YOUTH AND ONLINE RADICALIZATION: LAW, SOCIETY, DIGITAL PLATFORMS, AND LEGAL FRAMEWORKS IN THE CONTEMPORARY ERA

V. Iswariyalakshmi*

ABSTRACT

In December 2025, a shocking incident happened in Chennai when four minors attacked a migrant worker, K. Suraj, on a suburban train and recorded the assault to upload it on social media. This incident spread nationwide outrage and highlighted how unsupervised online platforms can influence youth behaviour, normalising violent acts for digital attention. The case demonstrates how online exposure, peer validation, and social media virality can contribute to youth radicalisation in both ideological and behavioural forms. This article explores the socio-legal dimensions of youth radicalization examines relevant Indian laws and constitutional provisions, discusses key judicial decisions, and proposes strategies for prevention and addressing the root causes of youth vulnerability and promoting positive digital engagement, which are key to safeguarding society and nurturing a digital generation. By situating online radicalisation within a broader socio-legal context, this paper argues that effective prevention requires not only punitive laws but also rights- based, youth-centric, and technology – responsive strategies. Ultimately, the study underscores that combating youth online radicalisation is as much a societal responsibility as it is a legal imperative in contemporary society. This K. Suraj issue affected me, so I decided to write an article about youth and online radicalisation.

Keywords: Youth Radicalisation, Peer Validation, Suraj Incident, Four Juveniles, Judicial Decisions.

*BA LLB, THIRD YEAR, GOVERNMENT LAW COLLEGE, RAMANATHAPURAM.

INTRODUCTION

The internet has become one of the most powerful influences on young minds in contemporary society. What once served as a space for learning and connection has gradually evolved into a platform where violence, extremism, and reckless behaviour can gain instant visibility. Young people, driven by curiosity, peer approval, and the desire for recognition, often find themselves influenced by content that blurs the line between entertainment and harm. In recent times, incidents involving juveniles committing violent acts for online attention have raised serious concerns about the role of digital platforms in shaping youth behaviour. Youth radicalisation today extends beyond traditional notions of extremism. It increasingly includes behavioural radicalisation, where violent or antisocial acts are performed to gain digital attention and social acceptance. This shift presents new challenges for law and society, requiring a balanced approach that addresses both accountability and reform. Against this backdrop, the present article examines the relationship between youth, online radicalisation, and the legal framework in India, while also exploring preventive measures necessary to safeguard young minds and social harmony. Online radicalisation is not always ideological; it can involve adopting extreme behaviours promoted online for peer approval. such phenomena intersect with law, psychology, digital culture, and public policy, requiring a multi-faced socio-legal response.

YOUTH VULNERABILITY AND THE NATURE OF ONLINE RADICALIZATION

Youth vulnerability to online radicalisation arises from a complex interaction of psychological development, social circumstances and digital environments. Unlike traditional forms of radicalisation, online radicalisation often operates subtly, embedding extremist ideas within everyday online interactions. Understanding why young individuals are particularly susceptible is essential for effective prevention.

Psychological Vulnerability: Young people often experience emotional uncertainty, identity confusion, and a need for recognition. These factors make them receptive to extremist narratives that promise purpose, pride and belonging. When young individuals encounter extremist content that validates their grievances, it can create a strong emotional attachment to radical ideas.

Role of Social Media Algorithms: Digital platforms promote emotionally charged content. Repeated exposure to similar viewpoints creates echo chambers where extreme ideas appear normal and justified. Digital platforms play a significant role in shaping youth exposure to

radical content. For young users lacking media literacy, repeated exposure can blur the line between opinion, propaganda, and fact.

Lack of Digital and Critical: Limited ability to assess online information increases vulnerability. Propaganda, misinformation and emotional narratives are often mistaken for facts. Many young users struggle to distinguish credible information from misinformation or propaganda.

Gradual Nature of Radicalisation: Online radicalisation develops slowly, often beginning with harmless content and progressing to extreme views. This makes early detection difficult. Memes, short videos, and emotionally persuasive content are commonly used to simplify complex political or social issues and responses.

Peer Validation: Peer validation plays a powerful role in youth radicalisation. When extremist views are rewarded with likes, shares, or approval within online groups, young individuals begin to associate acceptance with radical behaviour. This validation reinforces extreme beliefs, discourages self-reflection, and creates pressure to conform to group ideology.[1]

LEGAL AND CONSTITUTIONAL FRAMEWORKS

The challenge of youth radicalisation, particularly through online platforms, is addressed through a strong combination of constitutional safeguards and statutory laws. The legal framework seeks to balance national security with the protection of individual rights, especially freedom of expression.

