WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

LEGAL AND TECHNOLOGICAL SAFEGUARDS FOR PROTECTING CHILDREN'S RIGHTS ON THE DARK WEB

Aman Sinha*, Dr. Ratnesh Kumar Srivastava*

* Student, B.A. LL.B. (Hons.), Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.
** Assistant Professor, Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.

ABSTRACT :

The flourishing of digital technology brought opportunities and threats alike, one of which was the dark web-a big challenge to child safety in no time. The same anonymity can also be used by criminals to commit crimes such as child exploitation, and human trafficking, or even spread child sexual abuse material (CSAM) over platforms popular with children like Tor. That is what we're trying to take up in this study: examining the legal and technical instruments necessary to guarantee children's rights are protected when they go on the dark web in India. The Indian constitution, besides the Protection of Children From Sexual Offences (POCSO) Act 2012 the Information Technology (IT) Act 2000, and the UN Convention on the Rights of the Child (UNCRC) form the framework of legal regulations that protect children. But with these constantly evolving threats in cyberspace, legislation is no panacea. To extract the dark web, which obscured some key ways of tracing CSAM dissemination and acquisition, more advanced technological solutions are needed--such as AI detection of CSAM content and related forensic matters, blockchain analytics, or even ethical hacking. Joint action across the spectrum of agencies, in cooperation with Internet service providers and international bodies, further enforces cyber policing programs. Bachpan Bachao Andolan case and cases like it underscore the significant role of the judiciary in providing measures against child sexual exploitation on the Internet. To protect children in the digital age, the law needs to be reformed in many ways, as do the methods for blocking websites and supporting regional cooperation to combat child exploitation. The findings of this study call for an ongoing change in formal law, increased intervention by technology, and further internationalization of efforts aimed at stemming illegal child exploitation in the dark web.

Keywords: Dark Web, Child Exploitation, Cybercrime, Digital Forensics, Legal Framework, POCSO Act, Information Technology Act, Cybersecurity.

INTRODUCTION

Digital technology is how the societies have become congenitally aware, making it possible to communicate, learn, and achieve success. The dark side of this technological evolution, in the form of the dark web, is now a very threatening challenge, not only in terms of safety but also of the child's rights. Illegal, immoral, and harmful activity abounds on the dark web, a concealed part of the internet that can only be accessed through software like Tor, that, due to the increased anonymity, acts as a petri dish for child exploitation, organized crime, and the dissemination of abusive content. An approach to protecting children's rights amid this volatile environment is synergistic, legally framed, and technically sound. When one stops to think about it, in India, where the digital footprint is expanding at a rapid rate, it is both a moral imperative and a legal obligation to ensure very robust mechanisms that allow for fighting such threats (UNICEF, n.d.).

1.1 *Background and Context*

The dark web is the part of the internet that is kept hidden and has no direct link to the internet known to us. Often it requires the right software the possibility of configuration, or simply authorization to access. The dark web is identical to the surface web in a way that the dark web doesn't get indexed by search engines because it's run on encrypted networks and users' anonymity is secure. While this acts in respectable manners to protect personal privacy and free speech, it also encourages covert acts. Illegal marketplaces, forums, and platforms on the dark web are where crimes like drug trafficking, arms dealing and, most worryingly, child exploitation carry on rife. The anonymity it gives gives a boost to those who engage in very serious violations of children's rights such as the publication of child sexual abuse material (CSAM) or grooming as well as human trafficking.

Internet penetration in India has grown exponentially, with millions of children having access to the internet to learn and socialize. And as they grow their online presence so does the potential for online threats, including from the dark web. Due to the sudden surge of crimes against children, we need to frame rules, regulations, law and also use technology against it. In fact, online child exploitation cases have jumped multi-fold in recent years, according to National Crime Records Bureau (NCRB). Not only is the necessity of legally protecting individuals in this circumstance clear, but so too is the potential for the technologically facilitated means of detection and prevention to address it.

