ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC - NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

Data Sovereignty: A Trail of Global Governance and Cyberpowers

Author 1 - J Tanisha
Author 2 - Nishtha Wadhawan

Abstract

India has taken stock of emerging concepts of "techno-nationalism" and is responding to it in its own way. *Three* structural factors together driving this trend are the weakening of the post-war order, the politics of nationalism and the rapid rise of the digital economy. Indeed, right now we are at a point in history where the assumption that technology inevitably aids liberalisation is increasingly questioned especially with onset like AI. Rapid technological change, the *blurring* boundaries between war and peace and the primacy of the private sector have only compounded the challenges to global governance. The long-term interest lies in the growth and resilience of the domestic technology sector, projection of Indian technological solutions in different jurisdictions, guarding against supply chain risks, protecting the rights of its citizens and the security of its critical infrastructure. The emotive call has gone up to *'resist data colonialism'*. Being a nation-state, the citizen's data in India is treated as a *"national asset"*[1] with the objective to store and guard within its national boundaries. They aim to reserve the right to use that data and further, safeguard its strategic interests relating to defence. The country sets its vision high while embarking on its journey to data sovereignty and securing its national interests in the global economy. Secondary research has been conducted taking into account various expert opinions published publicly and mentioning historical accounts of various global superpowers shaping technology today.

Keywords - Data Sovereignty, national assets, privacy, data protection, security

[1] Vijay Govindarajan, Anup Srivastava, and Luminita Enache, *How India Plans to Protect Consumer Data,* December 18, 2019; Check on - https://hbr.org/2019/12/how-india-plans-to-protect-consumer-data (Last accessed on 28th Oct 2022)

ISSN: 2582-6433

[A] Introduction

India prides itself on having one of the world's youngest and most technologically advanced youth communities. Not just that, but the mass population also hone qualities of high adoption rates for digitally available technologies. Along with China and Indonesia, Asia might soon overtake the United States in consumer market contributions and key growth factors. A major definite amount of spending has been observed in the global market from these regions.

What is drawn is that India is on the journey of transforming into one of the biggest consumer markets of the world with humongous access to raw data around demographics, preferences, age etc. Now comes the word *"Digital Colonisation"* which gave way to energy and military colonialism.

People are exposed to various platforms on a daily basis, and these online accessible portals consume their data. Arises now is the factor of negligence and gross mistreatment on mentioned terms and conditions on such platforms and the effective use of these data beyond boundaries. *Two significant issues* are: at the national level, these accessible data might catalyse the government in stand and powerful corporate monopolies to establish dictatorial regimes and policies to intimate largely beneficial routes which might further lead to unequal societies; at the international level, comes loopholes in integrity and private authority of its citizen's activities over a certain state territory. In human history, only now with time and technology, people's activities and details can be constantly tracked over the internet through the help of several applications and portals even without their conscious consent. Sometimes, it so happens that these programmes seem to know individuals better than themselves. Decisions can be forecasted and conclusions can be derived. Hence, data can be used to alter variables. Additionally, it sprouts problems of influencing and shifting profits. Ability to change dynamics inside states, subjects and citizens, data has now taken the shape to become an issue of political and social.

ISSN: 2582-6433

[B] Defining Sovereignty

The concept of *"Data Sovereignty"* derives its meaning from the fact that the procedure of data collection and processing should be governed by the legal establishments of the nation within whose boundaries the data has originated. It is a fight against data colonialism and proprietorship over one's own data.

[C] Influence of Data Sovereignty over data security and governance

With the country's continuous engagement in developing laws around issues of sovereignty for border public interest, India holds the upper hand in affecting the enactment of global data governance and the development of laws. A wide population base, strong economy and consistently increasing internet users, all compositely keep India as a key stakeholder in data regulations. Our nation's steps through the years could be landmarks moments of constituting the *A. P. Shah Committee* on creating reports around data privacy, *Puttaswamy Judgment* and *Srikrishna Committee Report*

Extent of India's engagement can be summarised into three following criteria :

- Introduction of the *"Digital India Programme"*, which stands for the point that data which is sourced in India should only be used for national development and upliftment.
- India has remained to be outspoken in support of *'Data Localization'* in regard to regulations on data flows across cross-borders.
- As lines between economic and security blur, it is essential to safeguard citizens' data from any external threats. India has successfully done that by banning numerous Chinese apps.

