Virtual Confinement: Internet Restraints as a Form of State Punitive Action in India

Kailashika Verma
LL.M. (Cyber Law and Cyber Crime Investigation)- Final year
National Forensic Sciences University, Bhubaneswar, Odisha

Abstract- The contemporary scene of cyber-crimes growing statistically higher than ever and newer forms thereof arising each day, the cyber-legal regime demands for modern-day equipped legal action backed by legislative sanction. Despite the increase in instances of cyber and related offences, the rates of conviction are seemingly low. Further, the rising rates of offences also point towards the lack of deterrence in society against cyber-offenders.

This article is built around the premise that lack of evidence-based convictions, societal deterrence and punitive actions and challenges in establishing virtual liability are key- factors contributing towards the ever-increasing cyber-crimes, and hence must be dealt with. It proposes a design to introduce internet restraints, bans and confinements as a form of legitimate state punitive action and further discusses the manner and kinds of offences where the proposed punishment may be prescribed while also suggesting a mechanism of implementation in order to increase cyber-liability, punitive effects and societal deterrence. The aim is also to critically examine the constitutional interpretation of internet access as a right under Article 19 and 21, arguing for legislative reforms that recognize proportional internet restraint as a legitimate state action.

Key words: virtual confinement, internet restraints, cyber-crime, internet access.

> *"It is the obligation of the state to strengthen its cyber law and effective legal frameworks are absolutely essential. There is a need for international bondage which shall have singular aim to preserve cyber security. There is need for developing the requisite jurisprudential principles concerning cyber law."*
>
> *-Justice Dipak Misra,*
>
> *Address at the International Conference on Cyberlaw, Cybercrime and Cybersecurity, New Delhi (Nov. 15, 2016).*

I.INTRODUCTION

The digital age has arrived and ever-evolving; and with the digitalization of crimes and courts, as well as governance, digital punishments has become the need of the hour. The unprecedented rise in the number of cyber and related offences clearly exposes a lacuna in the existing legal framework and hence calls for a change to tackle undeterred malicious presences online. From spamming, cyberstalking and financial frauds, to a surge of falsified digital material, the landscape of cybercrimes encompasses a wide spectrum and in pursuance of these are a large number of perpetrators who have a tendency towards habitual repetition.

The responsibility of vigilance and care cannot be blindly imposed on public who eventually fall victim to cybercrimes and related offences; especially in a welfare state where the safety of public is the duty of the state, along with the prevention and due as well as befitting punishment of offences. In order to punish and deterrently curb cybercrimes, it is hence proposed to introduce "virtual confinement" and "internet arrest" as state imposed digital restrictions as novel forms of punishments for cyber offenders wherein their virtual/internet presence is suspended or where they may be deprived of 'access to internet'. The restriction can serve both, preventive as well as punitive purpose; further, upon its penal application, it could be imposed independently or supplemental to other punishments such as fines or incarceration. It is essentially proposing a paradigm shift—treating internet access like movement (incarceration) or property (fines)—as something the state can legitimately restrict.

The underlying thesis is: current punishments fail to deter cyber-crime because they lack specificity and immediacy to the offense's nature; internet

restrictions would be symbolically and functionally more effective.

II.THE NEED FOR A REFORM IN CYBER-JUSTICE SYSTEM

There has been a significant surge of cybercrimes across the nation signalling towards the radical digitalisation of mens rea manifesting into a broad spectrum and affecting all and everything connected to the internet including masses as well as governmental infrastructure. As per the National Crime Records Bureau (NCRB) data, cybercrimes in India have grown statistically higher than ever, increasing 63.14% from 52,974 cases in 2021 to 86,420 cases in 2023[1] (NCRB data) while conviction rates for cyber-crimes remain low at around 1.6% for cases registered between 2020-2022.[2] The Indian Cyber Crime Coordination Center (I4C) had also compiled a report wherein it recorded losses of about 19,813 crores in 2025 signaling towards a worrying surge in financial crimes such as investment traps, digital arrest, online scams and banking frauds.