Cyberspace — so children's rights in cyberspace is not something that can be dismissed altogether. India is a signatory of the United Nations Convention on the Rights of the Child (UNCRC) that states that children must not be exploited and abused of whatever form, including by way of digital technologies. In the Indian context the constitutional provisions

especially "Article 21" which contains the provisions for the right to life and personal liberty, and the statutory framework like "Protection of Children from Sexual Offences (POCSO) Act 2012" play a significant role in protecting the rights of children and children's welfare. However, cyber threats are constantly changing as threats become more advanced, especially on dark web platforms; hence, laws need to be in constant evolution along with advanced technological mechanisms. (Sorensen, 2020)

The landmark case of (*Shreya Singhal v. Union of India*, 2015), where the Supreme Court of India pointed out that to balance freedom of expression and removal of misuse of digital platforms, is of significance. However, it primarily dealt with the constitutional validity of 'Section 66A of the Information Technology Act, of 2000' but it set a precedent for regulating online content issues. It noted, however, that the state must protect people, including children, from online harm but that this does not compromise the fundamental rights of the public.

UNDERSTANDING THE DARK WEB AND ITS RISKS TO CHILDREN

While it brings great connectivity and access to information in the digital age, it has also opened more sinister doors for the less fortunate in life including children. The dark web is an encrypted network with so much anonymity. It is one of the most concealed and dangerous parts of the internet. Anonymity is helpful for privacy advocates and whistle-blowers, but it has been abused by those who engage in illegal activities such as child exploitation, trafficking, and illicit distribution. Since children are, by nature, very vulnerable, and immature, and are increasing online, they are disproportionally impacted. Predators operate with impunity on the dark web as it covers all these environments with cryptographic tools. To devise effective legal and technological safeguarding on forming the dark web technological framework and structural dynamics of the dark web and their corresponding risks, knowledge of the dark web among other things, is crucial. (Knodel, 2024)

1.2 *Structure and Functioning of the Dark Web*

There are three broad categories of the internet, denoted as surface, deep, and dark. The surface web refers to the part of the internet accessible through standard search engines like Google and Bing. This includes publicly indexed websites, including news portals, social media platforms, and e-commerce websites. Academically, the deep web is made up of content that is not searched by search engines such as academic databases, medical records, and many private administrative nets. In the case of the deep web, although the web itself is not inherently dangerous, being data behind paywalls or requiring logins, it is still inaccessible without very
specific permissions. (Kokolaki et al., 2020)

The deep web consists of the portion that is intentionally hidden and only accessible in special software — that is a lot smaller than the dark web. The main way to access the dark web is through the Tor network (The Onion Router), where users are anonymized by sending their communication over numerous servers around the world at each stage. The other prominent tool here is the Invisible Internet Project (I2P), which provides for secure and encrypted communication. While it's these technologies that were meant to enhance privacy, their robust anonymity has been exploited for criminal activities. Illegal goods are sold at marketplaces on the dark web as well as forums where criminal activities have become hot topics and networks for child exploitation. With such structural design, efforts to trace perpetrators are complicated yet; users as well as hosts remain largely unidentifiable without advanced cyber forensic tools. The dark web is used for the common purpose of selling illegal drugs and weapons, financial fraud, hacking services, and the distribution of child sexual abuse material (CSAM). Encryption technologies are continuously updated so that law enforcement agencies have learnt better ways to breach these networks. The characteristics of a networked world, such as the ability for criminal networks to mask identities, are not only emboldened through the dark web but create a complex legal landscape in which international cooperation and highly developed legal rods can be used to prosecute offenders.

1.3 *Risks Faced by Children on the Dark Web*

Direct targeting and access to harmful materials pose threats to children on the dark web. The child exploitation and abuse networks are among the most egregious threats. These are secretive communities that use encrypted forums and marketplaces for the exchange of CSAM, grooming techniques and live stream abuse for paying viewers. These individuals use dark web technologies to conceal their identity to successfully evade detection, which is a grievous challenge of law enforcement.

Online recruitment and grooming are also common. Predators use both surface and dark web platforms to approach potential victims while masquerading as peers to establish trust. When a connection is established the child can be forced or tricked into sending explicit photos, coerced into the conduct of abuse including transporting them across borders. Through the dark web, one can conduct such criminal activities with encrypted communication channels that make such criminal acts invisible to normal monitoring abilities.