Data security and localisation play a crucial role in *nation-building*, whether through agriculture, manufacturing, technology, etc. Definitely, there are opportunities as well as wide gaps with the growing prevalence and importance of data. And India triumphs in ensuring security through data sovereignty. It has successfully adopted a clear strategy along with adhering to its constitutional values by creating a fair and equitable vision along these lines.

ISSN: 2582-6433

[D] How Data Sovereignty is different from data localisation and data residency?

Where Data sovereignty is a government policy or an enacted law revolving around data and the privacy issues surrounding it for a specific geographical location - in our case India where we have few specific laws like the *Information Technology Act, 2000* and the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or information) Rules, 2011 ("SPDI Rules")* which have been framed to protect personal and sensitive data from getting unauthorised use. In recent times, in 2019, the government presented the parliament with the Personal Data Protection Bill ("PDP Bill") which was later sent for review at a joint session. On December 2021, a report was submitted with various recommendations and modifications which explained the width of the scope of the laws, taking into consideration of both personal and non-personal data. The bill now is popularly known as the *"Data Protection Bill, 2021" ("DP Bill")*.

On this note when we look at the concept of Data Localization, people have been using it as a synonym for each other. But the purview of localisation revolves around the regulations regarding where the governments can actually locate data. An example of this could be the *EU's GDPR*.

Further, Data Residency is entirely different; embodied in a private individual business for the basis of where they store their data and its specific geographical location. This liberalisation helps in finding a suitable country in consideration of the regulatory framework, tax benefits or performance.

[E] Considerations and Challenges

[E.1] Data at rest

Even before we look into choosing a country based on our convenience and maximum benefit offered, the initial efforts should be given to consider *"How and Where"* to store the data. Whether an entity opts to store data on-premise or in the cloud. Cloud storage makes it an even more difficult choice to determine the jurisdiction and thus, making it harder to govern its data sovereignty. If one elects to use the cloud, then issues related to replication and backup storage erupt. The provider may or may not allow huge liberalisation in regard to

ISSN: 2582-6433

selecting a geographical region of choice. In such scenarios, it becomes even more important to know and understand the requirements of each region

[E.2] Data in Transit

Now if the data is not at rest and is regularly or continuously transferred between different geographical regions, key considerations become its *frequency, where to where* and *type* of the data. These affect the way of collection and the process. Here, the mandates and regulations of the data destination are pivotal to data sovereignty. Modification in data flows helps to reduce legal issues and maintains it under an appropriate jurisdiction.

Steps to ensure Data Sovereignty in Cloud computing:-

- Leveraging the resources provided by the cloud service company:

In most cases, providers have a set of pre-decided *favourable geolocations* in regard to company requirements meeting your requisites. Such as data encryption.

- Uniform Data Sovereignty:

As each nation hones its own set of data sovereignty mandates, in the case of global operations, maintaining issues of data sovereignty becomes complex. A company might opt for one geographical location and apply to all others ever is the strongest and most stringent. Later, this helps in providing additional security in long term.

- Keeping track of backups:

As data sovereignty extends to backups, it is important to determine if the data is at rest on the premise using cloud services like *google drive, dropbox* act or public cloud services. Ensuring that these backup options are in line with your operating territory's requirements is of utmost significance.

[F] Sector Specific legislation

Currently, there are *no sector-specific legislations in India* but the government and regulating bodies have certainly provided for a set of regulations, directives and licensing conditions across sectors like payment systems, telecoms, healthcare, pharmacies etc.

ISSN: 2582-6433

[G] Territorial Scope in businesses outside India

The application of the rules given under the IT Act and the SPDI Rules are not very straightforward and rather remain grey. IT Act does not restrict entities incorporated within India. An extra-territorial jurisdiction can be extended *"for any offence or contravention"* irrespective of its nationality if it involves a *computer or a computer system in India*.
The Data Protection Bill, 2021 seems a bit clearer on this aspect. It applies to processing in data fiduciaries and processors present outside India but the business is carried out, offers goods and services or involves profiling of data principals within the Indian boundaries.

