalls, the pursuit of education is bound to be affected. This analysis supports the conclusion that the service offered by shadow libraries would fall within the educational exception.

Furthermore, there is convincing literature to demonstrate the inaccessibility of education in India. As Professor Scaria argues, given that many liberally funded universities in the West struggle to easily access scientific materials, one can only imagine the condition of researchers in the Global South.⁷⁴

In a paper, late Professor Basheer and colleagues show that most of the titles acquired by leading law schools in India were procured at prices corresponding to or higher than those prevailing in the West. At a leading law school, the National Law School of India University, some books are purchased using the concerned distributor’s foreign currency, further increasing the charge. The price also rises further in light of the cost of shipping.⁷⁵

In the same vein, Basheer and colleagues estimate the cost of two books for an American purchaser, assuming that such a purchaser would have to pay the same percentage of their income on buying the book as an Indian

⁷³ (1991) 2 NZLR 574.

⁷⁴ Arul George Scaria and Rishika Rangarajan, ‘Fine-tuning the Intellectual Property Approaches to Fostering Open Science: Some Insights from India’ (2016) 8 WIPO Journal 109, 111.

⁷⁵ Shamnad Basheer and others, ‘Exhausting Copyrights and Promoting Access to Education: An Empirical Take’ (2012) 17 Journal of Intellectual Property Rights 335, 341.

purchaser. They find that a book by Tsepon Wangchuk Deden Shakabpa would cost an overwhelming US\$ 5236. Similarly, the book ‘The Politics of Global Governance: International Organizations in an Interdependent World’ by Diehl and Frederking would cost US\$ 373.93 using this methodology.⁷⁶

In Delhi University, for instance, the subscription to around 40 journals have not been renewed since 2019.⁷⁷ A few other reports suggest that Indian Universities have outdated and sub-standard libraries.⁷⁸

Echoing the same sentiment, Sara Bannerman⁷⁹ argues that there exists a significant gap between developed and developing countries in terms of access and production of academic material. She points out that researchers in developing jurisdictions have hardly any access to academic materials because of high costs of subscription and the inaccessible and expensive distribution mechanisms. Researchers and other stakeholders involved in the research process have been adversely impacted by this gap.

It is also important to bear in mind the importance of shadow libraries in facilitating access to research and education for persons with disabilities [‘PwDs’]. For PwDs, lack of access to research materials is a huge issue. In India, for instance, only 1% of available books are accessible to the visually challenged. This is because such content is generally not available in soft copy form. Since shadow libraries make such content digitally available, they make content accessible to the visually challenged.⁸⁰ For those with locomotor disabilities, physically accessing libraries containing the research material they seek is a challenge. Shadow libraries make such access possible.⁸¹

This lack of access to research has a number of second order effects. For one thing, it results in the production of research outputs that are not as robust as they could be. Lack of affordable and accessible pathways to research means that individuals from marginalized backgrounds remain shut out from the research process. Absence of participation and inclusion

⁷⁶ *ibid.*

⁷⁷ Sukrita Baruah, ‘Subscriptions to More than 40 Databases not Renewed in DU, Research Takes a Back Seat’ (The Indian Express, 10 November 2019) <<https://indianexpress.com/article/education/subscriptions-to-more-than-40-databases-not-renewed-in-du-research-takes-a-back-seat-6112226/>> accessed 29 January 2023.

⁷⁸ ‘Govt College Library in Uttarakhand Keeps Outdated Books, Students Protest’ *National Herald* (13 July 2019) <<https://www.nationalheraldindia.com/national/govt-college-library-in-uttarakhand-keeps-outdated-books-students-protest>> accessed 29 January 2023.

⁷⁹ Sara Bannerman, *Access to Scientific Knowledge in International Copyright and Access to Knowledge* (Cambridge University Press 2016) 32-52.

⁸⁰ Rahul Cherian Jacob and others, ‘The Disability Exception and the Triumph of New Rights Advocacy’ (2012) 5 NUJS L Rev 603.