Arguably the blackest part of the dark web is how far CSAM has spread. However, even with laws such as "Section 67B Information Technology Act, 2000", which is the amendment that
also made it a criminal offense for someone to send sexually explicit mail to a child or publish sexually explicit material involving a child, the dark web's anonymity allows for the offenders to remain obscure. The psychological impact on victims is massive, and the continuous spread of this online is compulsive retraumatization of these individuals even after all things are said and done by the offender. Virtually all victims suffer from chronic anxiety, depression, and post-traumatic stress disorder, knowing that abusers have their images anywhere and everywhere. (Ferrara et al., 2021)

Also, the dark web's material is not just explicit. In addition to violence, extremist propaganda, and fraudulent organizations such as illegal drug markets, the sites can hurt impressionable, young minds. Such content may unintentionally be stumbled upon by children or deliberately be targeted towards them by a person acting to radicalize or manipulate the child. These risks combine to make the point that the cumulative effect of all these risks is an urgent need for robust legal frameworks and technological safeguards to protect children in this shadowy digital space.

1.4 *Case Studies of Child Exploitation on the Dark Web*

There are chilling case studies for the global landscape and one that is yet to be overcome that documents the dark web's involvement in the facilitation of child exploitation. Leading the way for such groups is Operation Darknet, by international law enforcement agencies going after child pornography networks on the Tor network. It was this operation that uncovered thousands of illicit websites and forums hosting CSAM and triggered many arrests around the world. The Playpen investigation also constitutes the other big case: a dark web child pornography website that had 150,000 users. However, thanks to the FBI's ability to seize control of the site and to use a Network Investigative Technique (NIT) to identify users, dozens of offenders are prosecuted all over the world.

For example, the dark web child exploitation networks in India were hit by the Central Bureau of Investigation (CBI). A good example of this was a large-scale investigation of a darknet syndicate selling CSAM across different encrypted platforms. The operation, which lasted over several states, led to the arrest of some individuals and, the removal of an organized network of individuals operating within the production of broadcast and dissemination of illegal content. Using innovative cyber forensics and international work, the CBI traced the digital 'footprints' of the offenders to demonstrate the need for police to work across borders in fighting dark web crimes.

An Indian case that caused so much attention was the arrest of persons in Kerala in the context

of an international child pornography ring running over the dark web. The technique of encryption proved sophisticated and transactions financed by the cryptocurrency were difficult to trace. Yet with the help of tools like blockchain analysis and deep packet inspection, cybercrime units had succeeded in putting these recovered funds on trial.

These case studies embed the dark web's threat to the safety of children and this demonstrates the importance of law enforcement in such matters. Also, they mention the legal complications associated with jurisdiction, the admissibility of digital evidence under 'Section 63 of Bharatiya Sakshya Adhiniyam', and the demand for cybercrime legislation. In these cases, the interplay between the use of the latest digital tools and legal development shows the need for constant reform of technology and new, highly investigative techniques to protect children from the dark web that hides their threats.

LEGAL FRAMEWORK FOR PROTECTING CHILDREN'S RIGHTS ON THE

DARK WEB IN INDIA

The development of the dark web has made the task of protecting children's rights even more challenging, for which there is a need for a strong, multilayered legal approach dedicated to existing and novel threats to their rights. The Indian constitutional mandates, statutes, and evolving cyber laws shape the legal landscape within India to ensure that children are protected from exploitation on the online front, including from threats from the dark web. However, these traditional laws like the Indian Penal Code (now largely replaced by the "Bharatiya Nyaya Sanhita" or BNS) deal with crimes against children, while the 'Information Technology Act, 2000' (IT Act) is a specialized law, which has specific tools and approach for cyber crimes. These acts of crime are difficult to enforce because of the sophisticated encryption and anonymity of the dark web, requiring constant new legal reform and technological pipelining. It moves in the space of constitutional provisions and statutory mechanisms that aim to keep children off the perils of the dark web; drawing on these rules, which adopt principles from specific cyberspace to address these distinctive needs. (Kumar, 2023)

