# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

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.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

# CYBER SOVEREIGNTY IN THE AGE OF DISINFORMATION: COMBATING FAKE NEWS AND ONLINE MANIPULATION

AUTHORED BY - JANESHWAR RAJ Y[1]

## ABSTRACT

The proliferation of disinformation and online manipulation poses significant challenges to cyber sovereignty, as governments strive to maintain control over their digital domains while protecting their citizens from the harmful effects of fake news and online propaganda. As cyberspace becomes increasingly weaponized for political and ideological ends, the concept of cyber sovereignty takes on renewed significance in the effort to safeguard national security and protect democratic institutions from malicious actors seeking to manipulate public opinion and undermine trust in the information ecosystem. This research paper examines the complex interplay between cyber sovereignty and the spread of disinformation, exploring the strategies employed by states to combat fake news, enhance digital literacy, and safeguard democratic processes. Through a comprehensive analysis of case studies, policy frameworks, and international norms, it aims to provide insights into how governments can reconcile the imperatives of cyber sovereignty with the need to preserve freedom of expression and ensure the integrity of democratic discourse in the digital age. By highlighting the multifaceted nature of the disinformation threat and the importance of international cooperation, this paper aims to provide insights into effective approaches to preserving cyber sovereignty in an era of online manipulation.

## INTRODUCTION

In recent years, the internet has emerged as a battleground for information warfare, with malicious actors exploiting digital platforms to spread disinformation, sow discord, and undermine democratic institutions. The phenomenon of fake news and online manipulation poses a grave threat to cyber sovereignty, as governments struggle to maintain control over their digital domains, while safeguarding the integrity of public discourse and democratic processes. By

[1] Authors are Assistant Professors at Saveetha School of Law, Chennai

ISSN: 2582-6433

analysing case studies and policy interventions, it seeks to elucidate the complex dynamics of information warfare in cyberspace and identify effective approaches to preserving national security, freedom of expression, and democratic governance in the digital age. Likewise, through international cooperation and collaboration, states can mitigate the threat of disinformation and preserve the integrity of global information ecosystems in the digital age.

In response to these threats, states have increasingly asserted their authority over the digital domain, invoking the concept of cyber sovereignty to regulate online content, combat foreign interference, and protect national security interests. However, the pursuit of cyber sovereignty raises complex ethical and legal questions regarding freedom of expression, privacy rights, and the role of government in regulating online speech along which might lead to arbitrary actions that violated the basic fundamental principles.

This research paper seeks to explore these issues in depth, analysing the evolving landscape of disinformation, the strategies employed by states to counter online manipulation, and the implications of cyber sovereignty for the future of democratic governance and human rights in the digital age.

## UNDERSTANDING DISINFORMATION

Disinformation, defined as false or misleading[2] information spread deliberately to deceive or manipulate audiences, has become increasingly prevalent in the digital era. Enabled by the ubiquity of social media and online platforms, malicious actors exploit algorithms, echo chambers, and anonymity to amplify false narratives, manipulate public opinion, and influence electoral outcomes. The spread of disinformation poses multifaceted challenges to cyber sovereignty, as governments grapple with the task of countering online manipulation while upholding principles of free speech, privacy, and information access.

## RISE OF DISINFORMATION IN CYBERSPACE

**Historical Perspectives:**

The phenomenon of disinformation is not new; throughout history, governments and other actors have sought to manipulate public opinion through propaganda, censorship, and psychological warfare. However, the advent of digital technologies and the internet revolutionized the

[2] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2023

ISSN: 2582-6433

dissemination of information, enabling the rapid spread of false or misleading content to global audiences with unprecedented speed and scale.

**Characteristics of Disinformation:**

Disinformation encompasses a wide range of tactics and techniques designed to deceive, manipulate, or mislead audiences for political, ideological, or commercial purposes. These may include the spread of false rumours, fabricated news stories, doctored images or videos, and coordinated disinformation campaigns orchestrated by state actors or non-state actors with specific agendas.

**Impact on Democratic Discourse:**

The accelerated spread of disinformation poses significant challenges to democratic governance and the integrity of public discourse. By sowing confusion, amplifying partisan divisions, and eroding trust in institutions and democratic processes, disinformation undermines the foundation of democratic societies and exacerbates social polarization.

