International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Beyond Borders: Addressing the Legal Quagmire of Jurisdiction in Cyberspace

Dr. Vijaykumar Shrikrushna Chowbe[1], Dr. Suryakant S. Bhosale[2]

[1]Professor and Head, Department of Law, Sant Gadge Baba Amravati University, Amravati (India)
[2]Principal, Shahu shikshan Santha's Devjibhai Hariya Law College, Shahad (W), Kalyan Mumbai.

Abstract:
This article delves into the complex scenario of governing cyberspace, addressing key issues such as accessibility, digital disparities, and the regulatory challenges posed by cross-border activities, and applicable test by judiciary across the globe while resolving such emerging issues. Despite technological progress, cyberspace largely remains an unregulated realm, creating opportunities for cybercrimes such as stalking, data breaches, exploitation of minors, and hacking. The lack of a cohesive global governance structure makes tackling these issues a formidable task.
The article offers a critical assessment of the Budapest Convention on Cybercrime, the sole international treaty on cybercrimes, pointing to its limited acceptance, especially among ASEAN nations. This hesitation underscores an ideological rift: some countries prioritize cyber sovereignty, while others support a multi-stakeholder model that incorporates contributions from governments, private enterprises, and civil society. These divergent views present barriers to legal harmonization and obstruct cross-border collaboration in prosecuting cyber offenders and ensuring data protection.
To address these multifaceted challenges, the article suggests a layered governance approach, integrating global frameworks with regional alliances and national strategies. This model encourages international cooperation while respecting national sovereignty, emphasizing the importance of public-private partnerships to bolster cybersecurity. Furthermore, it advocates for investments in digital infrastructure and cyber literacy programs to reduce the digital divide, facilitating broader, fairer access to online spaces. Ultimately, the proposed governance model seeks a balanced approach, safeguarding individual rights alongside the imperatives of security and accountability, and aiming to cultivate a cyberspace that is safer, more inclusive, and subject to responsible oversight.

Keywords: [cyberspace governance, digital divide, Budapest Convention, cyber sovereignty, multi-stakeholder model, cybercrime, international cooperation, data protection, privacy, public-private partnerships, cybersecurity]

1 Dr. Vijaykumar Shrikrushna Chowbe, Professor and Head, Department of Law, Sant Gadge Baba Amravati University, Amravati (India) See https://www.sgbau.ac.in/pages/ProfessorBiodataPDF/Law_Dr%20Vijaykumar%20Chowbe.pdf. Any suggestion, criticism, comment, or tip for improvement may be addressed to vijuchowbe@gmail.com. Thoughts, analyses made, opinions given, and criticism explored are those of the author, unless citations prescribe otherwise. The usual caveats apply. © authors

2 Dr. Suryakant S. Bhosale, Principal, Shahu shikshan Santha's Devjibhai Hariya Law College, Shahad (W), Kalyan Mumbai.

In 2021, WhatsApp Inc. became entangled in a significant legal conflict in India, highlighting a crucial question: how can a country regulate a platform that operates globally without a fixed jurisdiction? The case, WhatsApp Inc. v. Union of India, W.P. (C) 4425/2021, underscores the escalating tension between international tech giants and individual national laws. As an American-based company, WhatsApp resisted India's new IT Rules, 2021, which mandated that it trace the origin of private messages. WhatsApp argued that compliance would compromise end-to-end encryption, infringing on user privacy. In contrast, India argued that concerns over national security justified such demands, setting the stage for a contentious legal confrontation.

This conflict between global digital platforms and domestic regulations goes beyond privacy issues, exposing the inherent jurisdictional complexities in cyberspace. With billions of users, distributed servers, and cross-border transactions, determining the locus of legal accountability becomes a complex issue. Can India assert its legal reach over a platform headquartered overseas? Or does the nature of cyberspace necessitate a cooperative governance model that transcends traditional legal boundaries?

The WhatsApp case exemplifies the broader legal dilemma of jurisdiction in the digital age. This article examines how courts around the globe are approaching these challenges, the frameworks they've established—such as interactivity, intent, and harm-based tests—and the intricate balance required between sovereignty, privacy rights, and enforceability in a world without borders. This evolving landscape reflects the pace at which technology surpasses existing legal frameworks, underscoring an urgent need for innovative governance in the digital sphere.

Introduction

Cyberspace,[3] with its ability to transcend national boundaries, presents a complex challenge to domestic legal systems and international governance. Cyberspace is a dynamic realm that fosters commerce, social connections, and the exchange of knowledge, but it also opens doors for illicit activities. As people interact in this virtual space without physical boundaries, conventional methods of law enforcement and governance face significant challenges in adapting. This article delves into the frameworks of governance, the jurisdictional hurdles, and the delicate balance between individual rights and regulatory authority within the context of cyberspace.

Governance and the Digital Environment

Cyberspace provides a space for people to transact, communicate emotions, and share ideas freely. However, the absence of physical borders demands innovative governance strategies to prevent misuse

3 Cyberspace, as it denotes to the sum total of environment created by interlinking and interconnected computers, refers to the virtual realm formed through the interconnection of computers and digital networks. Although often used to describe the sum total of this interconnected digital environment, the term can sometimes be seen as a misnomer because it attempts to capture the complexities of a non-physical space with a single label. The word "cyberspace" was coined by William Gibson in his 1984 science fiction novel *Neuromancer*, where it described a virtual environment inhabited by entities resembling human consciousness—complete with emotions, interactions, and personalities—free from the constraints of identity, time, space, or physical form. Gibson imagined a space where electrons create a new dimension of interaction, simulating human experiences without the limitations of the real world. In this article, "cyberspace" refers to the global digital realm shaped by interconnected computer networks. It encompasses platforms where individuals communicate, share information, express emotions, conduct business, and engage in various transactions, all driven by the seamless flow of digital data. This virtual world supports a wide range of activities, from social media interactions to e-commerce, overcoming geographical and time constraints through the transmission of information in digital form. This definition highlights the functional and interactive qualities of cyberspace, where information technology dissolves traditional boundaries, creating a space that enables human activities to become more dynamic, immediate, and globally accessible.

and maintain order. The core challenge is to ensure that the digital realm reflects societal values and norms similar to those that govern our physical world. Laws must evolve to regulate behaviour online while safeguarding personal freedoms. The transnational scope of cyberspace adds complexity, often bringing traditional legal frameworks into tension with modern technological mechanisms designed to navigate this global landscape.

The governance dilemma lies in balancing two competing interests. On one hand, individuals seek freedom to express, access information, and engage in commercial activities. On the other, society demands control mechanisms to prevent misuse, such as cybercrimes, fraud, and data theft.[4] An effective governance framework must recognize this duality and create systems that maintain order without stifling innovation.

Jurisdictional Challenges in Cyberspace

One of the key legal challenges in cyberspace is determining jurisdiction. Traditional jurisdiction concepts are rooted in physical geography, which cyberspace defies by enabling instantaneous global interactions. Crimes committed in one country may have repercussions in another, complicating the question of which court holds legal authority.

In the case of Banyan Tree Holdings Ltd. v. A. Murali Krishna Reddy,[5] the Delhi High Court ruled that simply having a website accessible in a particular jurisdiction does not establish legal authority. The court emphasized that jurisdiction depends on the website's interactivity and the nature of any commercial transactions it facilitates. This approach aligns with the principles in Zippo Manufacturing Co. v. Zippo Dot Com, Inc.,[6] which introduced a "sliding scale" test to evaluate whether a website's interaction with users creates sufficient grounds for jurisdiction. This test differentiates between passive websites, which merely provide information, and interactive sites that engage in transactions, helping courts prevent misuse of jurisdiction, such as forum shopping, where parties seek favourable courts for their claims.