Hence, in the past few months, we have witnessed the banning of several applications and sites that steal and surreptitiously collect users' data through servers outside India. These bans can be justified as a means to protect the *severity, integrity and safety* of the country. Additionally, it maintains *public order* and ensures *protection from misuse* of data.

[H] Protection of consumer data

India has followed the EU's GDPR *("General Data Protection Regulation")* in allowing global technology-based companies to conduct business but with certain caveats. It is expected that the Data Protection Bill framed by the Indian Government in the future shall broaden the horizon beyond the EU regulations. Being a *nation-state*, the citizen's data in India is treated as a *"national asset"*[2] with the objective to store and guard within its national boundaries. They aim to reserve the right to use that data and further, safeguard its strategic interests relating to defence. The country sets its vision high while embarking on its journey to data sovereignty and securing its national interests in the global economy.

[H.1] India recognises "Privacy" as a fundamental right

In the Supreme Court of India's judgement (*Justice K. S Puttaswamy and Anr vs. Union of India*)[3] in 2017, the bench held privacy to be a constitutional right of Indian citizens under the right to life and liberty. [4] A visible trail is left every time one uses or transverses in the digital

[2] Ibid
[3] *Justice K.S. Puttaswamy and Anr. vs. Union of India (UOI) and Ors* (2019) 1 SCC 1
[4] *Article 21*, Constitution of India

ISSN: 2582-6433

world. Data sovereignty can be maintained at different stages but enact laws to control the collection, sale, storage, exploitation and security of user data. There have been examples of many companies that offer free services online in exchange for sharing the user data they secure. Hence, entities need to analyse their cost-benefit ratios if regulations are enacted on these lines. Digital firms will be at a run to re-invent their business models as they will no longer be in a position to retain and sell user data with the Indian regulatory framework in place.

[H.2] Obtaining consent from users

Before obtaining any of their data, regulations should be made to source one's data through explicit permission. Through this, the extent and scope should be widely elucidated. *Consent* across each data processing stage is crucial. As with advanced technologies, smart machines process data in such a way as to create new data from the existing data which no longer now belongs to the original user, and compliance becomes even trickier. Companies need to reform their operating procedures and data tracking methods. Digital data-obtaining companies are termed *"data fiduciaries"* and not just data collectors as they now carry the responsibility both for the original and processed data.

[H.3] Ownership of personal data

While the proposed Data Protection Bill of 2021 mentioned complete *full ownership* over the data of the source, these could be heavy implantation in digital companies. An example could be when a person deletes his/her Instagram account and aim to erase all the available data on it, with sole ownership it can be termed that it might want all its data to be returned but in the case of physical property it is possible, in the world of technology it goes beyond Instagram. The scenario could be that the company might have sold the data to a third party and now it cannot be erased completely. Hence, the complete ownership of one's own data comes to question.

[H.4] Classification of Data

The previously introduced Data Protection Bill had identified three categories: *Sensitive* which includes data like finances, health, intimate visuals, genetics, religious materials etc; *Critical* are those which along with time government modifies with time depending on the

ISSN: 2582-6433

requirements such as data based on military or affecting national security; *General* are those which are not specifically mentioned but whatever is left after bifurcating the above two.

To maintain authority over the user's data, all sensitive and critical data must be stored in servers within India. If for processing it is taken, it must be brought back for storage.

What comes with this *"bifurcation"* is the concept of the *"split internet"*. Storage and processing of data are usually done by companies according to the most convenient and efficient method appropriate to them but with imposed restrictions, high costs might be spotted leading to problems in sub-economic storage and processing capabilities.[5]

[I] Rising sovereignty, then what?

The GDPR does not impose any locational storage requirements for data to protect national interests. Currently, all internet-based giants logically own all the data as long as they can address the privacy guidelines mentioned under the law and meet consumer consent. Through DPB ("Data Protection Bill") earlier, the government added a clause that as the citizen's data is treated as a "national asset" what we deem is similar to how it extends control over physical properties, implying demand over citizen data in case of foreign attacks and surveillance, the digital companies have to assist in government's defence policy.