⁸¹ Written statement by Defendant No 1, p 90 [on file with the author].

of individuals from diverse backgrounds in the research process affects the diversity of the research produced and in turn also the quality of the research, and may also result in a failure to identify relevant research issues.⁸² As Cristin Timmermann points out, the unequal access to science for poorer researchers has the second order consequence of curtailing the diversity of scholarly outputs by making it one dimensional.⁸³

It suffices to say that shadow libraries serve the important function of ensuring equitable access to education and research – a goal whose importance the Division Bench in *Rameshwari* was at pains to underscore. Similarly, Professor David Vaver argues⁸⁴ that the grant of copyright is accompanied by a duty to keep the prices of copyrighted material reasonable and affordable. This is the essence of the copyright bargain. When copyright owners fail to uphold their side of the bargain (as is clear from the inaccessibility of research material), it is submitted that shadow libraries must be allowed to function as a legitimate corrective against this state of affairs.

Along the same lines, in General Comment 25, the Committee on Economic, Social and Cultural Rights emphasizes equal access to opportunities to participate in science. It recognizes the social function of IP. It calls on states to take measures to prevent: “unreasonably high costs for access to essential medicines, plant seeds or other means of food production, or for school books and learning materials, from undermining the rights of large segments of the population to health, food and education.”⁸⁵

Reverting back to the Division Bench’s judgment in the *DU* photocopy case, in order to determine if a use is fair, the Court held that the purpose of the use has to be seen.⁸⁶ And the determination of how much usage is fair will be decided based on whether the extent used is justified by the purpose. The Court held:

⁸² *ibid.*

⁸³ Cristin Timmermann, ‘Sharing in or Benefiting from Scientific Advancement?’ (2014) 20 *Science and Engineering Ethics* 111.

Also see, written statement by Defendant No. 1 [99] [on file with the author].

⁸⁴ David Vaver, ‘Publishers and Copyright: Rights Without Duties’ (2006) 24 *Oxford Legal Studies* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=902794> accessed 29 January 2023.

⁸⁵ Committee on Economic, Social and Cultural Rights, ‘General Comment No. 25 (2020) on Science and Economic, Social and Cultural Rights (arts 15(1)(b), (2), (3) and (4) of the International Covenant on Economic, Social and Cultural Rights)’ (UN Economic and Social Council, 30 April 2020) [62] <<https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=4slQ6QSmIBEDzFEovLCuW1a0Szab0oXTdImnsJZZVQdxONLLLJiul8wRm-VtR5Kxx73i0Uz0k13FeZiqChAWHKFuBqp%2B4RaxfUzqSAfyZYAR%2Fq7sqC7AH-Ra48PPRRALHB>> accessed 29 January 2023.

⁸⁶ *University of Oxford v Rameshwari Photocopy Services* 2016 SCC OnLine Del 6229 [32].

“33. In the context of teaching and use of copyrighted material, the fairness in the use can be determined on the touchstone of ‘extent justified by the purpose’. In other words, the utilization of the copyrighted work would be a fair use to the extent justified for purpose of education. It would have no concern with the extent of the material used, both qualitative or quantitative.”

Therefore, unlike Germany, for instance, where the fair dealing doctrine has quantitative limits, the Court eschewed the adoption of any such limits.⁸⁷

The Court therefore held that it does not matter whether the course-pack is reproduced in full from the textbook. The relevant question was whether the material used by the defendants was justified for the purpose of instructional use by the teacher to the class. This would require a consideration of the defendant’s course-packs with reference to: ‘the objective of the course, the course content and the list of suggested readings given by the teacher to the students.’⁸⁸

It may be argued that the DU photocopy judgment is inapplicable to the case at hand because the use here is of 100% of the copyrighted work. However, the above paragraph provides a complete answer to this charge. Arguably, the purpose of the use in the instant case is to enable affordable access to reading materials. This is self-evidently a fair purpose, as distinct, say, from the purpose of gaining commercial returns or capturing the plaintiff’s market. Since the purpose of the defendants is to serve as an affordable library, the extent justified is, arguably, the content in its entirety. This thus makes the defendant’s use acceptable as per the test outlined in the DU photocopy judgment.

Another crucial consideration in the fairness inquiry is the impact of the defendant’s work on the potential market for the plaintiff’s work. On this count, in the DU Photocopy judgment, the single judge [Justice Endlaw] concluded: ‘the students can never be expected to buy all the books, different portions whereof are prescribed as suggested reading and can never be said to be the potential customers of the plaintiffs.’⁸⁹ The Division Bench reaches two conclusions: [a] the beneficiaries of educational content are not ‘customers. [b]: the educational access provided by course-packs expands the market for the underlying copyrighted works, by making more people aware of the copyrighted content. Both these conclusions can be applied in the case at hand. First, the beneficiaries of the educational content that shadow libraries

⁸⁷ Mohan and Gupta (n 60) 32.

