ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 10, 2022

# THE JUXTAPOSING BOUNDARIES OF CRIME AND CENSORSHIP IN CYBERSPACE

**Jesmi Jacob**
Research Scholar, School of Indian Legal Thought, Kottayam
Assistant Professor, Rajagiri College of Management and Applied Sciences
jesmijacob29@gmail.com

## ABSTRACT

Crime is not a stagnant entity but it evolves shifts and remains an ever-tempting phenomena. Cyberspace adds sharper and eclectic edges to human imagination and ubiquity. Human mind constantly analyses the variables and manoeuvres available in committing and enacting crimes. The umbrella of networks with varying divergence tactics in cyberspace that hides and helps in anonymity and pervasiveness results in a pandemonium that is hard to control and harder to perceive. And that's where censorship comes into play. But the question arises whether it has succeeded in suppressing the anti-social human tendencies or failed to do so as society's vulnerability to cybercrime increases in tandem with the internet technology and its usage. Suppression of data directly conflicts with protection of data as it takes away access to data and information. Development of anti-censorship tools and the growing circumventing technologies puts the lawmakers into a bind regarding the viability of censorship. The article tries to examine whether prevention is better than cure and is censorship the only answer to cyber-crimes.
***Keywords:*** *Crime, Censorship, Internet, Data, Cyber, Technology, Cyberspace*

Censorship reflects the society's lack of confidence in itself

Peter Stewart

## INTRODUCTION

Censorship in actuality is curbing of self-expression implemented through social censorship and political censorship.[1] Censorship pertains to a simple fact of what can be included and what cannot be included under the right to freedom. But the definition of freedom itself is restrictive as its very essence depends on the particular democratic society or the political regime as freedom itself is not an independent variable. Censorship may come from the fear of not been able to control but more than fear it's the effortlessness that attracts the policy makers to implement it. But does it cure the root problem rather than examining why it is happening or how far it has impacted the population, censorship is sometimes applied blindly without taking into consideration neither the human rights violations nor its lack of effectiveness.

When coming to censoring the net the implications and elements amplifies and gets global. The activity and developments in the physical world have its own mirror image in the virtual. One is more dependent on digital technology that goes beyond the physical and personal space or needs. Internet censorship employs various methods such as blocking, filtering, tracking, surveillance, content grading, licensing policies, intermediary

[1] Rajeev Dhavan, *Publish and Be Damned Censorship and Intolerance in India* (Tulika Books 2020).

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed ( Group -I) Journal Volume 11, Iss 10, 2022

liabilities, government interventions and national law restrictions.[2] Most of these censoring are so inherent of internet access and embedded in networking that the general public is not even aware or conscious of it. Internet censorship is nor transparent neither in understandable norms as its always kept under the guise of confidentiality by the government which creates so many question marks regarding the concept of internet censorship itself.

## CENSORING CYBER CRIMES

One of the primary objectives promoted among its various initiatives of censorship in cyberspace is to control cyber-crime. Cyber-crimes are the progeny of cyber space and it flourishes in such environment.[3] Cyber-crime are called by many names like computer crime or internet crime and takes on many forms like cyber harassment or cyber bullying, cyber terrorism, identity theft, computer related offences, publication or transmission of sexually explicit act in electronic form, preservation and retention of information by intermediaries, cyber stalking, data theft, online financial fraud[4] etc. thereby computers and internet are instrumental to cyber-crime. And control and regulation of cyber crime is often interlinked to internet censorship and advocated as its most important objective wherein censorship takes on a positive shade despite its negativity.

However, majority of the public is even unaware of the fact that their everyday content, data and information are being censored which leads to people circumventing censorship without actually realising that they are breaking law. Especially youngsters they regard themselves as problem solvers and try to find solutions parallel to these circumventing techniques. On much complex and qualitative scale systems and techniques like tor, decoy routing, cache browser, domain fronting, DNS poisoning[5], meek and covert cast etc. are used to avoid being discovered.[6]

Even though censorship helps in regulating the cyber content to an extent when it comes to cyber-crimes its applicability weakens. From the statistics provided by National Crimes Record Bureau it can be clearly seen that cyber-crime has simply increased as the year goes by.[7]

---

[2]Jeffrey (Chien-Fei) Li*," Internet Control or Internet Censorship? Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan's Choice*," 14, 21-28(PLJ.12012) available at https://doi.org/10.5195/tlp.2013.131

[3]Donn B. Parker and d Susan H. Nycum, *Computer crime*, 27 313, 314-315 (Commun. ACM, 1984) available at https://doi.org/10.1145/358027.358770

[4] Information Technology Act, 2000, Acts of Parliament,2000 (India).