Another significant case addressing jurisdictional complexities in cyberspace is Amazon.com, Inc. v. Amway India Enterprises Pvt. Ltd.,[7] which dealt with jurisdiction in e-commerce transactions involving parties in different regions. The court held that jurisdiction could be established based on where the cause of action originated, such as the location where the transaction was initiated or where a breach occurred. This ruling highlights the challenges of determining jurisdiction in the digital realm, where traditional boundaries are less defined. With transactions involving participants across multiple jurisdictions,

4 This governance dilemma was addressed by the Supreme Court of India in Shreya Singhal v. Union of India, (2015) 5 SCC 1, where the Court struck down section 66A of the Information Technology Act, 2000. The Court emphasized that the individual's right to freedom of expression under Article 19(1)(a) of the Constitution of India, 1950 must take precedence over the state's interest in regulating online content to maintain law and order. The provision was declared unconstitutional due to its vague and overly broad restrictions, which risked creating a chilling effect on speech and expression. The judgment underscored the principle that the government must implement clear and specific regulations to combat cybercrimes without infringing on free speech. This decision stands as a landmark in cyberspace governance, affirming that individual freedoms must not be sacrificed in the name of public order.

5 Banyan Tree Holding (P) Ltd. vs. A. Murali Krishna Reddy & Anr., 2009 SCC OnLine Del. 3780

6 In *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997), the U.S. court introduced the sliding scale test, a foundational framework for establishing personal jurisdiction in cyberspace. This test distinguishes between passive websites, which merely provide information, and interactive websites, which actively engage users in transactions. The court held that jurisdiction is appropriate when a website intentionally conducts business with users in the forum state..

7 Amway India Enterprises Pvt. Ltd. v. Amazon Seller Services Pvt. Ltd., SLP© No. 6460/2021

deciding which court has authority is essential. Ambiguity in these matters can lead to delays, legal uncertainty, and complications in conflict resolution.

The decision underscores the importance of strong legal frameworks that can effectively address cyberspace jurisdictional issues. As e-commerce continues to expand, establishing legal clarity is crucial to ensuring fairness, fostering trust in digital platforms, and resolving disputes promptly. A consistent framework will allow courts to address cross-border issues in a way that aligns with the digital age's realities, treating all parties fairly.

India's Information Technology (IT) Act, 2000, seeks to address jurisdictional challenges by extending extraterritorial jurisdiction under Section 75.[8] However, unilateral inclusion of such provision in domestic enactments, requiring its enforcing beyond borders would not suffice without cooperation with foreign jurisdictions through agreements like Mutual Legal Assistance Treaties (MLATs).[9] Without such collaboration, legal efforts may be limited, leaving gaps in online regulation.

Legal Governance and Rights in the Digital World

For cyberspace to serve as an integral part of civil society, it must embody the values and norms that shape the physical world. Individuals should have access to the same legal protections online as they do offline, including rights to privacy, freedom of expression, and property. The challenge is to create digital rights frameworks that can evolve alongside new technologies while remaining practical and enforceable.

Law is essential for maintaining order and ensuring that society functions cohesively, preventing chaos. As cyberspace becomes a significant sphere of human interaction, legal frameworks must adapt to regulate this domain, upholding order and safeguarding rights. The objective is to craft laws that encourage responsible conduct and address emerging issues like cyberbullying, data theft, and misinformation.

National Sovereignty and International Cooperation

Governance of cyberspace requires a careful balance between national sovereignty and the need for global collaboration. Countries must protect their citizens from cyber threats while honoring international norms. Initiatives like the Budapest Convention on Cybercrime[10] are vital steps toward coordinated international

8 Section 75 of the Information Technology (IT) Act, 2000, grants India extraterritorial jurisdiction over offenses committed outside its borders if the act involves a computer, computer system, or network located in India. This provision extends India's legal authority into cyberspace, acknowledging the borderless nature of online activities and the limitations of traditional jurisdiction.

While Section 75 aims to address the cross-border nature of cybercrimes, it faces practical enforcement challenges. Although it enables India to prosecute foreign offenders targeting Indian networks, effective implementation relies heavily on international cooperation. The absence of Mutual Legal Assistance Treaties (MLATs) with many countries limits this extraterritorial reach, as gathering evidence and prosecuting offenders abroad require cooperation that may not always be forthcoming.

A significant limitation lies in determining where a cybercrime "occurs" in the virtual world. Many offenses span multiple jurisdictions, complicating which country's laws should apply. For instance, a cybercriminal based in one country could target an Indian user through servers in a third jurisdiction, creating a complex jurisdictional web. In such cases, Section 75 alone is insufficient to secure justice, as collaboration between affected countries becomes essential.

While Section 75 is a progressive step toward addressing cross-border cybercrimes, its effectiveness is limited by enforcement challenges and jurisdictional overlaps. To enhance its impact, India must engage in global cooperation efforts and align its laws with international frameworks like the Budapest Convention on Cybercrime. Such alignment would promote better coordination in investigating and prosecuting cybercrimes across jurisdictions.

9 Mutual Legal Assistance Treaties (MLATs), Ministry of External Affairs, Government of India.

10 The *Budapest Convention on Cybercrime*, developed by the Council of Europe in 2001, is the first international treaty to establish a comprehensive framework for combating cybercrime. Its primary goals are to harmonize national laws, promote

efforts, offering frameworks for cross-border investigation and prosecution. However, this cooperation must adapt continually to meet emerging challenges.

Effective governance in cyberspace calls for a comprehensive legal framework that carefully balances individual freedoms with societal responsibilities. Legal systems must evolve to address jurisdictional complexities, establish clear guidelines for resolving cross-border disputes, and ensure that people enjoy the same rights online as they do offline. Collaborative efforts among nations will be crucial in fostering a secure and fair digital environment that embodies the principles of justice and order.

Through strong governance mechanisms and international cooperation, cyberspace has the potential to become an extension of civil society—a realm where freedom and innovation flourish within the boundaries of law and order.

Analysing the Legal Complexities of Governing Cyberspace

Cyberspace challenges traditional concepts of jurisdiction, presenting unique obstacles for legal governance. Unlike the physical world, cyberspace is a borderless domain without specific governments, dedicated law enforcement agencies, or judicial bodies capable of consistently regulating behaviour or resolving disputes. A functioning legal system typically relies on essential elements: a sovereign authority to enact laws, individuals and entities subject to those laws, institutions to enforce them, and mechanisms to address violations. In cyberspace, these foundational elements are largely absent, creating a governance gap that complicates the enforcement of both national and international laws.