⁸⁸ *ibid* [56].

⁸⁹ *University of Oxford v Rameshwari Photocopy Services* 2016 SCC OnLine Del 6229 [87].

provide are also not ‘customers’, using the same logic that the DB deploys. Second, arguably, but for shadow libraries, students would not be exposed to much of the content provided by shadow libraries in the first place, settling instead for whatever resources they can readily access. By providing access to such content, shadow libraries expand the possibility of the content they host reaching more people and potentially expanding the footprint of the relevant publishers.

In addition, as Mohan and Gupta argue, individual researchers rarely buy subscriptions of libraries; they access research material principally through libraries. Pointing to their own paper, Mohan and Gupta argue that it would have been impossible for them to formulate the same, were it not for their university’s library access, either through subscriptions or inter-library loans.⁹⁰

Further, as defendant no. 1 points out in its written submissions, it earns no financial returns for its services. The only financial returns that it earns are in the form of voluntary donations. And the amount so donated is not used for ‘personal profit, for the purpose of trade, or to prejudicially affect the economic interests of the copyright owners.’⁹¹

To those contending that this interpretation of Section 52[1][i] is overbroad and makes the rights of copyright owners a dead letter, the DB offers a good answer. The court holds: “Thus, it is possible that the melody of a statute may at times require a particular Section, in a limited circumstance, to so outstretch itself that, within the confines of the limited circumstance, another Section or Sections may be muted.”⁹² Given the above analysis, the holding of DU photocopy commends itself for application on all fours to the case at hand.

In the DU photocopy judgment, the DB rejected the four-factor analysis for evaluating whether a defendant’s conduct constitutes fair dealing that had been affirmed by the Delhi High Court in the case of *India TV Independent News Service (P) Ltd. v Yashraj Films (P) Ltd.*⁹³ and *ICC Development (International) Ltd. v New Delhi Television Ltd.*⁹⁴ Even so, we have evaluated the instant case from the standpoint of these four factors, for the sake of completeness. These four factors have been statutorily spelt out in Section 107 of the US Copyright Act, embodying the fair use doctrine in that jurisdiction. The factors are:

⁹⁰ Mohan and Gupta (n 60) 47.

⁹¹ Written Statement (n 52) [23].

⁹² *University of Oxford v Rameshwari Photocopy Services* 2016 SCC OnLine Del 6229 [77].

⁹³ 2012 SCC OnLine Del 4298.

⁹⁴ 2012 SCC OnLine Del 4919.

- (1) the purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.

Nikhil Purohit has conducted an illuminating analysis of how these factors can be applied in the case at hand.⁹⁵ Apropos the first factor [purpose and character of use], the defendants are making academic articles available free of cost, making the use one for a ‘non-profit educational purpose’. As Elbakyan indicated in an interview to the Wire, Sci-Hub’s aim is to ensure that science is not monopolized by a few but is in fact ‘a dynamic network of learned societies’.⁹⁶ Further, in 2015, Sci-Hub removed from its archive some journals that ‘exemplify openness.’⁹⁷ Based on this evidence, as Mohan and Gupta contend, it can be plausibly argued that the purpose of the operation of these shadow libraries is: ‘facilitating research and democratising the availability of academic scholarship.’⁹⁸ The defendants, we submit, could also argue that their use of the underlying content is transformative. This is because they index the content and make it more easily available. While the defendants do receive donations for their operations, these are not sufficient to make the activity they engage in commercial, as explained earlier.

On the second factor [nature of the work copied], typically, the more creative the content that is copied, the less likely the copying is to constitute fair dealing. Conversely, the more factual the underlying content, the more likely is the court to support a finding of fair use.⁹⁹

⁹⁵ Nikhil Purohit, ‘Sci-Hub and Libgen Up Against Academic Publishers: A Death Knell for Access to Research? – Part II’ (*SpicyIP*, 28 December 2020) <<https://spicyip.com/2020/12/sci-hub-and-libgen-up-against-academic-publishers-a-death-knell-for-access-to-research-part-ii.html>> accessed 18 June 2022.

⁹⁶ Sidharth Singh, ‘An Interview With Sci-Hub’s Alexandra Elbakyan on the Delhi HC Case’ (*The Wire Science*, 22 February 2021) <<https://science.thewire.in/the-sciences/interview-alexandra-elbakyan-sci-hub-elsevier-academic-publishing-open-access/>> accessed 21 February 2022.