"The Special Rapporteur believes that the Internet is one of the most powerful instruments of the 21st Century for increasing transparency in the conduct of the powerful, access to information and for facilitating active citizen participation in building democratic societies. Indeed, the recent wave of demonstrations in counties across the Middle East and North African region has shown the key role that the internet can play in mobilising the population to call for *justice, equality, accountability* and *better respect for human rights*"[6]

In 2012, in Iran, the users of the internet were bombarded with advertisements which stated *'Access to free internet is your inalienable right'*. Such an advertisement had various tools together wrapped under this statement to stir the internet. Across the middle east, many similarly tailored ads were delivered through Facebook, Google and other social media platforms. A rough estimate is around 1.5 million people click over the ad under this

[5] Supra Note 1
[6] Frank La Rue, UNGA, *Human Rights Council, ' Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression,*16 May 2011.

ISSN: 2582-6433

campaign. The ads were part of the US Department of State's attempt to promote freedom of speech in authoritarian regimes hostile to American interests.[7]

Such an adverse situation lead Asian countries like Tajikistan, Uzbekistan, China and Russia etc to ask the then UN Secretary to propose their document in the general assembly formulated on the *International Code of Conduct for Information Security (the Code)*. The document clearly stated that the free flow of information must not have any dire effect on *domestic stability.* For the first time, there was an emphasis made on the "multilateral nature of Internet governance" i.e to promote state control. It stressed the importance of international bodies like the UN can bring between states through enhanced coordination and cooperation. This was a diverging approach from America's preference for a multi-stakeholder approach. The latter focuses on the involvement of civil society and the private sector through less traditional groups such as *Internet Governance freedom*.

Hillary Clinton's senior advisor Alec Ross somewhat prophetically told *the Washington Post* that, *'If the great struggles of the 20th century were between left and right…. The conflict of the 21st century will be between open and closed."*[8]

All this was done with the expectation that as offline rights are difficult to replicate in an online scenario, liberal democracies might give better conclusions. In 2013 however, these expectations were put to rest. *The Guardian* along with other newspapers revealed that details of the mass electronic surveillance were made by *National Security Agencies (NSA)* which collected a massive amount of data from American citizens and individuals from all around the world. It was noted that such intelligence data was collected through Facebook posts, emails, Twitter chats etc.

The NSA contractor heading this was *Edward Snowden*, who after such revelations, on one side was hailed as a national patriot who protected the values of freedom, while on the other was termed as a traitor to have compromised national security. Whatever side one falls in, this incident is definitely marked as a landmark point in - *foreign policy choices and global internet governance.*

[7] Fergus Hanson, *Internet Freedom: The Role of the US State Department, Brookings,* 25 October 2012.
[8] Will Englund, *Russia hears an Argument for Web Freedom; Washington Post;* 28 October 2011.

ISSN: 2582-6433

[J] The emergence of Cyber Powers

Perceived American domination over the internet is strongly challenged by China's growing cyber power. An important aspect to note here is its rejection of western media companies in Chinese social affairs. To implement this objective, it has taken a multifaceted approach of *censorship, government monitoring, unfair trade regulations* and *enormous spending on Chinese national industries.* As stated, in China access to the internet is a privilege granted by the state and not a freedom to be enjoyed.[9] This idea is completely against the libertarian vision.[10]

After Hillary Clinton argued for global recognition of a universal right to the internet, for the first time China released an English Language State Council White Paper outlining its vision for *"Interest Sovereignty"*. Within the Chinese territory, the internet is under the jurisdiction of Chinese sovereignty. The internet sovereignty of China should be respected and protected.[11] It was justified by basing its facts to *preserve state interests* and *social harmony*.

While these methods are disruptive, Snowden's previous revelation around the US happily undermining digital protections has been proved through the *Cambridge Analytica Scandal* which allowed a private firm to mine data of millions of Americans for electoral targeting in 2018 just how powerful and unaccountable Silicon Valley is. As we now pass through an age where most powers understand the strategic value of dominating emerging technologies, the race to control them will only grow fiercer.

[K] The Indian Way

The *Modi Government* has indeed introduced reforms in regard to restrictions over e-commerce rules to favour domestic companies. The long-term interest lies in the growth and resilience of the domestic technology sector, projection of Indian technological solutions in different jurisdictions, guarding against supply chain risks, protecting the rights of its citizens

[9] Shashi Tharoor and Samir Saran, *"The new world disorder": And the Indian Imperative;* Pg 149
[10] Ibid
[11] China Foreign Ministry, *'Protecting Internet Security', Beijing*: Government White Papers.