Key Legal Challenges in Governing Cyberspace

Absence of Territorial Boundaries and Fragmentation of Jurisdiction – Traditional legal systems are territorially based, with jurisdiction typically defined by physical boundaries. Cyberspace, however, enables interactions that cross national borders effortlessly. For instance, a person using a mobile network in one country may engage with services hosted in another. Additionally, the underlying hardware and infrastructure[11] supporting these interactions often span multiple jurisdictions. This fluidity poses a challenge for legal frameworks, as determining the applicable jurisdiction for a specific online activity can become highly complex. The interconnected nature of global networks means that no single country can fully control or regulate all activities within cyberspace.[12]

Establishing Jurisdiction Over Users and Networks – Establishing jurisdiction over online users or networks presents significant challenges, especially when services operate across multiple countries. Many software applications and platforms function in several jurisdictions without legal registration in the countries where they are accessed. This lack of regulatory oversight creates enforcement gaps, making it difficult to apply local laws to international platforms. The issue is compounded by the anonymity of users, who may operate under false identities—a common issue in India, where identity theft has led to numerous cases of financial fraud. Even when offenders are identified, the legal process to gather

mutual assistance, and facilitate cross-border investigations. The convention requires member countries to criminalize cyber offenses, including unauthorized access, data interference, and misuse of devices. It also sets forth procedures for expediting evidence-sharing and fostering collaboration through legal channels, such as Mutual Legal Assistance Treaties (MLATs).

11 Such as SIM cards or Wi-Fi networks

12 For example, the Whatsapp is the application that may be used abroad without SIM of the mobile registered at home country. Thus, person having Whatsapp account in India, may use it from Francs, Labia, Argentina by using the same number without being registered in the jurisdiction of the country. At the same time, the network of that country may be employed.

evidence, build cases, and secure convictions is complex and time-consuming, contributing to the low conviction rates for cybercrimes.

Conflicting Legal Standards Across Jurisdictions – Countries have differing laws and standards regarding privacy, freedom of speech, and criminal responsibility. While some nations emphasize protecting individual liberties, others enforce stringent regulations on speech and data privacy. This variation creates challenges in holding offenders accountable when crimes span multiple jurisdictions. For instance, a criminal operating from a country with more lenient laws may evade liability, even if their actions impact users in a region with stricter regulations. Moreover, prosecuting offenders based abroad requires international cooperation, a process often complicated by diplomatic and legal hurdles, as seen in the difficulties surrounding Mutual Legal Assistance Treaties (MLATs).

Low Conviction Rates and Challenges in Evidence Collection Even when offenders are identified and jurisdiction is established, tracing digital activities and collecting admissible evidence poses significant challenges. Cybercrimes often involve encrypted data, anonymous networks, or false identities, making investigations complex and resource-intensive. Law enforcement agencies frequently face obstacles in accessing crucial evidence, especially when data is stored on servers in foreign jurisdictions. These procedural hurdles contribute to India's low conviction rate for cybercrimes, as many cases struggle to progress to final resolution.

The Need for Harmonized Legal Frameworks and International Cooperation

Given the fragmented nature of jurisdiction and the diverse legal standards worldwide, developing more consistent international frameworks is crucial. Initiatives like the Budapest Convention on Cybercrime aim to encourage cooperation between nations, facilitating more effective cross-border investigations and prosecutions. However, many countries, including India, have not yet ratified the convention, underscoring the need for more inclusive and widely accepted international agreements.

Beyond harmonized frameworks, countries must adopt flexible legal mechanisms that account for cyberspace's unique characteristics. Courts have begun addressing these issues, as demonstrated in Banyan Tree Holdings Ltd. v. A. Murali Krishna Reddy,[13] where the Delhi High Court ruled that simply accessing a website does not confer jurisdiction, highlighting the importance of assessing interactivity and targeted engagement in online activities. Likewise, the U.S. case Zippo Manufacturing Co. v. Zippo Dot Com, Inc.[14] introduced the "sliding scale test" to determine whether a website's interactions with users warrant jurisdiction.

Governance of cyberspace demands a nuanced approach that balances national interests, individual rights, and international collaboration. Legal frameworks must evolve to address jurisdictional ambiguities, promote accountability, and protect users without stifling technological progress. Adaptive regulations[15]

13 Banyan Tree Holding (P) Ltd. vs. A. Murali Krishna Reddy & Anr., 2009 SCC OnLine Del. 3780). This judgment settled two conflicting views on jurisdiction over online disputes. In Casio India Co. Limited vs Ashita Tele Systems Pvt. Limited 2003 (27) PTC 265 (DE), the Delhi High Court took a broad approach, holding that mere accessibility of a website from a specific location conferred jurisdiction. However, in (India Tv) Independent News Service Pvt ... vs India Broadcast Live Llc And Ors. 2007(35)PTC177(DEL), the court took the opposite view, emphasizing the need for interactivity and intent for jurisdiction. The Banyan Tree ruling reconciled these approaches by introducing the interactivity test, marking a significant development in Indian cyber jurisprudence.

14 Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).(USA)

15 Adaptive regulation is a flexible approach to policy-making and enforcement that allows legal frameworks to evolve in step with technological, economic, and social changes. Unlike rigid regulations, which may become outdated as technology progresses, adaptive regulations are designed to be responsive and adaptable to new developments. This model emphasizes

and joint collaborative efforts[16] among nations are essential for establishing a legal structure in cyberspace that aligns with principles of justice and fairness. As cyberspace continues to expand, legal systems must adopt dynamic, technology-informed solutions to ensure effective governance in this boundary-less digital landscape.

Legal Complexities in Regulating Cyberspace

Regulating cyberspace poses distinct legal and operational challenges that persist despite diplomatic efforts to establish cyber norms. Cyberspace lacks a cohesive legal framework, instead depending on a patchwork of national laws and sector-specific policies, leading to inconsistencies in enforcement. This fragmented approach complicates efforts to police, monitor, and conduct surveillance across borders effectively. The lack of global consensus on governance mechanisms results in a disordered environment, as countries apply different standards shaped by their own national priorities.

Cyberspace faces following challenges in legal enforcement -

Fragmented Regulatory Frameworks – Cyberspace operates without a unified set of governance rules. Countries manage their internet spaces through domestic laws, such as India's Information Technology Act, 2000, or the European Union's General Data Protection Regulation (GDPR).[17] However, the lack of a global framework leads to overlapping jurisdictions and conflicts in enforcement. Initiatives like the Budapest Convention on Cybercrime attempt to bridge these gaps, but their impact remains limited as key countries, including India, have yet to ratify them..

Sophistication of Cybercriminals – Cybercriminals frequently use sophisticated tools, such as encrypted networks and anonymizing technologies, to commit offenses while leaving little to no traceable evidence. These individuals are adept at exploiting jurisdictional loopholes, often operating across multiple countries with the knowledge that cross-border cooperation among law enforcement agencies can be slow and inconsistent. By the time their activities are detected, they have often vanished, making prosecution a challenging task..

---

continuous monitoring, regular review, and active engagement with stakeholders, ensuring that regulations stay relevant and effective in addressing emerging challenges. In the context of cyberspace governance, adaptive regulation is particularly crucial due to the rapid pace of technological innovation and the emergence of new threats such as cybercrime, misinformation, and privacy breaches. For instance, laws governing digital platforms must continually adapt to tackle issues like data privacy, artificial intelligence, and blockchain technology. Adaptive frameworks enable regulators to introduce incremental changes or new policies informed by real-time data, current trends, and stakeholder input, striking a balance between fostering innovation and safeguarding public interest.

For further reading, see Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding Regulation: Theory, Strategy, and Practice*. Oxford University Press.

16 Joint collaborative efforts are crucial for implementing adaptive regulations in the complex and ever-evolving technological landscape. Adaptive regulation depends on continuous feedback and cooperation among various stakeholders—governments, private companies, civil society, and academia—to effectively address emerging challenges and maintain the relevance of regulatory frameworks.