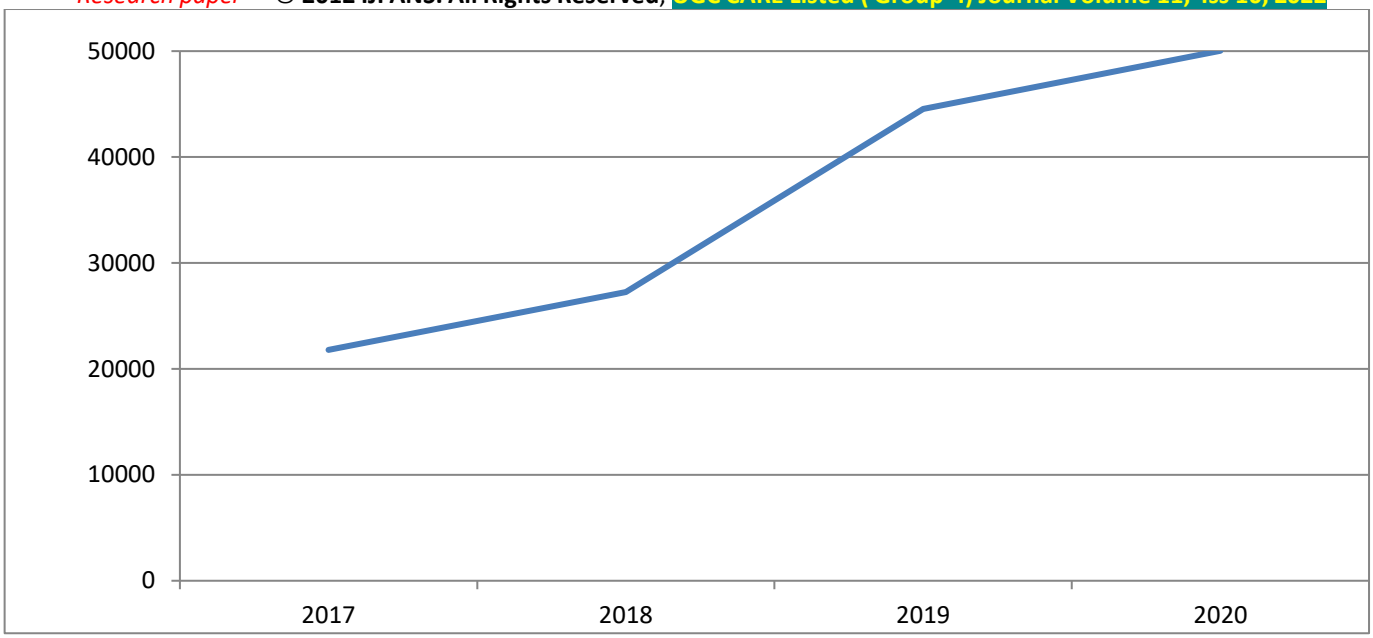
[5] Hacking vulnerabilities in a Domain Name System.

[6] Amir Houmansadr et.al., *The Parrot Is Dead: Observing Unobservable Network Communications*. 65-79. Conference: Security and Privacy (SP), IEEE Symposium (2013) DOI:10.1109/SP.2013.14; Richard McPherson et.al., *CovertCast: Using Live Streaming to Evade Internet Censorship*. Proceedings on Privacy Enhancing Technologies. (2016). DOI:10.1515/popets-2016-0024

[7] A total of 52,974 cases were registered under Cyber Crimes, showing an increase of 5.9% in registration over 2020 (50,035 cases). Crime rate under this category increased from 3.7 in 2020 to 3.9 in 2021: *Crime in India 2021*: Statistics Volume, National Crime Records Bureau (Ministry of Home Affairs)

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed ( Group -I) Journal Volume 11, Iss 10, 2022




***Content Regulation Versus Cyber Crime***

One of the most relatable factors with censorship are the criterions under which censorship is initiated in cyberspace. Now these grounds are not given under a particular law, national or international but one has to assume so after going through the available literature, case laws and combining the two prominent legislations Indian Penal Code and Information Technology Act 2000 along with its subsequent rules and guidelines. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provides a very detailed structure regarding duties of intermediaries and due diligence of intermediaries however it gives unnecessary autonomy to government and puts heavy pressure on intermediaries.[8] Despite different national policies and regulations, the most common grounds around the world and in India for censorship are child pornography, data protection and privacy, national security, copyright violation and defamation. Regardless, whether taken individually or taken together the grounds are more relatable to content regulation rather than cyber crimes when seen from the perspective of censorship.