ISSN: 2582-6433

and the security of its critical infrastructure. The emotive call has gone up to *'resist data colonialism'*.[12]

Now with the emergence of AI, governments are able to conduct even more effective surveillance of their citizens. It offers a greater degree of precision and specificity than ever before. This might lead to authoritarian governments using economic development to increase democratisation. Hence it can converge that AI can work and give the government a social control tool through which they can keep tight control of dissidence and encourage growth and prosperity.

Not just countries but technology giants have also tried to colonise the internet. In 1981, Tom McPhil said - *a vision of the internet colonised by mass media companies whose intent was to capture the minds and attention span of larger parts of the world*.[13]

"Data is the new Oil", 1995 Irving Goldstein predicted that information will be for the twenty-first century what oil and gas were for the beginning of the twentieth century.[14] While one part of the race was bringing people online, more accurately to online platforms but after that comes the crucial part of - *control over the behaviour*.

[L] Conclusion

The Internet's governance landscape is marred by conflicting normative visions, competing for commercial realities and cyber geopolitics.[15] The *US's divest in Huawei* in 2018 has promulgated its self-serving nature in regards to the *"globalist approach"* to technology. Meanwhile, China's tech sector and Communist Party make the brand ChinaTech an omnipresent security risk. Therefore, India cannot relegate itself to choosing between these two- but rather it must develop its own *indigenous system* that is responsive to its jurisdiction. The now seemingly out-of-date idea of sovereign borders melting away in the face of rampant techno-globalism rests its assumption on the fact that all states shared the same values in the international system. We have spotted many countries emulating their preference for *authoritarian nationalism* over *internationalist liberalisation*, techno-globalism is giving way to a new phenomenon of technological nationalism.

[12] Supra Note 8
[13] Thomas L. McPhail, *Electronic Colonialism: the Future of International Broadcasting and Comumunication, Newbury Park: SAGE Publications Inc*, 1987
[14] Shaun M Powers and Michael Jablonski, *The Real Cyber War*, Pg 75-76
[15] Supra Note 8

ISSN: 2582-6433

When asking questions like - c*ore function controls, political boundaries, vision for the internet* and *the over whole control lies*? The conventional wisdom rightly points out that it is through *multiple stakeholders*. Unlike multilateral decision making where it has greater state representation, the multi-stakeholder model focuses on equal footing over both *businesses* and *civil society representatives.* It can be termed as a wider trend in re-imaging *"global governance".* The Internet is now in a dismaying state and is struggling between *liberal democracy* and *digital authoritarianism* along with *transnational colonialism* and *assertive technonationalism*. Even if not a perfect one, what India needs right now is an effective Data protection bill in place to secure the national interest and rights of its citizen. With a widened scope and application, our democracy enshrined under the constitution can be maintained.

Bibliography

Articles

1. Fergus Hanson, *Internet Freedom: The Role of the US State Department, Brookings*, 25 October 2012.

2. Vijay Govindarajan, Anup Srivastava, and Luminita Enache, *How India Plans to Protect Consumer Data*, December 18, 2019.

3. Will Englund, *Russia hears an Argument for Web Freedom; Washington Post;* 28 October 2011.

Books

1. Shashi Tharoor and Samir Saran, *"The new world disorder": And the Indian Imperative;* Pg 149

2. Shaun M Powers and Michael Jablonski, *The Real Cyber War*, Pg 75-76

3. Thomas L. McPhail, *Electronic Colonialism: the Future of International Broadcasting and Comumunication, Newbury Park: SAGE Publications Inc*, 1987

ISSN: 2582-6433

Case

1. *Justice K.S. Puttaswamy and Anr. vs. Union of India (UOI) and Ors* (2019) 1 SCC 1

Documents

1. China Foreign Ministry, *'Protecting Internet Security', Beijing*: Government White Papers.

2. Frank La Rue, UNGA, *Human Rights Council, ' Report of the Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression,*16 May 2011.

Statutes

1. *Article 21*, Constitution of India

2. Data Protection Bill, 2021

3. European Union's GDPR *("General Data Protection Regulation")*

4. Information Technology Act, 2000

5. Information Technology *(Reasonable Security Practices and Procedures and Sensitive Personal Data or information)* Rules, 2011 ("SPDI Rules")