Collaboration ensures that adaptive regulations remain both flexible and effective, fostering an ongoing exchange of knowledge and expertise. In an era of rapid technological advancement, collaborative governance models are essential for balancing innovation with public safety and promoting accountability. This collective approach enables regulators to respond proactively to new developments while minimizing unintended consequences.

17 The General Data Protection Regulation (GDPR), enforced from May 25, 2018, is a data privacy law introduced by the European Union to regulate the handling of personal data. It applies not only within the EU but also to companies outside the region that process the data of EU residents. GDPR provides individuals with rights such as access to their data, correction or deletion, and ensures that consent is mandatory for data collection. Organizations must also report data breaches within 72 hours. Non-compliance results in significant fines, promoting responsible data management and transparency in data practices.

Limitations of Traditional Law Enforcement - Law enforcement agencies are constrained by traditional investigative methods and a shortage of technologically skilled personnel**.** While the police have significant powers under various legal enactments,[18] often struggle to apply these powers effectively in cyberspace. Many cybercrimes originate from anonymous sources or foreign jurisdictions, complicating investigations. The low conviction rate for cybercrimes in India[19] reflects these challenges,[20] as tracing offenders and gathering admissibility of digital evidence[21] is often beyond the capabilities of traditional law enforcement methods. In addition, the chain of custody of electronic evidence also pose further challenges during criminal trial that lower down the conviction rate in cybercrimes. The SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra[22] is the glaring example that exhibit how difficult to appreciate the digital evidence in the course of criminal proceeding.

Operational Constraints in Law Enforcement - Police forces are often required to focus on administrative or non-crime-related tasks, reducing the resources available for cybercrime investigation. Given their limited manpower and competing priorities, law enforcement agencies struggle to allocate sufficient attention to complex online crimes that require specialized skills and equipment. These operational constraints further widen the gap between offenders and enforcement agencies, making it harder to bring cybercriminals to justice.

18 Such as such as the Information Technology Act, 2000 and the Indian Penal Code, 1860

19 Even among cybercrime cases that completed trial, the conviction rate stood at just 42.5. Out of the 1,155 cases that completed trial in 2021, only 491 ended in a conviction. Meanwhile, 591 cases, which is more than half of the total, ended in an acquittal and another 87 cases got discharged. See, https://www.moneycontrol.com/news/india/cyber-crimes-in-india-rise-6-a-year-in-2021-telangana-tops-list-ncrb-data-9115161.html visited on 25.03.2022

20 The conviction rate for cybercrimes in India remains low, highlighting challenges in enforcement. According to NCRB data, although cybercrime cases are steadily increasing—reaching nearly 66,000 registered cases in 2022—the rate of convictions is concerningly low due to challenges like weak forensic capabilities, procedural delays, and jurisdictional issues. Some states and Union Territories reported zero convictions despite multiple cases. Strengthening cyber forensics, streamlining procedures, and enhancing international collaboration are essential to improving this situation.

21 In India, the admissibility of digital evidence faces challenges related to authenticity, reliability, and compliance with legal procedures. Courts require strict adherence to Section 65B of the Indian Evidence Act, 1872, which mandates proper certification of digital records for them to be admissible. Failure to comply often results in the rejection of evidence. In *Anwar P.V. vs P.K. Basheer & Others* (AIR 2015 SC 180), the Supreme Court ruled that electronic records must fulfill the criteria under Section 65B to be admissible. This requirement was reinforced in *Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal* (AIR 2020 SC 4908), where the Court emphasized the importance of procedural rigor in certification. These rulings underscore the need for meticulous collection and documentation of digital evidence to ensure its acceptance in court..

22 The case of *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra* (CM APPL. No. 33474 of 2016) underscores significant challenges in balancing digital and physical evidence in cyber defamation disputes. The case involved a former employee allegedly sending defamatory emails to tarnish the reputation of the company and its Managing Director. The Delhi Court issued an ex-parte injunction based on prima facie evidence, but the ruling highlighted the difficulty in directly linking the defendant to the emails due to weak digital evidence.

Although private computer experts traced the emails to a cybercafé, the evidence remained inconclusive. The defendant's identification by the cybercafé attendant using a group photograph was also insufficient, as the photograph was not presented as evidence. Additionally, discrepancies in email timestamps raised further doubts. The court's reliance on circumstantial rather than direct digital evidence highlights the complexities in cybercrime cases where digital trails are fragmented or inadequately preserved.

This case illustrates the critical need for robust digital forensic practices and stringent evidentiary standards, especially when physical evidence is absent or weak. It also emphasizes the importance of procedural rigor under Section 65B of the Indian Evidence Act, which governs the admissibility of electronic records. To address such complexities in cyberspace governance, effective legal frameworks and cross-jurisdictional cooperation are essential.

Judicial Response to Jurisdictional Challenges in Cyberspace

The court at several instances encounter the issues of jurisdictional challenges in cyberspace. While attempting to resolve the same, Courts have developed various tests, such as the interactivity test,[23] intent-based test,[24] sliding scale test,[25] Minimum Contacts Theory,[26] effect test[27] and harm-based tests,[28] to address jurisdictional issues in cross-border digital activities. These rulings reflect the evolving approach to internet governance, underscoring the complexities of applying national laws to a global cyberspace and the need for harmonization across jurisdictions.

Judicial responses to jurisdictional challenges in cyberspace reveal evolving principles shaped by Indian and international cases. In Banyan Tree Holdings v. A. Murali Krishna Reddy,[29] the Delhi High Court introduced the interactivity test, ruling that the mere accessibility of a website does not establish jurisdiction unless it actively targets users. Similarly, in India TV v. India Broadcast Live LLC, [30] the court emphasized intent-based jurisdiction by asserting authority over a foreign-hosted website specifically targeting Indian users.

In the United States, Zippo Manufacturing v. Zippo Dot Com[31] pioneered the sliding scale test, where jurisdiction is determined by the level of a website's interactivity. In contrast, Australia's Dow Jones &

23 Interactivity Test - This test determines whether a website is passive (merely informational) or interactive (engaging users in transactions). The Delhi High Court in Banyan Tree Holding (P) Ltd. vs. A. Murali Krishna Reddy & Anr., 2009 SCC OnLine Del. 3780) ruled that mere accessibility does not confer jurisdiction unless the website interacts with users in the forum state.

24 Intent-Based Test - This test focuses on the intent of the online entity to target users within a specific jurisdiction. In (India Tv) Independent News Service Pvt vs India Broadcast Live LLC And Ors. MIPR 2007 (2) 396, the court asserted jurisdiction because the foreign website intentionally targeted Indian users.

25 Sliding Scale Test - Developed by the U.S. District Court in Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).(USA), this test assigns jurisdiction based on the level of interaction between the website and users in the forum state. Higher interactivity increases the likelihood of jurisdiction.

26 The Minimum Contacts Theory helps courts determine jurisdiction when one or both parties are located outside the court's territorial limits. This concept was established by the U.S. Supreme Court in Washington v. International Shoe Co., where the court ruled that jurisdiction can apply if a defendant engages in activities within the forum state, thereby benefiting from its protections.

The theory requires three elements:

i. The defendant must purposefully avail themselves of the forum's benefits.
ii. The claim must arise from the defendant's forum-related activities.
iii. The exercise of jurisdiction must be reasonable.