***Child Pornography***

[8] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, section 3: Content that belongs to another person and to which the user does not have any right; is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force; is harmful to child; infringes any patent, trademark, copyright or other proprietary rights; violates any law for the time being in force; impersonates another person; threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource; is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person; cannot be hosted, displayed, uploaded, modified, published, transmitted, stored, updated or shared.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 10, 2022

Pornographic data, messages specifically child pornography has been the top most factor under world legislations for regulating content in cyberspace and prominent in keyword filtering used by intermediaries becoming an indivisible ground for censorship. In India the Information Technology Act 2000, Indian Penal Code 1860, Protection of Children from Sexual Offences Act, 2012 (POCSO) and National Cyber Security Policy, 2013 provides legal framework for prevention, investigation and prosecution of cybercrimes against children. Sexually explicit content is often filtered and blocked by ISP's[9] either directly applying its terms and conditions or by giving take down notices explicitly. And while most of the social media and online platforms engage in censorship to avoid government sanctions, most users do not notice the censorship or come across it until they come across such third-party hyperlinks or pop ups.[10]

In spite of these censorious guidelines even though content regulation in a normal viewable platform can be regulated as public forums are always strictly scrutinised however the offence of child pornography in the cyberspace has no sign of diminishing and is conversely at a rise with far reaching implications. Owing to the borderless nature of information technology such sexually explicit materials can be easily viewed, disseminated, circulated and accessed by any ordinary person without using any sort of circumventing technologies. Most of such viewing platforms are hosted outside India and implements anti tracking software's that not only blocks but also alters the network nodes to keep the host untraceable.

***National Security***

There is no clear definition or meaning of national security anywhere under Indian legislation however its often brought under the crime of sedition and has been long used as a political tool to subdue any political dissent that may spread through internet technology. Any sensitive concerns, comments or criticism or posts made regarding government are often removed or blocked and the individual is arrested under the guise of national integrity and protection. Most of these circumstances are often left to judicial interpretation that often results in the support of government action regarding the content regulation, however falls flat when taken under the shadow of sedition.[11] One of the mostly, evoked censoring grounds that has a post restraint principle rather than employing prior restraint often carters to the political regimes whim. From the serious offence of sedition to whether it has affected public order or is there incitement to violence or hatred[12] it becomes a purely executive action without any procedural constraint. Such action often leads to internet shutdown, network blackout on large scale often employed by government under the excuse of combating cyber terrorism without providing any reason or

[9] Internet Service Providers or intermediaries that provides internet and network connectivity.

[10] Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace (Ronald Deibert et.al. eds., 2010) DOI: https://doi.org/10.7551/mitpress/8551.001.0001

[11] Muzamil Butt v. State of Jammu and Kashmir, 2022 SCC OnLine J&K 272.; Disha A. Ravi v. State (Nct Of Delhi) & Ors., W.P.(C), 2297 Of 2021.

[12] Patricia Mukhim v. State of Meghalaya, 2021 SCC OnLine SC 258 : "The disapprobation of governmental inaction cannot be branded as an attempt to promote hatred".

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 10, 2022

adhering to time limit restrictions.[13]Most of these charges of seditions are made to stop the dissemination of information that puts the government in a negative shade and often used as a weapon to sooth the wounded vanity of political leaders which contravenes with the principles of democracy and right of a citizen to debate, dissent, disagree, question state policies or partake in peaceful protests online.