Constitutional Framework: The Constitution of India provides the foundation for regulating online radicalisation while safeguarding the welfare of the people.

Article 19 (1) (a): It guarantees freedom of speech and expression. This right allows individuals, including youth, to express opinions online and participate in digital discourse. However, this freedom is not absolute.

[1] '4 Juveniles Film attack for social media 'The times of India (Chennai, 29 December 2025) https://timesofindia.indiatimes.com/city/chennai/4-juveniles-flim-attack-for-social-media/articleshow/126277680.cms> accessed on 6th January 2025.

Article 19 (2): Under Article 19 (2), the state may impose reasonable restrictions in the interest of sovereignty, integrity of India, public order, and security of the state. Any content that promotes violence can be lawfully restricted.[2]

Article 21: Article 21, which guarantees the right to life and personal liberty, and protects[3] freedom and right of citizens. So, the constitutional framework and collective security require a careful and proportionate approach to regulation.

STATUTORY LEGAL FRAMEWORK

Several laws address online youth radicalisation and related activities, such as:

The Information Technology Act, 2000: The Information Technology Act 2000 regulates online conduct. It empowers the government to take action against digital content that threatens national security or public order and places responsibility on online intermediaries to prevent misuse of their platforms.

Section 66 F: Cyber Terrorism: It deals with Cyber terrorism and applies when digital platforms are used to threaten national security, unity, or sovereignty. So online radicalisation that encourages violent acts may fall within this provision.

Section 69 A: Power to Block Online Content: It empowers the government to block public access to online content in the interest of national security, public order, or sovereignty. This provision is frequently used to restrict websites and social media accounts.

Section 79: Intermediary Liability: It provides conditional protection to intermediaries such as social media platforms, messaging services, etc. And to enjoy this protection, platforms must follow due diligence requirements and remove unlawful content when notified.

Unlawful Activities (Prevention) Act, 1967: The Unlawful Activities (Prevention) Act, 1967 (UAPA), aims to prevent activities that threaten the sovereignty, integrity, and security of the nation. This act doesn't directly mention online radicalisation, but it prevents unlawful activities.

[2] Constitution of india,1950, art (19)(1)(a),19(2),21.
[3] Information technology act ,2000, sec 66F,69A,79.
[4] Unlawful activities (prevention) at, 1967 sec 2(o),13

Section 2 (o): Unlawful activities: This section defines "unlawful activity" as any action, whether by words, signs or representation, that promotes violence and creates public disorder.

Section 13: Punishment for Unlawful Activities: In this Section, 13 clearly mentions that punishment for individuals who take part in or support unlawful activities. The punishment for imprisonment is 7(seven) years, and the offender shall also be liable to a fine.[4]

BHARATIYA NYAYA SANHITA, 2023 (BNS)

Section 109: Attempt to Murder: This section deals with attempts to commit murder. It applies when a person intentionally performs an act with the knowledge or intention that, if it caused death, would amount to murder, but the death does not occur. Imprisonment, which may extend to ten years, and a fine.

Section 111: Organised Crime: This section deals with organised criminal activity carried out by a group acting in a structured and continuing manner for unlawful purposes, including activities conducted through digital or cyber networks.

Section 115: Voluntarily Causing Hurt: This provision deals with intentionally causing bodily pain, disease, or infirmity to another person. It applies when physical harm is inflicted, irrespective of the motive behind the act. Imprisonment may extend to one year, or with fines which may extend to ten thousand rupees.

Section 130: Assault: This provision deals with assault, which means intentionally threatening or attempting to use criminal force against another person, causing fear of immediate harm.

Section 131: Punishment for Assault or Criminal Force Otherwise than on Grave Provocation: This provision provides the punishment for the offence of assault. It states that whoever commits assault shall be punished with simple imprisonment, which may extend to three months, or with a fine, or with both.

[5] Bharatiya Nyaya sanhita,2023 sec 109,111,115,130.

BHARATIYA SAKSHYA ADHINIYAM, 2023 (BSA)

Section 61: Electronic or Digital Record: This provision provides electronic records such as videos, CCTV footage, mobile recordings, social media posts, and message call data as legal evidence.

Section 62: Special Provisions as to Evidence Relating to Electronic Record: Content of electronic records. This section links section 61 to section 63, clarifying that the content of electronic records must be proved in accordance with the conditions laid down in section 63.