In CompuServe, Inc. v. Patterson 89 F.3d 1257 the court extended this theory to cyberspace, holding that online contracts also establish minimum contacts, provided the interactions meet the above criteria. This approach ensures fairness by limiting jurisdiction to cases where meaningful interaction or harm occurs within the forum state.

27 The effect test establishes jurisdiction over non-residents in cases where their actions intentionally cause harm within the forum state, even if they have no direct contact with it. In Calder v Jones ,465 US 783 (1984), the U.S. Supreme Court ruled that personal jurisdiction was appropriate in California because the defendants, though based in Florida, published defamatory content targeting a California resident, knowing the harm would be felt there. Similarly, in Panavision International v Toeppen,141 F 3d 1316 (9th Cir1998), the California court asserted jurisdiction over a non-resident defendant involved in trademark misuse, applying the effect test to cyberspace crimes.

28 Harm-Based Test - This test establishes jurisdiction based on the location where harm occurred. In Dow Jones & Co. v. Gutnick (2002) 77 ALJR 255 (Australia), the court ruled that jurisdiction could be asserted in the place where defamatory content was accessed, emphasizing the impact on the victim

29 Banyan Tree Holding (P) Ltd. vs. A. Murali Krishna Reddy & Anr., 2009 SCC OnLine Del. 3780

30 (India TV) Independent News Service Pvt vs India Broadcast Live LLC And Ors. MIPR 2007 (2) 396

31 Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).

Co. v. Gutnick[32] relied on an impact-based approach, holding that harm from online defamation establishes jurisdiction where the content is accessed.

Adding to this complexity, the French court in Licra v. Yahoo! Inc.[33] asserted extraterritorial jurisdiction, regulating content hosted outside its borders. On the evidentiary front, the Indian Supreme Court in Arjun Panditrao Khotkar v. Kailash Gorantyal[34] emphasized adherence to Section 65B of the Indian Evidence Act, reinforcing strict procedural requirements for the admissibility of digital evidence.

These cases collectively illustrate the diverse judicial approaches—based on interactivity, intent, harm, and procedural compliance—that are shaping global jurisprudence on cyberspace jurisdiction. They underscore the pressing need for harmonized frameworks to reconcile conflicts between national laws and international governance standards.

Comparative Analysis of Jurisdictional Tests in Cyberspace

Courts have developed various tests to address the challenges of jurisdiction in the digital world, each with distinct strengths and limitations. Below is a comparison of the interactivity test**,** intent-based test**,** sliding scale test**,** minimum contacts theory**,** effect test**,** and harm-based test**.**

1. Interactivity Test

Key Idea: This test differentiates between passive websites (information-only) and interactive ones (engaging users in transactions or communication).

Strength: Assists courts in identifying meaningful interactions with a specific jurisdiction.

Weakness: Assessing interactivity can be subjective and may overlook websites that provide substantial non-transactional engagement, such as social media platforms.

Notable Case: Banyan Tree Holdings v. A. Murali Krishna Reddy (India) – Jurisdiction was established based on the interactivity of the website, specifically targeting users.

2. Intent-Based Test

Key Idea: Jurisdiction applies if the defendant intentionally targets the forum state or its residents.

Strength: It prevents arbitrary jurisdiction by focusing on deliberate actions.

Weakness: Proving intent can be challenging, especially in cases of ambiguous online activity.

Notable Case: India TV v. India Broadcast Live LLC (India) – website targeted Indian users intentionally, establishing jurisdiction.

3. Sliding Scale Test

Key Idea: Jurisdiction is determined by the level of interaction and commercial activity on a website. Passive websites do not attract jurisdiction, while highly interactive ones may.

Strength: Provides a nuanced framework based on the extent of user interaction.

Weakness: The subjective assessment of interactivity levels can complicate consistent application.

Notable Case: Zippo Manufacturing v. Zippo Dot Com (USA) – Introduced the sliding scale test for determining jurisdiction over web-based interactions..

4. Minimum Contacts Theory

Key Idea: Jurisdiction can be established if the defendant has substantial connections, or "minimum contacts," with the forum state, even without physical presence.

32 Dow Jones & Co. v. Gutnick (2002) 77 ALJR 255

33 Licra v. Yahoo! Inc. 169 F. Supp. 2d. 1181 (N.D. Cal. 2001)

34 Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal AIR 2020 SC 4908

Strength: Promotes fairness by requiring that defendants have meaningful ties to the jurisdiction.
Weakness: In cyberspace, determining "sufficient contacts" is challenging as online activities often span multiple regions.
Notable Case: Washington v. International Shoe Co. (USA) – Established the foundational principle of minimum contacts in jurisdiction.

5. Effect Test

Key Idea: Jurisdiction is applicable if the defendant's actions, though conducted outside the forum state, intentionally cause harm within it.
Strength: Emphasizes the location of the harm, making it especially relevant for cases of defamation and cybercrimes.
Weakness: This approach can extend jurisdiction broadly, potentially subjecting defendants to litigation in multiple locations.
Notable Case: Calder v. Jones (USA) – Jurisdiction was established as the defamatory publication caused harm in California.

6. Harm-Based Test

Key Idea: Jurisdiction is determined by the location where the impact or harm of the defendant's actions is felt, regardless of where the perpetrator is located.
Strength: Valuable for cases involving defamation, fraud, or exploitation, as it considers the harm experienced by victims.
Weakness: Like the effect test, this approach can expand jurisdiction broadly, potentially complicating enforcement.
Notable Case: Dow Jones & Co. v. Gutnick (Australia) – Jurisdiction was established where defamatory material was accessed by the affected party.

Comparative analysis of various tests determining Jurisdictional issues in Cyberspace

Test	Strengths	Weaknesses
Interactivity Test	Identifies targeted engagement	Subjectivity in determining interactivity
Intent-Based Test	Focuses on Deliberate Targeting	Providing Intent is difficult
Sliding Scale Test	Evaluates degrees of interaction	Subject to interpretations
Minimum Contacts Theory	Ensures fairness with meaningful connections	Hard to apply consistently in cyberspace
Effect Test	Considers intentional harm	Risk of Overextending Jurisdiction
Harm-Based Test	Focuses on Victim's location of Harm	Complicates cross-border enforcement

Which Test is Most Sustainable?

The sliding scale test and minimum contacts theory stand out as more sustainable approaches for determining jurisdiction in cyberspace. The sliding scale test offers a balanced perspective by assessing different levels of interaction, which aligns well with the fluid and evolving nature of online activities. Meanwhile, the minimum contacts theory ensures fairness by requiring a genuine connection to the forum state, thereby preventing arbitrary assertions of jurisdiction.

While the effect and harm-based tests are useful in cases where harm occurs remotely, they risk overextending jurisdiction, which can lead to legal uncertainties and cross-border conflicts. Similarly, the interactivity and intent-based tests, although valuable, may fall short in addressing complex cases involving ambiguous online behavior.

In examining judicial approaches to modern jurisdictional challenges in cyberspace, a hybrid approach that combines elements of the sliding scale test with minimum contacts theory appears most effective. This approach allows courts to evaluate both the degree of interaction and the meaningful connection to the forum state, promoting a fair and consistent application of jurisdiction. Such a framework would provide a balanced approach to fairness, accessibility, and accountability, making it well-suited to the dynamic and boundaryless nature of cyberspace.