1.5 *Constitutional Provisions*

Several fundamental rights and directive principles, collectively, make up the cornerstone for the protection of children's rights, and those enshrined in the Indian Constitution as the supreme law of the land, constitute the Indian Constitution. This is found in "Article 21" which is the protection of the human right to life and personal liberty. In the case of "*(Maneka Gandhi v. Union of India,* 1978)", the Supreme Court interpreted the word 'Article 21', expansively to

encompass the right of the child for the dignity of living, as part and parcel of that provision, would protect children from exploitation, abuse, and dirty or dangerous physical environment and also the dirty and dangerous digital environment. This constitutional right is being constantly violated by the presence of child exploitation on the dark web, where child sexual abuse material (CSAM), child grooming, and child trafficking all occur. Consequently, there is a constitutional obligation on the State to pass and administer laws that protect children's dignity in real and virtual spaces.

Provisions under "Article 39(e)" and "Article 39(f)" further strengthen this protective framework enshrined under 'Directive Principles of State Policy' (DPSP). However, these clauses have the effect of obliging the State to discharge its duty aimed at preventing abused children and providing them an opportunity and facilities for development in a healthy way without exploitation and moral degradation. DPSPs are nonjusticiable meaning courts cannot enforce them, and are to be guiding principles for legislative and executive actions. The constitutional vision successfully imposes the duty upon the government to confront the new age threat that the dark web can present through suitable legal arrangements as well as policies. For instance, the Protection of Children from Sexual Offences Act, 2012 (POCSO Act) can be understood as another legislative response facilitating the DPSP's objective of protecting children from sexual exploitation in the digital era.

The protection of children's rights already goes beyond the domestic obligation in the international conventions. The ratification of the United Nations Convention on the Rights of the Child (UNCRC) by India only makes this obligation of the country immovable to protect children from all forms of exploitation and abuse, including online threats. "*(Vishaka & Ors. v. State of Rajasthan & Ors.,* 1997*)*" case and the Supreme Court in it relied on the fact that international conventions, although not directly enforceable, can be read into the constitutional framework to fill legislative gaps. IO considering this principle permits the Indian courts to expand the interpretation of constitutional provision and to fully incorporate the international standards of child protection in the era of the digital age. Therefore, the Constitution serves to render the moral and legal basis of ensuring that children's rights on the

dark web are protected, and in addition, provides the state with the tool to institute and enforce laws effectively fighting new cyber threats. (Vithalani, 2023)

1.6 *Indian Penal Laws and Cyber Laws*

Apart from constitutional protections, India's statutory framework bears a major role in having them dealt with when children are victims of crimes through the dark web. Several provisions

web as it evolves and thereby renders its conflict law suitable for the protection of the basic rights and of the 'Bharatiya Nyaya Sanhita' (BNS) which has replaced the Indian Penal Code, criminalize physical and digital sexual exploitation, trafficking, and abuse. Consider that Section 76 of the BNS criminalizes trafficking in persons, among them for purposes of sexual exploitation which is a common offense linked to dark web activities. Moreover, provisions relating to criminal conspiracy, obscenity, and exploitation are deemed applicable to online crimes so as not to help those accused of a crime in cyberspace to evade liability because the offense was conducted in cyberspace. (Gupta, n.d.)

The "Information Technology Act, of 2000" complements BNS India's predominant law relating to cybercrime. The IT Act specifically defines the offenses covered under 'section 67B' and such offenses pertain to the offenses of publishing, transmitting, or accessing children in sexually explicit material. It is a proviso with strict penalties under it including imprisonment for up to five years for first-time offenders and thereafter punishment will be increased as the law states. This law is essential for fighting the distribution of CSAM in the dark web, by allowing the prosecution of those involved in either creating, sharing, or indulging in such content no matter how the activity is conducted, anonymously on encrypted networks.

Additionally, the ''Protection of Children from Sexual Offences Act, 2012'' (POCSO Act) is a complete legislation to tackle sexual crimes against children. The Act is technology neutral, thereby applicable to offenses committed both offline and online. The POCSO Act was amended in 2019 and more severely; the death penalty was imposed for aggravated sexual assault reflecting the legislature met to dissuade such heinous crimes against children. Provisions of POCSO are invoked along with the IT Act in the digital context to deal with cases of online grooming, cyberbullying, and the distribution of CSAM.