***Copyright Violation***

One another common ground for censorship in cyberspace and content regulation is copyright violation. Internet on one hand provides an ideal platform to artists, authors and performers to disseminate and promote their work quickly and efficiently and on another also becomes the stage where most of the copyright violation or infringement takes place as it becomes an easy medium where the original work can be edited, altered, distorted or redistribute without the copyright holders permission.[14]Digital technology can be used to make unlimited number of digital copies allowing copying to be done quickly, cheaply, easily, with no loss in quality, and then distributed to potentially millions of people in few seconds.[15]

With the wide spread use of internet and information technology offenders uses catching, proxy catching, linking, framing, uploading and downloading copyrighted material, RAM copying, digital formal licences, musical rights, meta search etc. on everyday basis which has become so part of the norm that it is getting disassociated with copyright violation despite its legal ramifications. Censorship becomes impossible when copying is done at such large scale and simultaneously. Indian law has inadequate circumvention technological measures and the rights management information to protect copyright on the Internet which needs proper ground support.

***Defamation***

Reputation of an individual is an inviable right that can't be separated from a person's dignity and repute which cannot and shouldn't be publicized as it infringes the right to privacy.[16] Debasing and ruining people are often censored in the cybersphere on individual complaints to government interventions. Most of the content regulations based on defamation are instances of celebrity or famous personnel who file complaints when their private spheres of activities are circulated on social media or related fake news is published on public forums. However most of these instances seldom grow into a cyber-offence and are generally buried under content removal, apology and monetary compensation.

***Data Protection and Right to Privacy***

[13] Anuradha Bhasin v. Union of India, WP (C) No. 1031/2019; Foundation for Media Professionals v. Union Territory of Jammu and Kashmir & Anr. WP (C) 10817 of 2020.
[14] Tom G Palmer, *Are Patents and Copyrights Morally Justified? The Philosophy of Property Rights and Ideal Objects*, 817, 819-865 (Harv. J.L. & Pub. Pol'y,1990) available at http://tomgpalmer.com/wp-content/uploads/papers/morallyjustified.pdf
[15] Neil Netanel, *Copyright and a Democratic Civil Society*, ., 283-287 (Yale L.J., 1996) DOI:10.2307/797212
[16] Information Technology Act, 2000 (Act 21 of 2000), s. 67; Indian Penal Code, 1860 (Act 45 of 1860), s. 499

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 10, 2022

One of the most important elements of cyberspace is data handling wherein the issue of data protection, confidentiality and privacy arises.[17] Data privacy or information privacy related to personal data is one of the basic rights of an individual.[18] Censorship of data entails two perspective; one where data is protected from unauthorized access or use, deletion of inadequate or inappropriate data, protects from cyber threats or data manipulation etc. here censoring is taken in a positive light as it can protect data and uphold the right to privacy by censoring unauthorized data on net. But on the other hand more worryingly it conflicts with the other tactics employed that is surveillance; monitoring and intrusive technology employed by state and non-state actors for ease of censorship. As stated, "In a democratic country governed by the rule of law, indiscriminate spying on individuals cannot be allowed except with sufficient statutory safeguards or by following the procedure established by law under the Constitution".[19]Without the element of consent, transparency and accountability protecting personal data in the public sphere of cyberspace is difficult and challenging.

## CONCLUSION

On a positive note, censorship set borders and rules about what can or cannot be expressed online and what does and doesn't belong to public sphere providing guidelines to public discourse in cyberspace. However, negatively censorship is not transparent and is shrouded in secrecy and blurred which causes the rampant violations actively or passively. Cyber crimes blooms in cyberspace as the options that internet technology provides are endless and most of the unauthorized acts are done knowingly or unknowingly which shows the lack of concern that offenders have towards censorship and cybercrimes. The following conclusions can be drawn:

- The more technical savvy an individual is they are more likely to use circumventing technology and engage in cybercrime.
- There is a misconception as to when majority does something it loses its legal implications for example downloading copyrighted data or using unlicensed software.
- No consent is obtained or procedure is made known or applied when censoring data both prior to commission of cybercrime and afterwards which contributes to the lack of awareness.
- Misuse of social media which is often encouraged by peers and as source of revenue generation often leads to adverse repercussions.
- The perception towards censorship itself is often disassociated with cyber crime as it is perceived that content is filtered and there is no criminality to be found.

[17] Information Technology Act,2000 (Act 21 of 2000), s. 72A If a person reveals personal information in violation of a contract or without the agreement of the affected party with the purpose to cause or knowledge that disclosure is likely to cause wrongful loss or wrongful gain, he is subject to criminal penalties

[18] Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., AIR 2017 SC 4161.