Proposed Solutions for Effective Governance

Establishing a Global Governance Framework - There is a need for an international framework that harmonizes cyber laws across jurisdictions. The Budapest Convention on Cybercrime offers a starting point, but countries must overcome political differences and ratify a common treaty to streamline cooperation in cybercrime investigations. Establishing clear jurisdictional rules will help prevent forum shopping and ensure that offenses committed in cyberspace are effectively prosecuted.

Enhancing Cross-Border Collaboration - Nations should strengthen mutual legal assistance treaties (MLATs)[35] to expedite evidence sharing and prosecution in cross-border cybercrimes. A robust mechanism for international cooperation will allow countries to hold offenders accountable, even if they operate from foreign jurisdictions.

Upgrading Law Enforcement Capabilities – Police forces need to modernize their investigative tools and techniques, placing a stronger focus on cyber forensics and digital evidence management. Recruiting and training personnel skilled in information technology is crucial for tracking and apprehending sophisticated cybercriminals. Additionally, law enforcement agencies should collaborate with private-sector partners, such as internet service providers and cybersecurity firms, to enhance efforts in detecting and preventing online crimes.

Efficient Allocation of Resources – Governments should allocate sufficient resources to law enforcement agencies, ensuring that officers are not weighed down by non-essential tasks. By prioritizing cybercrime prevention, authorities can more effectively address the growing threat of online offenses and work toward improving overall conviction rates..

35 Mutual Legal Assistance Treaties (MLATs) are international agreements between two or more countries designed to facilitate cooperation in criminal investigations, prosecutions, and law enforcement. MLATs enable the sharing of evidence, execution of warrants, and transfer of witnesses or suspects across borders. These treaties are vital for addressing cross-border crimes such as cybercrime, terrorism, and money laundering, where international cooperation is crucial for effective enforcement. However, challenges like procedural delays and differing legal standards between countries often impede their efficiency.

Effective governance of cyberspace demands a multi-faceted approach that balances national interests, international collaboration, and individual rights. Law enforcement agencies must adapt to the shifting landscape of online crimes by adopting advanced technologies and fostering international partnerships to close the gap between offenders and the law. Establishing a unified framework for cyber governance and building specialized capabilities within police forces will be crucial in addressing the challenges of cyberspace and promoting accountability in the digital realm.

Cyberspace: Issues of Accessibility, Digital Inequality, and Governance Challenges

Cyberspace offers unparalleled opportunities but also presents substantial challenges, exposing structural inequalities and governance gaps that are not easily resolved. Key issues include the digital divide,[36] unregulated content,[37] threats to privacy and security[38]—particularly for vulnerable groups such as women and children—and conflicting international interests.[39] These challenges call for thoughtful legal and policy solutions to ensure a safer and more inclusive digital environment.

Digital Inequality: The Divide Between the Haves and Have-Nots

Access to cyberspace is still largely confined to certain privileged groups, deepening existing social and economic inequalities. The digital divide—the disparity between those with access to technology and those without[40]—presents a serious challenge for governance. Recent estimates suggest that while India

36 The digital divide refers to the gap between individuals or communities with access to digital technologies, like the internet and computers, and those without. This divide is often shaped by factors such as economic status, education, infrastructure, and geography, leading to unequal access to information, opportunities, and essential services. In today's digital age, this disparity has become even more pronounced, as governments increasingly depend on online platforms for public services, education, and healthcare. Those lacking digital access are at a significant disadvantage, further reinforcing social and economic inequalities.

37 Unregulated content refers to online material that lacks oversight by regulatory authorities, making it challenging to control or monitor. This includes harmful content such as hate speech, misinformation, child exploitation material, extremist propaganda, and illegal marketplaces. Without regulation, there is often a proliferation of misleading information, public harm, and privacy violations. While platforms may implement internal moderation tools, enforcement is frequently inconsistent. Balancing free expression with content regulation remains a central challenge in cyberspace governance, underscoring the need for well-balanced regulatory frameworks..

38 Privacy and safety have become pressing concerns in the digital age. With the rise of data breaches, cyberstalking, identity theft, and online harassment, individuals are increasingly at risk. Personal information shared online can be exploited, leading to financial fraud, reputational damage, or targeted harassment. Vulnerable groups, particularly women and children, are especially susceptible to threats like cyberbullying and exploitation. Weak data protection policies, unregulated platforms, and insufficient cybersecurity measures further intensify these risks. Addressing these challenges calls for stronger data privacy laws, robust security protocols, and effective international cooperation.

39 Conflicting international interests in cyberspace governance stem from the differing political, economic, and regulatory priorities of various nations. Countries like China and Russia advocate for cyber sovereignty, prioritizing state control over internet governance within their borders. In contrast, the United States, the European Union, and other liberal democracies support a multi-stakeholder model that includes private entities and civil society in decision-making. These ideological divides make it challenging to establish unified frameworks for combating cybercrime and protecting privacy. The absence of global consensus complicates cooperation in areas such as cross-border data flows, cybersecurity, and online content regulation.

40 The digital divide has led to differing priorities among nations, hindering efforts to harmonize domestic cybercrime laws with international standards. A notable example is the Budapest Convention on Cybercrime, the first and only international treaty dedicated to combating cybercrime. Despite its significance, the convention has not been signed or ratified by any ASEAN member states, indicating the region's hesitancy to adopt a common legal framework for cybercrime regulation.

The Budapest Convention promotes cooperation among states in investigating and prosecuting cybercrime by establishing uniform legal standards. It encourages signatories to implement both substantive and procedural laws targeting offenses related to data confidentiality, system integrity, and technology misuse. These offenses include unauthorized access to computer systems, illegal interception of data transmissions, interference with computer functions, and the deployment of malicious software or devices.

has around 833 million internet users, many of these individuals maintain multiple connections, which can distort data on actual accessibility.[41] A significant portion of the population, particularly in rural areas and low-income communities, remains disconnected from the benefits of digital infrastructure.
Governments increasingly rely on digital platforms for public services**,** including the transfer of subsidies through Aadhaar-linked accounts, distribution of welfare benefits, and digital literacy campaigns. However, marginalized populations, particularly the poor and illiterate, find it difficult to access these services, deepening existing inequalities.[42] The reliance on online governance risks excluding large portions of the population, failing to uphold the principle of equal access to public services.

Legal and Policy Response:

- Bridging the digital divide requires targeted investment in infrastructure and digital literacy programs**.** Policies need to ensure universal access to affordable internet services and introduce offline alternatives for public service delivery to avoid exclusion.
- Courts in India have underscored the importance of digital accessibility in governance, emphasizing that exclusion from digital systems should not deprive individuals of their legal rights.[43]

Governance and the Risks of an Unregulated Cyberspace

The lack of effective governance in cyberspace has made it a breeding ground for illegal activities such as child pornography, data theft, cyberstalking**,** and the spread of misinformation. Websites promoting harmful activities, including unauthorized dating sites, are difficult to regulate under existing legal frameworks. With the advent of technology, cyber-crime and victimization of women are on the high and it poses as a major threat to the security of a person as a whole.[44] Similar state of affair prevails in case of children too and child pornography rather more rampant in cyberspace. With emergence of technology, Cyberspace emerges with a new horizon controlled by machine for information and any criminal activity[45]

While the treaty seeks to support cross-border investigations and expedite evidence-sharing through mutual legal assistance mechanisms, resistance from ASEAN countries underscores the difficulties of adopting universal cybercrime frameworks. This reluctance often stems from concerns over cyber sovereignty, differing governance models, and fears of external influence on domestic law enforcement policies.