⁹⁷ Daniel S Himmelstein and others, ‘Research: Sci-Hub Provides Access to Nearly All Scholarly Literature’ (2018) 7 *eLife* e32822, 4.

⁹⁸ Mohan and Gupta (n 60) 43.

⁹⁹ ‘More Information on Fair Use | U.S. Copyright Office’ <<https://www.copyright.gov/fair-use/more-info.html>> accessed 18 June 2022.

In the instant case, this determination would depend on the content of each article being copied. In general, however, as Purohit argues, it is safe to assume that academic articles are more factual than creative. This factor, therefore, would support a finding of fair dealing.

On the third factor [amount and substantiality of use], the defendants reproduce the full text of the articles concerned. Consequently, this factor would, *prima facie*, weigh in the plaintiffs' favour. However, as Mohan and Gupta point out, copying a plaintiff's copyrighted material in its entirety is not dispositive in a fair dealing/use analysis. Specifically, relying on the Hathi Trust and Google Books cases in the United States, they argue that: 'when public interest dictates, a complete appropriation of the copyrighted material cannot be the singular yardstick to determine a fair-use analysis.'¹⁰⁰

The fourth factor [the effect of the use upon the potential market for or value of the copyrighted work], is likely to be the subject matter of some contestation. However, as explained earlier, the defendants, on balance, have a good case on this score. Consequently, an evaluation of the defendants' conduct through this framework would also support a finding of fair dealing.

VII. CONCLUSION

The shadow library litigation brings into focus the need to introspect on whether the publishing industry is attaining its founding objectives. As Divij Joshi notes, Sci-Hub is not the ideal solution (notwithstanding our argument that it is legal) to the problem of access to research. However, the litigation should serve as a launching point to initiate a conversation on developing new business models in the publishing industry, the way Napster did for the music industry or Netflix did television.¹⁰¹ The fact of the matter is that even though these shadow libraries are unable to ensure optimal access to research materials; they are able to improve the level of access. It is necessary to explore systemic solutions to overhaul the publishing industry. Possible solutions could include: [a] government funding of publishing houses that can ensure affordable and widespread access; [b] a system for depositing

¹⁰⁰ Mohan and Gupta (n 60) 46.

¹⁰¹ Divij Joshi, 'Driving Them Up the (Pay) Wall – Sci-Hub and the Disruption of the Academic Publishing Industry' (SpicyIP, 25 July 2017) <<https://spicyip.com/2017/07/driving-them-up-the-paywall-sci-hub-and-the-disruption-of-the-academic-publishing-industry.html>> accessed 29 January 2023.

research outputs in national library repositories for wider access; and/or giving peer reviewers a greater say in ensuring affordable access.¹⁰²

A thoughtful judgment by the Delhi High Court, that rules in favour of shadow libraries and outlines some of the aforementioned questions for the consideration of relevant stakeholders could be a valuable contribution. It can set in motion a well-considered thought process for addressing the ills that currently plague the publishing industry.

¹⁰² Swaraj Paul Barooah, 'Time to More Seriously Question the Spectre of Copyright in the Realm of Education' (SpicyIP, 23 December 2020) <<https://spicyip.com/2020/12/time-to-more-seriously-question-the-spectre-of-copyright-in-the-realm-of-education.html>> accessed 29 January 2023.

INFORMATION ABOUT THE JOURNAL

The *Indian Journal of Law and Technology* (ISSN 0973-0362) is an academic journal, edited and published annually by students of the National Law School of India University, Bangalore, India. All content carried by the Journal is peer-reviewed except for special comments and editorial notes. The Journal comprises:

- the Board of Advisory Editors, consisting of professionals and academicians pre-eminent in the field of law and technology, which provides strategic guidance to the Journal;
- the Article Review Board, a panel of external peer-reviewers;
- the Editorial Board, consisting of students of the National Law School of India University, which is responsible for selecting and editing all content as well as contributing occasional editorial notes;

OPEN ACCESS POLICY

The *Indian Journal of Law and Technology* is a completely open access academic journal.

- Archives of the journal, including the current issue are available online with full access to abstracts and articles at no cost.
- Please visit the website of the Indian Journal of Law and Technology at “<http://www.ijlt.in>” to get additional information and to access the archives of previous volumes.