[19] Manohar v. Union of India, Writ Petition (Crim.) 314 of 2021: media organizations from around the world, including one Indian organisation revealed a list of some 50,000 mobile numbers which were allegedly infiltrated by Pegasus software and thus under surveillance by clients of the NSO Group. The case dealt with the allegations of unlawful surveillance, cyberattack and breach of privacy of Indian citizens.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 10, 2022

- Vulnerable groups like children often fall prey to cyber criminals due to sharing personal information or due to skipping cyber security procedures due to lack of knowledge.
- Internet shutdown, blocking websites and removal of data and content is done without any procedure that challenges accountability and diminishes transparency.

Censorship regulates content that comes under the cyber-crime aspects rather than controlling the crime as such. Passive and aggressive content filtering, internet blocking, web filtering, monitoring and tracking all cannot be optimised without solving the basic issues.

- Proper awareness and education must be inculcated among youngsters regarding cyber-crime, the deviousness of web, cyber security and content that falls within the ambit of censorship.
- Law relating to censorship and content regulation should be enacted supplementing Information Technology Act and a body should be constituted that decides on content regulation, censorship and the criminal aspects of it which can be frequently updated and enforced.
- Internet policies and regulations must be easily accessible and understandable to a layman without its technical jargons.
- Proper channel must be created to obtain consent and maintain confidentiality of personal information.
- Under the data processing activities in cyberspace privacy and data protection must be embedded as a default action point.
- Strict rules must be devised for state and non-state actors regarding censorship and content regulation and supporting bodies at regional levels must be constituted for private and public support in cyberspace. Censorship is an equal responsibility that has to be born by both government and intermediaries. Autonomy to government as provided under IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 will create discrimination and dissent which may later change into state surveillance.
- The governing bodies must be accountable on defaulting and strict compliance structure must be created for the system to be fair and lawful.

A balance has to be created between censorship and content regulation to fight cybercrime in the ever-changing world of cyberspace.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 10, 2022

## BIBLIOGRAPHY

Comer, Douglas E. *The Internet*, CRC Press, 2019.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan L. Zittrain. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT Press, 2010.

Dhavan Rajeev, *Publish and Be Damned Censorship and Intolerance in India*. Tulika Books, 2020.

Grewlich, Klaus W. *Governance in Cyberspace: Access and Public Interest in Global Communications*, Kluwer Law International, 1999

G Palmer, Tom. *Are Patents and Copyrights Morally Justified? The Philosophy of Property Rights and Ideal Objects*, Harvard Journal of Law & Public Polity,1990, http://tomgpalmer.com/wp-content/uploads/papers/morallyjustified.pdf

Houmansadr., Amir, Chad Brubaker and Vitaly Shmatikov. *The Parrot Is Dead: Observing Unobservable Network Communications*. Conference: Security and Privacy, IEEE,2013, DOI:10.1109/SP.2013.14

Li,Jeffrey (Chien-Fei), *Internet Control or Internet Censorship? Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan's Choice*, 2012, https://doi.org/10.5195/tlp.2013.131

McPherson, Richard, Amir Houmansadr, and Shmatikov, Vitaly. *CovertCast: Using Live Streaming to Evade Internet Censorship. Proceedings on Privacy Enhancing Technologies*., 2016.DOI:10.1515/popets-2016-0024

Netanel, Neil, *Copyright and a Democratic Civil Society*, Yale Law Journal, 1996, DOI:10.2307/797212

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed ( Group -I) Journal Volume 11, Iss 10, 2022

Parker, Donn B. and Susan H. Nycum, *Computer crime*, Communications of the ACM, 1984, https://doi.org/10.1145/358027.358770

Sharma, Vakul. *Handbook of Cyber Law*, MacMillan India, 2002.

Warf, Barney. *Geographies of global Internet censorship*, Geo Journal, 2011.

**INDIAN CASES**

Anuradha Bhasin v. Union of India, WP (C) No. 1031/2019

Disha A. Ravi v. State (Nct Of Delhi) & Ors., W.P.(C), 2297 Of 2021.

Foundation for Media Professionals v. Union Territory of Jammu and Kashmir & Anr. WP (C) 10817 of 2020

Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., AIR 2017 SC 4161

Manohar v. Union of India, Writ Petition (Crim.) 314 of 2021

Muzamil Butt v. State of Jammu and Kashmir, 2022 SCC OnLine J&K 272

Patricia Mukhim v. State of Meghalaya, 2021 SCC OnLine SC 258

**INDIAN LAWS**

Indian Penal Code, 1860

Information Technology Act, 2000

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,