To address this gap, regional frameworks and cooperative initiatives adapted to local contexts may serve as a viable alternative until broader consensus on international cybercrime regulation is achieved..

41 Total population of India is estimated in 2021 is 135 crores expected entireness are 83.3 means 61.6 %. However, there are multiples connection, and therefore, a guess of only 48 % of netizens of total populations estimated. Source, https://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users visited on 22.09.2021

42 The Aadhaar system has been essential for streamlining government services, but it has also led to significant exclusion, especially among marginalized populations. Problems such as biometric failures, lack of access to technology, and difficulty in updating Aadhaar details disproportionately affect the poor, elderly, and disabled, making it hard for them to access welfare services. Delayed, blocked, or diverted payments—particularly in schemes like MGNREGA and pensions—further worsen the situation, leaving many without critical benefits. These systemic challenges highlight the need for alternatives to digital-only service delivery to ensure inclusivity and equity in welfare distribution. See, https://www.insightsonindia.com/2021/10/02/concerns-about-using-aadhaar-in-welfare-schemes/

43 See, Justice K.S.Puttaswamy (Retd) vs Union Of India AIR 2018 SC (SUPP) 1841. Popularly known as ‘Aadhar case’.

44 Jain (Dr) Jain Monika, Victimization of women beneath cyberspace in Indian Upbringing, Publsihed in Bharati Law Review, April – June, 2017 pg. 2. Available at http://docs.manupatra.in/newsline/articles/Upload/786274E9-B397-4610-8912-28D6D03230F9.monika_jain_pdf_1-1111.pdf visited on 03.12.2021

45 Jeet Shobhna, Cyber-crimes against women in India: Information Technology Act, 2000, Elixir Criminal Law 47 (2012) 8891-8895, Elixir International Journal.

where computer or network is used as the source, tool or target is known Cybercrime.[46] There are also issues with data theft, hacking, and denial-of-service attacks**,** which can disrupt essential services, including military operations and critical infrastructure.

Legal and Policy Challenges:

- Content regulation remains inconsistent, as different jurisdictions apply varied standards for regulating offensive or illegal content. While some countries adopt stringent internet censorship policies, others prioritize freedom of expression over regulation, making enforcement challenging.
- International treaties, such as the Budapest Convention on Cybercrime**,** offer a framework for cooperation, but differences between countries over cyber sovereignty and multi-stakeholder governance models—championed by Russia and China versus liberal democracies—hinder global consensus.

Legal Response:

- India has enacted the Information Technology Act, 2000, to regulate cyber activities, but its effectiveness remains limited due to jurisdictional challenges and evolving cyber threats. The lack of international cooperation further complicates enforcement.
- A renewed focus on data protection laws**,** as seen in the Digital Personal Data Protection Act, 2023, aims to safeguard privacy and mitigate risks, but enforcement remains uneven.

Safety and Security for Women and Children in Cyberspace

Cyberspace presents serious risks for women and children, including cyberstalking, online harassment, and the spread of child pornography.[47] Women often face privacy violations, blackmail, and identity theft, which discourage their engagement on digital platforms. The lack of effective legal protections and enforcement mechanisms worsens these issues, leaving vulnerable groups more susceptible to exploitation and harm in online spaces.

Legal and Policy Recommendations:

- Strengthening laws addressing cyberstalking and online abuse—such as provisions under the Indian Penal Code and Information Technology Act—is essential to ensure accountability.

46 However, it has to be noted down that the word 'crime' has no where defined in the legal books (Except in General Clauses Act, 1897 but with very general context). The word that employee in the legal provisions is the 'offences' which has been well defined, and there is separate Chapter XI in the Information Technology Act, 2000 that deal with the offences committed in the cyberspace. Therefore, in this article, the word offences and contravention has been used to denote any harm or contravention committed in cyberspace.

47 Cyber technology has been weaponized in numerous ways against women and children, who are often targeted for exploitation. Both groups are frequently objectified and commodified through the sharing of pornographic material online, with offenders using this content for blackmail or extortion. Victims experience stalking and harassment, with perpetrators hiding behind fake identities or creating false profiles to mask their actions. Children are especially vulnerable to grooming, trafficking, and child pornography, while women face threats like revenge porn and identity theft. The anonymity provided by cyberspace allows offenders to evade detection, and the absence of strong cross-border cooperation complicates enforcement efforts. Addressing these issues requires robust legal frameworks, timely enforcement, and improved international collaboration. See for more details, Sinclair-Blakemore, Adaena, Cyberviolence Against Women Under International Human Rights Law, 23 Hum. Rts. L. Rev. 1 (2023)

- Courts have taken a proactive stance in protecting privacy, as highlighted in cases like Justice K.S. Puttaswamy v. Union of India,[48] affirming the right to privacy as a fundamental right. However, the enforcement of these protections remains a challenge.
- Collaborations between governments, tech companies, and civil society are essential to implement cybersecurity protocols and promote safe online spaces for women and children.

Conflicting International Models of Cyber Governance

The most significant hurdle in establishing global governance in cyberspace is the ideological divide among nations. Some countries, like China and Russia, advocate for cyber sovereignty, where individual states control the internet within their borders. In contrast, liberal democracies[49] favour a multi-stakeholder model,[50] emphasizing global cooperation among governments, private entities, and civil society. This conflict impedes the creation of a unified regulatory framework for cyberspace.

Proposed Solution:

A global consensus on cyberspace regulation should align with social contract principles, balancing state interests with individual freedoms. International cooperation is crucial to harmonize regulations, tackle cybercrime, and safeguard users' rights worldwide.

Effective governance of cyberspace requires innovative legal solutions that address accessibility, inequality, safety, and cross-border collaboration. Bridging the digital divide, regulating harmful content, and protecting vulnerable users are essential steps toward creating a safer, more inclusive digital environment. Nations must adopt flexible governance models[51] that adapt to the evolving nature of cyberspace, ensuring accountability and protecting individual rights while fostering cooperation across jurisdictions.

However, the biggest hurdle in bringing the harmony in governance in cyberspace is the conflicting interest that divide the nations. The divide between nations that support governance models based on cyber sovereignty, primarily China and Russia, and those that believe in the multi-stakeholder model, including most liberal democracies, is one of the most prominent ideological conflicts dividing

48 Justice K.S.Puttaswamy (Retd) vs Union Of India AIR 2018 SC (SUPP) 1841. Popularly known as 'Aadhar case'.

49 Liberal democracies are political systems that uphold individual freedoms, the rule of law, and governance through elected representatives. They emphasize values such as freedom of expression, human rights, and privacy. In cyberspace governance, liberal democracies support a multi-stakeholder model, promoting collaboration among governments, private companies, and civil society to regulate the internet. This approach contrasts with cyber sovereignty models, where states exert strict control over online activities. By balancing regulation with innovation, the approach of liberal democracies aims to protect digital rights while addressing evolving cyber challenges..

50 A multi-stakeholder model emphasizes inclusive governance by engaging governments, private companies, civil society, and academia in decision-making processes. This approach ensures that policies are shaped by diverse perspectives, promoting innovation while addressing public interests. In cyberspace governance, it fosters collaboration to tackle challenges like cybercrime, data privacy, and content regulation. Unlike state-controlled frameworks, this model distributes responsibilities across stakeholders, enhancing transparency and accountability. It aligns with the values of liberal democracies, aiming for a balanced, adaptive, and inclusive regulatory framework.