The heavy rise can be factually attributed to the lack of cyber-liability and further challenges to identifying the bearer of such liability. This in turn results into lower conviction rates and hence lack of fear of punishment and hence, it could be inferred that most cyber-offences are without consequence to the offender. It cannot be contended that effective punishment acts not only as a form of retribution but also as a deliberate mechanism to deter crime by ensuring certainty of consequences, and hence, deterring habitual offenders and strengthening social order.

With regard to cybercrimes wherein an individual is a victim of spamming, stalking, or financial and e-commerce fraud, as well as where the offense is against the public at large such as promulgation of misinformation, obscenity, pornography etc, restricting the source of it would serve as not only a protection to masses but also as a method to prevent recidivism.

III.EXAMINATION OF VIRTUAL CONFINEMENT THROUGH JURISPRUDENTIAL LENS

In present era, the access to internet can be unambiguously attributed to one's leisure of life and liberty; it has become an indispensable part of one's routine through serving as medium of entertainment and social activity, economic and financial services, political awareness and participation and hence the exercise of fundamental rights. Placing a restriction on internet presence, therefore, touches the core of what may be referred to as a person's *'digital liberty'*- the bundle of freedoms that are available to one through internet access.

The proposal to introduce virtual confinement as a penal measure requires examination under two broad perceptions: first, in the light of classical and contemporary theories of punishments and, second, against constitutional and juridical limits that provide and protect liberty and expression. Hence, to imbibe statutory restriction on an individual's access to internet and internet presence for the purpose of prevention or punishment of cyber-and-related-offences, it is imperative to firstly evaluate the jurisprudential effect and alignment of this newer form of punishment with principles of penology and, secondly, to critically formulate it into the contemporary criminal justice system in India in a way that conforms with constitutional standards, judicial scrutiny and principles of legality, necessity and proportionality.

The punitive and deterrent theory of punishment is based on the premises that punishment is justified by its ability to reduce recidivism as well as causes general discouragement to public from committing such offences by making them appear as an apparent ill-deal through implementing and instilling a fear of penal action. In context to cyber offences, virtual confinement targets the offender's digital presence, the very medium intended to be used for

[1] TOI Business Desk, *India's Cyber Fraud Epidemic: Rs 22,845 Crore Lost in 2024; 206% Jump from Previous Year, Says Government*, TIMES OF INDIA (July 22, 2025, 9:24 PM IST), https://timesofindia.indiatimes.com/business/cybersecurity/indias-cyber-fraud-epidemic-rs-22845-crore-lost-in-just-a-year-206-jump-from-previous-year-says-government/articleshow/122840099.cms.

[2] Only 1.6% Conviction Rate in 2 Yrs Amid Surge in Cybercrime Cases, THE TRIBUNE (Jan. 27, 2026, 10:15 AM IST), https://www.tribuneindia.com/news/india/only-1-6-conviction-rate-in-2-yrs-amid-surge-in-cybercrime-cases-2.

commission. It will lead to a form of extramural incapacitation of mens rea as it seeks to disable the offender's digital tools rather than place him under actual physical confinement. Additionally, punishment also communicates social condemnation, as an integral part and in modern scenario, the removal of one from access to social and public platforms/ networks carries symbolic weight akin to banishment. Hence for serious, repeat cyber offenders who depend on online platforms for victim contact or coordination, removal from digital platforms and spaces can operate as an effective manner of preventing further instances and punishing the wrong-doer.

IV.JUDICIAL AND REGULATORY FOUNDATIONS FOR VIRTUAL CONFINEMENT AS A STATE-IMPOSED DIGITAL SANCTION IN INDIA

The Supreme Court's decision in Anuradha Bhasin v. Union of India[3] serves as a reference point for discussions on right to access to internet and limitations thereof. The court in this matter had given recognition to internet access as a right integrally connected with the exercise of fundamental rights under Article 19(1)(a) and 19(1)(g) of the Constitution of India. However, on being affiliated with Article 19, the right to internet automatically becomes 'not absolute' and hence subject to reasonable restrictions. Further, the test of legality, necessity, proportionality, and procedural safeguards as laid down in a previous judgment of Supreme Court in the case of K.S. Puttaswamy v. Union of India[4]. The apex court further refined this understanding in the judgment delivered in the case of Foundation for Media Professionals v. Union Territory of Jammu and Kashmir[5], reiterating that while indefinite or opaque restrictions on digital liberty violate constitutional guarantees, the power of state to impose such restrictions cannot be held as impossible; emphasizing on structured decision-making, judicial review, and administrative accountability. Thus, it is unarguably established that digital liberty is constitutionally protected but it is not non-derogable and may be curtailed through *procedure established by law*.