## CYBER SOVEREIGNTY

Cyber sovereignty refers to the authority of states to govern and regulate the internet within their borders according to their own laws and policies. Therefore, the state, or the citizens of the state, if involved in attacking other states or non-state actors' cyber facilities, also come under the ambit of cyber sovereignty[3]. In the context of combating disinformation, cyber sovereignty entails the ability of governments to enact and enforce regulations to mitigate the spread of fake news and online manipulation while upholding democratic values and human rights principles.

## THREAT TO CYBER SOVERREIGNTY

Disinformation threatens cyber sovereignty on multiple fronts, undermining trust in democratic institutions, eroding social cohesion, and exacerbating geopolitical tensions. By exploiting vulnerabilities in digital ecosystems, hostile actors seek to subvert the informational integrity of target populations, destabilize political systems, and advance their strategic objectives. The weaponization of fake news and online manipulation poses significant challenges to states' ability to govern their digital domains and protect their citizens from the harmful effects of information

[3] Cyber sovereignty: In search of definitions, exploring, implications, https://www.orfonline.org/, (last visited Oct. 6, 2023).

ISSN: 2582-6433

warfare.

## REGULATION OF ONLINE CONTENT

In response to the growing threat of disinformation, governments have implemented a range of strategies aimed at countering fake news, enhancing digital literacy, and strengthening resilience against online manipulation. These include legislative measures to regulate online content, investment in media literacy programs, and collaboration with technology companies to mitigate the spread of false information. While these efforts have yielded some success, challenges remain in addressing the root causes of disinformation and promoting a culture of critical thinking and information discernment among internet users.

States employ various regulatory approaches to combat disinformation and protect the integrity of the information ecosystem. These may include legislation targeting intermediaries. Intermediaries are entities that store or transmit data on behalf of other persons, and include telecom and internet service providers, online market places, search engines, and social media sites[4]. The regulatory frameworks are aiming for content moderation and establishment of fact-checking unit[5] to prevent misleading information from floating on the internet.

International cooperation mechanisms to address cross-border disinformation campaigns and foreign interference in democratic processes have also been advocated to achieve the removal of harmful and unnecessary information across borders. Given the transnational nature of disinformation, international cooperation is essential to effectively combatting fake news and online manipulation. By sharing intelligence, coordinating responses, and promoting norms of responsible behaviour in cyberspace, states can enhance their collective resilience against the spread of disinformation and safeguard the integrity of global information ecosystems. Initiatives such as the Global Partnership on Artificial Intelligence[6] and the Paris Call for Trust and Security in Cyberspace[7] provide frameworks for international collaboration on addressing the multifaceted challenges posed by disinformation in the digital age.

[4] The Information Technology Act, 2000, Section 2 (1) (w), No. 21, , Acts of Parliament, 2000 (India)
[5] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023
[6] Global Partnership on Artificial Intelligence. (2020). Key Documents. Retrieved from https://www.global-ai-partnership.org/key-documents, (last visited Oct. 19, 2023).
[7] Macron, E. (2018). Paris Call for Trust and Security in Cyberspace. Retrieved from https://pariscall.international/en/the-call/, (last visited Oct. 14, 2023).

ISSN: 2582-6433

The regulation of online content in the name of combating disinformation raises complex legal questions regarding freedom of expression[8], privacy rights[9], and the role of government in shaping public discourse. Critics argue that overly broad or draconian measures to suppress disinformation may infringe on individual liberties, stifle dissent, and empower governments to censor political opposition or dissenting voices under the guise of national security or public order.

In Shreya Singhal v. Union of India[10], the Supreme Court of India, passed a landmark judgment, declaring "Sending material through a computer resource or a communication device that is egregiously offensive, menacing, or causes irritation, discomfort, danger, obstruction, insult, harm, criminal intimidation, hostility, hatred, or ill will[11]" as illegal under section 66A of the Information Technology Act, 2000, as unconstitutional.

The issue before the court was whether section 66A violated the Fundamental Right to freedom of speech and expression guaranteed by Article 19(1)(a) of the Indian Constitution.

**The court held that section 66A was vague and overbroad**. Therefore, it did not satisfy the test of constitutionality laid down under Article 19(2) of the Constitution, which provides for reasonable restrictions on the freedom of speech and expression.