51 Adaptive governance models are designed to respond flexibly to changing conditions and uncertainties. These frameworks rely on continuous feedback, collaboration among stakeholders, and iterative decision-making processes to address complex issues effectively. Adaptive governance is commonly applied in fields like cybersecurity and environmental policy, where conditions evolve rapidly, requiring constant policy updates. It encourages public-private partnerships, regulatory experimentation, and innovation, allowing systems to remain resilient and relevant over time.

cyberspace.[52] However, the battle for supremacy and competitive interest involve prohibit bringing all international community on any agreed platform. This again reflects the need of revisiting the agreed ideology of 'social contract'[53] on cyberspace

Conclusion: Addressing the Gaps in Cybercrime Governance

The evolving nature of cyberspace presents significant challenges for national and international legal systems. The digital divide has created divergent priorities among nations, complicating efforts to harmonize cybercrime laws across borders. While the Budapest Convention on Cybercrime offers a foundational framework for cooperation, its limited adoption—particularly among ASEAN states—illustrates the reluctance of many countries to relinquish aspects of cyber sovereignty.

This resistance underscores the core challenge of creating a universal model for cyber governance amid diverse political, legal, and cultural perspectives. Additionally, the borderless nature of cyberspace complicates the application of traditional, geography-based legal principles. Cybercriminals exploit jurisdictional loopholes, leveraging encryption, anonymity, and cross-border inconsistencies to evade detection and prosecution, exposing major vulnerabilities in legal systems. The lack of consistent international collaboration and fragmented enforcement mechanisms,[54] leads to accountability gaps, leaving nations struggling to protect data confidentiality, privacy, and system integrity.

Furthermore, current frameworks often fall short in addressing the specific threats faced by vulnerable groups, especially women and children, who increasingly encounter risks like cyberstalking, online harassment, and exploitation. Although national governments have started implementing data protection laws[55]—such as India's Digital Personal Data Protection Act, 2023—enforcement is inconsistent, and limited cooperation between countries hinders efforts to effectively prosecute offenders.

52 Eric Rosenbach & Shu Min Chong, Governing Cyberspace: State Control vs. The Multistakeholder Model, published at Belfer Center for Science and International Affairs, Harvard Kennedy School. Available at https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model visited on 14.12.2021. The authors attempted to analyses various models and different theories for probable governance of internet.

53 Social contract theory, nearly as old as philosophy itself, is the view that persons' moral and/or political obligations are dependent upon a contract or agreement among them to form the society in which they live. In its wider connotations the theory of Social contract argue that individuals have consented, either explicitly or tacitly, to surrender some of their freedoms and submit to the authority (of the ruler, or to the decision of a majority in exchange for protection of their remaining rights or maintenance of the social order. The author of this article, emphasis the need of yet another 'social contract', this time amongst the nation themselves to surrender some of their freedoms and submit to submit to the international authority that collectively form to regulate the cyberspace in exchange for protection of their remaining rights or maintenance of the social order. (Emphasis added)

54 Fragmented enforcement mechanisms highlight the challenges of coordinating across jurisdictions to regulate and address cross-border issues, such as cybercrime and data privacy violations. Differences in legal standards, regulatory frameworks, and enforcement priorities make effective international cooperation difficult. This fragmentation results in investigative delays, weakens accountability, and allows offenders to exploit jurisdictional gaps. Harmonizing laws and strengthening international collaboration through treaties like the Budapest Convention are essential steps toward achieving more cohesive enforcement.

55 The proposed Digital Personal Data Protection Act, 2023, soon tabled in Parliament, evolved from recommendations by the 2017 Committee of Experts on Data Protection. The act follows the Supreme Court's judgment in Justice K.S. Puttaswamy vs. Union of India, which recognized the right to privacy as part of the fundamental right to life under Article 21 of the Constitution. A 2019 bill was introduced but referred to a parliamentary committee, which issued its report in 2021, leading to the formulation of the 2023 Act to protect personal data.

A Proposed Solution: The Multi-Layered Cyber Governance Model

To address the challenges of cybercrime governance effectively, a multi-layered governance model[56] is proposed. This model integrates global, regional, and national frameworks, providing a flexible yet coordinated approach that can accommodate diverse legal systems while promoting cooperation.

Global Framework for Core Principles - At the global level, core principles of cyber governance should be established through a new international treaty modeled after the Budapest Convention**,** with provisions that address the concerns of non-signatory nations, such as data sovereignty and jurisdictional autonomy**.** The treaty would concentrate on:

Defining universal offenses related to data integrity, including hacking, illegal data interception, and malware distribution.

Establishing minimum standards for data protection and privacy safeguards.

Creating mechanisms for mutual legal assistance and fast-tracked evidence-sharing to tackle the challenges of cross-border investigations.

Regional Cooperation and Harmonization of Laws – Regional organizations, such as ASEAN, the European Union, and the African Union, should develop frameworks that align with global treaties while accommodating local socio-political contexts. Regional cooperation can promote harmonization by:

Offering localized training and capacity-building programs for law enforcement agencies.

Creating regional cybersecurity centers to monitor threats and facilitate intelligence sharing.

Facilitating joint investigations and extradition agreements to ensure accountability across borders.

National-Level Implementation and Community Engagement At the national level, countries should enhance their domestic legal frameworks by:

Incorporating provisions from global treaties into domestic laws to promote consistency and enforceability.

Investing in cybersecurity infrastructure and training technologically skilled personnel to combat advanced threats.

Promoting digital literacy and public awareness campaigns to empower citizens and mitigate risks of online exploitation..

Multi-Stakeholder Governance Model – Beyond formal legal frameworks, this model supports a multi-stakeholder approach that brings together governments, technology companies, civil society, and international organizations. Such collaboration helps ensure that cyber governance policies reflect the diverse interests of all stakeholders. Key components of this approach include:

Establishing public-private partnerships to strengthen cybersecurity measures.

Engaging civil society organizations in policy-making to protect fundamental rights and promote transparency.

Encouraging self-regulation by technology companies to monitor and control the spread of harmful content.

56 A multi-layered governance model provides a flexible approach for addressing complex issues, integrating global, regional, and national frameworks. In the realm of cyber governance, this model ensures that international cooperation aligns with regional priorities and respects national sovereignty. It fosters collaboration among governments, private companies, and civil society to tackle challenges such as cybercrime and digital inequality. By balancing regulation with innovation, this layered approach promotes adaptive and inclusive policies while strengthening cross-border enforcement through frameworks like the Budapest Convention.

A Path Forward for Inclusive and Effective Cyber Governance

The multi-layered governance model presents a promising approach to addressing the challenges of cybercrime while respecting the diversity of national legal systems and political ideologies. By balancing global cooperation with regional and national autonomy, this model offers a flexible and inclusive framework for cyber governance. It recognizes the importance of individual freedoms while enabling governments to effectively tackle cybersecurity threats.

Postulates for the success of a multi-layered governance model

The fundamental requirement for the success of this model lies in creating a safer and more equitable digital environment. Achieving this goal depends on -

- trust and collaboration between nations,
- a willingness to prioritize collective security over narrow national interests.
- harmonising legal standards**,**
- investing in technological capabilities, and
- fostering multi-stakeholder engagement

Only through coordinated efforts can the international community reduce the risks of cybercrime, protect vulnerable groups, and foster a secure and inclusive cyberspace for all users.