When the regime of legislative and state policy in India is to be examined regarding cyber-criminal justice, the core and central position is occupied by the Information Technology Act, 2000[6] and rules made thereunder. Section 69, 69A and 69B of the act permits extensive executive control over digital spaces by authorizing interception, blocking and monitoring of digital information. The regulatory framework for digital restraint is more visible under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[7] and its interpretation in consonance with its parent act articulates a clear position that digital platforms are no longer neutral conduits but regulated spaces subject to state supervision and jurisdictional control. Thus, while a strict categorisation of internet restrictions as punishment does not exist under the country's justice system, authorised content takedowns, account suspensions, access blocking, traceability requirements, and cooperation with law-enforcement agencies is not alien to Indian legal landscape. However, the provisions are preventive and regulatory, to be exercised by the executive wing or "intermediaries' and not a judicially pronounceable punishments, it still forms a premise for the possibility of introducing virtual confinement as a statutory penalization. A noteworthy feature about contemporary scenario is that the government, through the IT Rules [8], has pushed most of enforcement and compliance down to platforms/intermediaries and Significant Social Media Intermediaries by obligating them to:

- take down or disable access to content upon official notification,
- facilitating traceability of users and originators,
- mandatorily maintain internal grievance and compliance systems that align with State demands,

In this manner, this enforcement model equips the state to maintain order across the digital space without direct legislation, making intermediaries an

[3] Anuradha Bhasin vs Union of India (2020) 3 SCC 637
[4] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1
[5] Foundation for Media Professionals v. Union of India (2020) SCC Online SC 25
[6] Information Technology Act, 2000 (No. 21 of 2000)
[7] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[8] Supra

essential vector of digital restrictions and accountability in India. while it is somewhat practicable, a more constitutionally sound approach would be to vest the power to impose internet-based restraints directly in judicial institutions, rather than shifting this responsibility onto intermediaries. Digital platforms are not law-enforcement bodies, nor are they institutions tasked with administering justice. Expecting them to decide when and how digital freedoms should be curtailed risks arbitrariness and lack of accountability. If internet restrictions are to function as a form of punishment or restraint, they must flow from judicial reasoning, backed by due process and constitutional safeguards.

Another recent policy inculcation in India, still on rolling basis, is being introduced through a telecom-feature under the directions of Telecom Regulatory Authority of India (TRAI) and Department of Telecommunications (DoT). The feature is being called as Calling Name Presentation (CNAP) and its function is to battle anonymity of calls that facilitate identity thefts and related frauds. On being called by an unknown number, the user will automatically and in real time be presented with the name of the person in who's name SIM KYR/registration has been furnished. This policy measure seeks to keenly identify presence over mobile networks, encouraging identification and hence ensuring accountability.

4.1 Recent Trends in Court-Imposed Virtual Restraint and Confinement

With a rise in cyber and internet related offences, courts are becoming increasingly aware that contemporary harm, mobilisation, and illegality often unfold not in physical spaces but virtual and digital ones. This awareness is manifesting in a jurisprudential shift in conceptualising restraint, punishment, and prevention of crime in the present era of digitally-mediated society; where restraint is no longer confined to bodily custody or territorial limits but extends into the digital sphere. This very shift may be described as an early form of court-imposed digital confinement.