Similarly, in Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors[12], the Court in its judgement stressed upon the following points,
It was held that privacy concerns in this day and age of technology can arise from both the state as well as non-state entities and as such, a claim of violation of privacy lies against both of them.

The Court also held that informational privacy in the age of the internet is not an absolute right and when an individual exercises his right to control over his data, it may lead to the violation of his privacy to a considerable extent.

It was also laid down that the ambit of Article 21 is ever-expanding due to the agreement over

[8] INDIA CONST. art. 19, cl. 1
[9] INDIA CONST. art. 21

[10] Shreya Singhal v. Union of India, AIR 2015 SC 1523
[11] The Information Technology Act, 2000, Section 66A, No. 21, Acts of Parliament, 2000 (India)
[12] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1

ISSN: 2582-6433

the years among the Supreme Court judges as a result of which a plethora of rights has been included within Article 21.

The judgement in this landmark case was finally pronounced upholding the fundamental right to privacy emanating from Article 21. The court stated that Right to Privacy is an inherent and integral part of Part III of the Constitution that guarantees fundamental rights.

Despite numerous judgements stressing the importance of privacy and freedom of speech, the IT Rules, 2023 pose a significant threat to the fundamental rights. However, it is justified under the functions of the government to curb the spread of misleading or false information that could potentially disrupt the peace of the nation.

## STRATEGIES AND CHALLENGES IN COMBATING MISINFORMATION

**China's Great Firewall**

China's approach to regulating cyberspace exemplifies the concept of cyber sovereignty, whereby the state exercises strict control over online content and information flows to maintain social stability, preserve political control, and protect national security interests. The Great Firewall of China, a sophisticated system of internet censorship and surveillance, enables the government to block access to foreign websites, filter online content, and monitor online activities to suppress dissent and maintain ideological conformity.

**Russia's Information Warfare Tactics**

Russia has emerged as a prominent actor in the global disinformation landscape, leveraging information warfare tactics to manipulate public opinion, sow discord, and undermine democratic institutions in Western democracies and neighbouring countries. The Kremlin employs a combination of state-sponsored media outlets, troll armies, and covert influence operations to disseminate propaganda, amplify divisive narratives, and exploit existing fault lines within target societies to advance its geopolitical objectives.

**European Union's Regulatory Framework**

In response to the growing threat of disinformation, the European Union has adopted a comprehensive regulatory framework aimed at combating online manipulation, safeguarding

ISSN: 2582-6433

democratic processes, and promoting media literacy and digital resilience among citizens. Initiatives such as the Code of Practice on Disinformation[13], the Digital Services Act, and the European Democracy Action Plan[14] seek to enhance transparency and accountability among online platforms, improve the detection and removal of disinformation, and empower users to critically evaluate and navigate the information environment.

Examining methods from around the world provides valuable insights into the effectiveness of different approaches to combating disinformation and preserving cyber sovereignty. From the European Union's efforts to combat online disinformation through the Code of Practice on Disinformation to Singapore's regulatory framework for addressing fake news, each country and region faces unique challenges and opportunities in countering the spread of false information online. By analysing these case studies, policymakers can glean valuable lessons learned and identify best practices for enhancing resilience against information warfare in cyberspace.

## CONCLUSION

As the proliferation of disinformation continues to pose significant challenges to global stability and democratic governance, the concept of cyber sovereignty assumes greater relevance in the effort to regulate online content, combat online manipulation, and protect the integrity of democratic discourse in the digital age. While states have a legitimate interest in safeguarding national security and combating malicious actors seeking to undermine public trust in the information ecosystem, they must also uphold fundamental rights and democratic principles, including freedom of expression, privacy, and due process. Achieving a balance between the imperatives of cyber sovereignty and the protection of individual liberties requires a multifaceted approach that combines regulatory measures, technological solutions, and international cooperation mechanisms to address the root causes of disinformation while preserving the openness and inclusivity of the internet as a global public good.

[13] European Commission. (2018). Code of Practice on Disinformation. Retrieved from https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation, (last visited Oct. 29, 2023).
[14] European Commission. (2020). European Democracy Action Plan: Making Our Democracies Stronger in a Digital Age. Retrieved from https://ec.europa.eu/info/publications/european-democracy-action-plan-making-our-democracies-stronger-digital-age_en, (last visited Oct. 29, 2023).