INFORMATION FOR CONTRIBUTORS

The Indian Journal of Law and Technology seeks to publish articles, book reviews, comments and essays on topics relating to the interface of law and technology, particularly those with a developing world perspective.

MODE OF SUBMISSION

Submissions can be in electronic form or in hard copy form. However, submissions in electronic form are strongly encouraged in order to expedite the submission review process. Please address submissions in electronic form to the Chief Editor of the Indian Journal of Law and Technology at “ijltedit@gmail.com”.

REGULAR SUBMISSION REVIEW

The Journal shall communicate an acknowledgement to all authors shortly after the receipt of their submissions. The preliminary review of

the submissions shall be completed within four weeks of receipt in usual circumstances. The submissions that are initially accepted shall be blind-refereed by the Article Review Board. The Journal shall make due efforts to complete the entire peer-review process within a reasonable time frame. The Journal shall notify the authors about the exact status of the peer-review process as required.

EXPEDITED SUBMISSION REVIEW

This option is available to those authors who have received an offer of publication from another journal for their submissions. The authors may request an expedited submission review. However, the decision to grant an expedited submission review shall remain at the discretion of the Editorial Board. Please note that requests for an expedited submission review can only be made in relation to submissions in electronic form. All such requests must be accompanied by the following details:

- Name(s) of the author(s) and contact details;
- Title of the submission;
- Details about the journal(s) which has/have offered to publish the submission;
- Whether the offer is conditional or unconditional and, if the offer is conditional, then what conditions are required to be met for final acceptance;
- The date(s) on which the offer(s) expire(s).

The Journal shall make due efforts to accommodate the existing offer(s) and applicable deadline(s). However, upon an offer of publication pursuant to the expedited submission review, the authors shall have to communicate their decision within five calendar days of the notification or the offer. If there is no response, then the journal shall have the discretion to withdraw the offer.

SUBMISSION REQUIREMENTS

- All submissions must be accompanied by:
 - (1) a covering letter mentioning the name(s) of the author(s), the title of the submission and appropriate contact details.
 - (2) the résumé(s)/curriculum vitae(s) of the author(s).
 - (3) an abstract of not more than 200 words describing the submission.

- All submissions in electronic form should be made in the Microsoft Word file format (.doc or .docx) or in the Open Document Text file format (.odt).
- All text and citations must conform to a comprehensive and uniform system of citation. The journal employs footnotes as the method of citation.
- No biographical information or references, including the name(s) of the author(s), affiliation(s) and acknowledgements should be included in the text of the submission, the file name or the document properties. All such information can be provided in the covering letter.
- The Journal encourages the use of gender-neutral language in submissions.
- The Journal shall be edited and published according to the orthographical and grammatical rules of Indian English that is based on British English. Therefore, submissions in American English shall be modified accordingly. The Journal encourages authors to use British English in their submissions in order to expedite the editing process.
- The authors are required to obtain written permission for the use of any copyrighted material in the submission and communicate the same to the Journal. The copyrighted material could include tables, charts, graphs, illustrations, photographs, etc. according to applicable laws.

COPYRIGHT

The selected authors shall grant a licence to edit and publish their submissions to the Journal but shall retain the copyright in their submissions. The aforementioned licence shall be modelled as per a standard author agreement provided by the Journal to the selected authors.

DISCLAIMER

The opinions expressed in this journal are those of the respective authors and not of the Journal or other persons associated with it.

PERMISSIONS

Please contact the Chief Editor of the Indian Journal of Law and Technology for permission to reprint material published in the Indian Journal of Law and Technology.

ORDERING COPIES

Price Subscription (inclusive of shipping) of the IJLT is as follows:

Hard Copy for 2022	Rs.
Hard Copy for 2021	Rs. 1100
Hard Copy for 2020	Rs. 900
Hard Copy for 2019	Rs. 900

Order online: www.ebcwebstore.com

Order by post: send a cheque/draft of the requisite amount in favour of 'Eastern Book Company' payable at Lucknow, to:

Eastern Book Company,

34, Lalbagh, Lucknow-226001, India

Tel.: +91 9935096000, +91 522 4033600 (30 lines)

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission.

The published works in this issue may be reproduced and distributed, in whole or in part, by nonprofit institutions for educational and research purposes provided that such use is duly acknowledged.

© The Indian Journal of Law and Technology