The hon'ble Delhi High Court, in the case of Dabur India Ltd. v. Ashok Kumar & Ors.[9] Was confronted with the persistent inadequacy of traditional remedies in tackling online fraud, particularly where wrongdoers exploit anonymity, rapid domain re-registration, and the fragmented nature of digital infrastructure. Although rendered in the context of trademark infringement and online fraud, the judgment is doctrinally significant far beyond intellectual property law. It was duly observed that individual identification and prosecution often lag the pace of digital misconduct and hence, the Court adopted a more structural approach. It authorised domain takedowns, IP-level blocking, restrictions on re-registration of infringing domains, and mandatory identity verification through e-KYC mechanisms. The court expressly gave recognition to the systematisation of digital harm, enabled by anonymity, rapid domain churn, and infrastructural opacity and laid down valuable directions including mandate of e-KYC verification and periodic re-verification for the purpose of domain registration will battle anonymity and ensure accountability and elimination of "privacy by default' by requiring disclosure of details by domain name registrars. It further directed banks to activate the "Beneficiary Bank Account Name Lookup" facility, allowing users to verify recipient identity before online payments.

The judgment has made a courageous endeavour into the realm of digital anonymity being practiced in the name of privacy while recognising infrastructural lacunas causing mass vulnerability.

A more individual-level digital restraint was observed in Supreme's court decision in Gulfisha Fatima v. State (NCT of Delhi)[10] while granting bail under the Unlawful Activities (Prevention) Act, whereby, stringent conditions that go well beyond territorial or custodial controls were imposed. The accused on bail have been prohibited from attending rallies or public meetings and on circulating posters, banners, or any other material in any form, whether physical or virtual. Without explicitly theorising the issue, the Court accepted that liberty can be meaningfully curtailed through restrictions on speech, visibility, and participation in digital forums. In effect, the accused were released from physical custody while remaining confined within carefully drawn digital boundaries.

[9]Arising in CS (COMM) 135/2022 & I.As. 3423/2022, 1221/2023 & 8858/2025; December 24th, 2025

[10] Arising in SLP (CRL.) NO. 13988/2025; January 5th, 2026

When read together, these two judgments reveal a common judicial intuition: digital space has become too central to social and political life to be ignored in the architecture of restraint. The Delhi High Court's approach operates at the level of infrastructure, disabling the systems that sustain unlawful online activity. The Supreme Court's intervention operates at the level of the individual, restricting digital expression and engagement as a condition of liberty. The common ground between both is the willingness on the part of courts to move beyond reliance on intermediaries or executive action for securing digital spaces and to exercise direct judicial control over digital access and limitations to such access.

V.IMPLEMENTATIONAL AND INFRASTRUCTURAL CHALLENGES IN OPERATIONALISING VIRTUAL CONFINEMENT

While the idea of virtual confinement offers a promising penal action for addressing digital harm through lawful restraint, its practical application raises certain implementational and infrastructural concerns. The digital space has no boundaries and jurisdictional challenges are hefty. Unlike traditional physical confinements executed through state machinery like prisons and jails, the imposition of digital restraint would have to be carried out in the digital ecosystem, largely managed by private actors and entities such as internet service providers, social media platforms, domain registrars, hosting and streaming platforms, e-banking infrastructure, etc. therefore, a coordination amongst all such parties would be required to implement virtual restraint and confinement.

Another challenge relates to technological adaptability and its ever-evolving nature. Blocking, deleting, restricting or tracing the usage of internet in an era where anonymity is so easy to attain is a difficult task. Technical solutions for effective but proportionate restriction over digital spaces will be required. These challenges, hence do not negate the functionality and practicability of digital restrictions and virtual confinement as a form of statutory punishment; rather, they highlight the care and measures with which provisions must be designed.

VI.CONCLUSION

The digitalization of mens rea as well as nature and scene of crime and the spike in such occurrences cannot be dealt in traditional penal manners. This paper demonstrates that virtual restraint and confinement are no longer speculations within Indian legal system and there already exists legislative and policy framework as well as instances of judicial application. However, the formalization of the same in the form of a statutorily regulated punishment is yet to be made.

If internet restrictions are to function as a form of state-imposed penal action as well as cause deterrence, they must originate from judicial reasoning, be guided by constitutional safeguards, and remain subject to review. Legislative engagement in this area would not only clarify the scope and limits of virtual confinement but would also ensure that emerging digital penalties are applied transparently, proportionately, and in a manner consistent with the rule of law.