Section 63: Admissibility of Electronic Records: This provision states that electronic records are admissible as evidence in court. digital material such as videos, messages, emails, and CCTV footage can be relied upon if produced according to legal requirements. The focus is on the authenticity and reliability of the source.

Juvenile Justice (Care and Protection of Children) Acts, 2015: Juvenile Justice (Care and Protection of Children) Acts, 2015 is a central legislation enacted to provide Care, protection, rehabilitation, and social reintegration of children who are either in conflict with the law or in need of care and protection. The act replaced the juvenile justice act of 2000, introducing a more balanced approach between reformative justice and accountability.

Section 15: This section allows the juvenile justice board to conduct a preliminary assessment of children aged 16-18 years accused of a heinous offence to determine their mental and physical capacity, ability to understand the consequences and circumstances of the assessment. Based on this assessment, juveniles may be tried as adults.[5]

LANDMARK CASE LAW FOR ONLINE YOUTH RADICALIZATION

Arsalan Feroze Ahenger vs National Investigation Agency (2025: DHC:5522-DB): In this case, Ahenger was accused of actively sharing extremist material on platforms like Facebook, WhatsApp, Telegram, Instagram, Twitter and creating online groups to spread radical content linked to outlawed outfits such as The Resistance Front. The national investigation agency (NIA) charged him under various UAPA provisions, including section 17,18,18B,38 and 39 –

[6] Bharatiya Nyaya Sanhita, 2023, sec 61,62,63.
[7] Juvenile justice (care and protection of children) Act, sec 15.

covering funding, conspiracy, recruitment organization along with offence under the BSA (Bharatiya Sakshaya Adhiniyam) 2023.

Judgement: A division bench of justice Subramaniam Prasad, Harish Vaidyanathan Shankar held that section 18 of the UAPA **(**Unlawful Activities Prevention Act 1967), which deals with punishment for conspiracy, abetment, incitement and terrorist acts, is broad enough to cover online activities. The court observed that the act does not require a physical act of terrorism; digital dissemination of radical information and ideology with the intent to promote or incite extremist conduct falls within its ambit. Based on prima facie material indicating that Ahenger used social media to incite and radicalise youth, the court held the refusal of bail under the Unlawful Activities Prevention Act (UAPA Unlawful Activities Prevention Act 1967).

State of Tamil Nadu v. Juvenile accused (Suraj Assault Case) 2025: Famously known as the Suraj case (Chennai suburban train assault). The case is very important. In this case, K. Suraj, a migrant worker, was assaulted by a group of juveniles inside a Chennai suburban train. The attack was allegedly recorded on a mobile, reportedly for circulation on social media, which brought public attention to the growing influence of digital validation and online trends on youth violence. The accused being juveniles, proceedings were initiated under the Juvenile Justice (Care and Protection of Children) Act 2015, along with relevant provisions of the BNS (Bharatiya Nyaya Sanhita) 2023. The case is pending before the juvenile justice board, and no final judgment has been delivered. This case is a great example of youth online radicalisation.

NIA (National Investigation Agency vs. Jameesha Mubin (2022): Famously known as the Coimbatore car bomb blast case. The Coimbatore car bomb blast is related to a suicide bomb explosion that occurred on 23 October 2022 near the Kottai Eswaran temple, Coimbatore. The deceased Jamesh Mubin was identified as the suicide bomber. Investigation by the National Investigation Agency (NIA) revealed that he and his associates were radicalised through online platforms, including Telegram and WhatsApp, and were influenced by ISIS ideology and extremist digital propaganda. The accused were charged under the Unlawful Activities (Prevention) Act 1967, along with provisions of the BNS (Bharatiya Nyaya Sanhita)2023 and the Explosive Substances Act 1908.

Twitter, Inc. v. Taamneh 598 U.S. 471 (2023): In Twitter, Ing v. Taamneh, the U.S. Supreme Court examined whether social media companies can be held legally responsible for terrorist attacks because extremist organisations used their platforms. The was filled by the family of a

victim killed in a 2017 ISIS (Islamic State of Iraq and Syria) terrorist attack at a nightclub in Istanbul. The plaintiff argued that Twitter, Google, and Facebook violated the antiterrorism ats, 18 U.S.C. Sec 2333, by allowing ISIS to use their platforms to spread propaganda, recruit followers, and radicalise users online. The main legal issue was whether providing general social media services could amount to "aiding and abetting "terrorism. The Supreme Court unanimously ruled in favour of Twitter. The court held that simply hosting content, failing to remove all extremist material, or using neutral recommendation algorithms does not meet the legal standard for aiding and abetting terrorism.