Secondly, procedural laws relating to the investigation and prosecution of dark web crimes are included in the realm of legal enforcement in the form of the "Bharatiya Nagarik Suraksha Sanhita" (BNSS). The BNSS also gives law enforcement agencies the power to investigate cybercrimes, seize digital evidence, and persecute offenders effectively. Furthermore, Section 63 of the 'Bharatiya Sakshya Adhiniyam' deals with the admissibility of electronic evidence, because digital data may be the basis of the prosecution's case. (*Anvar P.V. v. P.K. Basheer & Ors.*, 2014) is an example of adapting wherein courts have recognized that it will be important to consider electronic evidence in cybercrime cases as the Supreme Court in its guidelines for admitting digital evidence to ensure that the delivery of justice will not be compromised owing to technological complexities.

In the meantime, specialized agencies like the Cyber Crime Investigation Cell, the Indian Computer Emergency Response Team (CERT-In), and the National Crime Records Bureau

(NCRB) help the country in its fight against transnational cybercrimes in alliance with international law-spurring bodies. Yet, legal provisions alone are not enough; continuous capacity building of law enforcement, judicial sensitization, and technological enhancement to conform with the dynamic of the cyber landscape must be adequately influenced. A dynamic legal system responsive to emerging threat environments in the form of the dark web is indispensable due to the transient form of the dark honor of children, as per the Indian Constitution.

1.7 *The Protection of Children from Sexual Offences (POCSO) Act, 2012*

One of the key Indian legislative acts aimed at derailing the coronavirus attacks on children is the Prevention of Children from Sexual Offences Act, 2012 (POCSO Act), comprising acts committed on the dark web. The Act specifies a child as any person under 18 years of age and crimes, ranging from penetrative and non-penetrative assaults, sexual harassment, and the use of children in the promotion of pornography. When the POCSO Act is applied to the dark web, it is especially applicable to the offenses related to child abuse within the digital environment as it takes the exploitation into account, as not just physical space is exploited. There are many forms: online grooming, the creation and circulation of child sexual abuse material (CSAM), cyberbullying, etc. The expansive Act covers offenses committed through the dark web encrypted platforms so that the offenses perpetrated through these platforms would not fall outside the purview of Indian law.

The POCSO Act focuses on online grooming, which is when an offender builds emotional relationships with children to manipulate, exploit, or abuse them. Grooming often starts on the open web and then moves to dark web platforms where they feel they are less visible. The Act makes it illegal to use children in the creation, possession, or offering of any CSAM. The amendments to the POCSO Act of 2019 see heftier penalties for child pornography offenses: harsher imprisonment terms of up to seven years along with a fine. This is the latest move in legislative history, towards policies weeding out dark web monopolies, for onward transmission of illegal content with growing force and anonymity.

1.8 *The Information Technology Act, 2000 (Amended 2008)*

The main law governing Internet crime in India is the "Information Technology Act of 2000, amended in 2008", and it includes crimes on the dark web committed by adults against children. Critical to India's drive against child pornography is "Section 67B". This part of the law deems

to be a crime the act of publishing, transmitting, or causing material that shows children engaged in sexually explicit activities, or indeed having a file deemed as CSAM reside on one's device. It also explains the techniques used to search for such websites and everything people can download from them, as well as how long they may store those things without fear of discovery. When new material is harvested online from innocent victims, it becomes part of the larger network for child exploitation: virtually spreading that every man should scan "digital child pornography" by some who also produce it. The punishment for a first offender who violates section 67B is up to five years in prison and a fine, and for a subsequent offense, the penalty is more severe. That is surely the intention of lawmakers.