The court explained that liability under the Antiterrorism Act requires knowing, intentional, and substantial assistance to a specific terrorist act. In this case, there was no proof that Twitter directly supported or helped plan the attack. The connection between the platform's services and the terrorist act was too indirect. This judgment is important in the discussion on online radicalisation, as it limits the legal responsibility of social media platforms while highlighting the need for clear evidence of intentional support for extremist violence.

Shreya Singhal vs Union of India AIR 2015 SC 1523;(2015) 5 SCC 1: In this case, the Supreme Court struck down Section 66A of the Information Technology Act, 2000, for violating freedom of speech. The court held that online expression can only be restricted when it amounts to incitement or threatens public order, which is crucial when assessing online radical content involving youth. All the above cases highlight the changing pattern of youth crime in the digital age and underscore the need for preventive legal measures, digital literacy, and effective juvenile rehabilitation mechanisms.[6]

PREVENTIVE STRATEGIES

Prevention of online radicalisation begins not with punishment, but with understanding, guidance, and timely support that helps young people question extremist ideas before they take root. And the following ways to prevent and De – Radicalization strategies.

[8] Arsalan Feroze Ahenger v National Investigation Agency [2025] DH 5522 (DB).
[9] State of Tamil Nadu v Juvenile accused (Chennai suburban train assault) (Madras HC, pending).
[10] National Investigation Agency v Jameesha Mubin (special NIA court, pending).
[11] Twitter, Ing v Taamneh 598 US 471 [2023].
[12] Shreya Singhal v Union of India AIR 2015 SC 1523; [2015] 5 SCC 1.

PREVENTION AND DE-RADICALIZATION STRATEGIES

Education and Digital Literacy: Education remains the most effective preventive tool. Digital literacy programs must equip youth with the ability to critically assess online content, identify propaganda, and resist emotionally critical thinking, which reduces passive consumption of extremist material.

Community and Family Engagement: Families and community institutions play a vital role in early intervention. Open dialogue, emotional support, and mentorship can prevent young individuals from seeking validation in extremist spaces. Community – based counseling and rehabilitation programs have proven effective in de-radicalisation efforts.

Role of Technology Platforms: Social media companies must acknowledge their responsibility in curbing extremist content. Transparent moderation policies, ethical algorithm design, and cooperation with legal authorities are essential. At the same time, content regulation must respect freedom of expression to avoid alienating users and communities.

Family and Community Engagement: Open communication within families and emotional security. A strong support system reduces the likelihood of youth seeking validation in extremist spaces. Where families create safe spaces for discussion, young individuals are less likely to seek validation from harmful online groups.

Legal and policy measures: Promote legal and policy laws. Clear laws addressing online extremism, combined with fair enforcement and judicial oversight, help maintain security without infringing fundamental rights.

School and University – Based Awareness: Education institutions should introduce counselling services, peer-support programs, and awareness workshops. Safe spaces for dialogue on identity, grievances, and social justice prevent youth from seeking validation in extremist online forums. Safeguarding the younger generation**.**

CONCLUSION

Online radicalisation of youth challenges the very foundation of public order, constitutional morality, and the rule of law. The state's duty is not limited to prosecution after harm occurs, but extends to prevention, accountability of digital platforms, and protection of vulnerable minds. law must function not only as a punitive instrument, but as a safeguard against the

misuse of cyberspace for violence and hatred. A rights-based, reformative, and technologically responsive legal framework is essential to ensure that digital spaces do not become breeding grounds for extremists. Especially the Suraj Case has created a huge impact on me about youth online radicalization it reflects the dangerous convergence of online provocation, peer validation, and juvenile violence in contemporary India.

Youth radicalisation is not only a law-and-order issue; it is a failure of guidance, digital responsibility and timely intervention, accountability of platforms, active parental and institutional supervision, and a strong legal system that balances security with rehabilitation. In my point of view If society ignores what happened on the child screen today, it will have consequences in its huge impact on tomorrow. Protecting youth online is not censorship – it is prevention, areas and the preservation of humanity itself. My suggestion about youth online radicalisation is that protecting young minds online is not a matter of restriction, but a constitutional obligation to secure a safer, just and human future.