Section 67B is particularly significant in the context of the dark web since it allows law enforcement agencies to prosecute the individuals who take advantage of the anonymity offered by encrypted networks for the distribution of CSAM. Such broad language in the section makes even actions not

directly related to victim interaction such as downloading or sharing abusive material offenses. This is a legal framework that allows the authorities to target it goes even beyond facilitating producers and consumers of CSAM and works to break down the intricate supply chains within dark web ecosystems. (Crepax et al., 2022)

"Another important provision is Section 69 which allows the government to take the advantage of intercepting, monitoring, and decrypting any information transmitted through any computer resource for the good of the national security, the public order or to prevent the incitement of the commission of an offense." However, the application of this section has been subject to debate in the context of privacy, but it is important to use this section if there's a case of child exploitation on the dark web. This will allow us to identify offenders, collect evidence, and break illegal networks. The exercise of these powers, however, is circumscribed by procedural safeguards to prevent misuse.

Under the IT Act, intermediaries are also expected to provide data related to cybercrime as per legal requests. As per the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", the platforms have to report such cases to the necessary authorities. The combined effect of this is to bring about a collaboration of legal environment, where the private sector participates in fighting the use of children online. Overall, the IT Act on its provisions and the regulatory framework empowers the Indian judicial system with the means to conquer the challenges beclouded by the dark web, without compromising that enforcement capability with constitutional inhibitions.

1.9 *The Indian Penal Code (IPC), 1860*

The "Indian Penal Code, 1860" (IPC), which is now replaced by the "Bharatiya Nyaya Sanhita" (BNS), was passed a long time before the digital era; yet nonetheless, several of its provisions are still applicable in demonstrating the offenses that people commit against children in the dark web. An example 'section' like this is 'section 78' which means that ones such as stalking (including cyberstalking) will be punishable. In particular, this is relevant when dark web offenders use the internet to track, intimidate, and harass children. Cyberstalking, in its more decisive forms, can wreck for life of a person, a family, or an entire community, as it may involve persistent monitoring, sending threatening messages, and utilizing technology to invade the privacy of a child. As technology aids in abuse, an understanding of how it can be used as a potential weapon and the legal recognition of stalking in both physical and digital forms indicates that we are coming to grips with this.

The BNS defines acts of insult to the modesty of a woman in 'Section 79'. In traditional cases of verbal or physical harassment, courts interpreted this section to include electronic crimes like sending obscene messages or sharing explicit content without consent. This provision can be used to punish those on the dark web who share non-consensual images or online harass children. Such offenses against minors do not only have a psychological impact but need stringent legal responses as Section 79 gives such offenders a fair ground for prosecution.

According to the BNS, section 143, human trafficking is defined as the process of observation, transportation, harboring, or receipt of human beings, with the use of coercion, fraud, or the use of power. Traffickers have used the dark web to coordinate such trafficking of children for sexual exploitation, forced labor, and other forms of abuse, and the dark web is now a tool. It also gives a legal basis in Section 143 to prosecute such offenses even if they are performed by cryptocurrencies through encrypted platforms.

Read along with specialized legislation like the POCSO Act or the IT Act, the provisions of the BNS's broad criminal provisions cover crimes committed against children, including those committed on the dark web. The law will keep evolving as this is the application of the traditional legal principles with the modern interpretation of the law to cope with new modes of criminal behavior. Indian courts have made efforts to read existing statutes in light of technological changes and thus resolve the disparity between historical legal ideas and the cyber threats of today. In the age of the dark web, it is crucial to protect children for this dynamic approach to safeguarding children.

INTERNATIONAL LEGAL FRAMEWORK AND INDIA'S COMPLIANCE

In a world where nothing can be done at the level of the nation and everything is globalized, in which the protection of children's rights is beyond the boundaries of the nation, it is imperative to have strong international legal instruments to tackle the threats like the dark web. Transnational crimes happen with ease on the dark web, which is characterized by encrypted and anonymous architecture: child sexual exploitation, trafficking, and the dissemination of child sexual abuse material (CSAM). As a result, conventions, treaties, and protocols have been created internationally to encourage cooperation between countries in the face of these offenses. To the extent that the domestic framework that is now India's legal framework on child protection is shaped by the international law governing the rights of the child, India has consented to such conventions. These instruments do not only set global standards for protecting the rights of children, but also put into place obligations on the state parties to promote conditions of prevention, investigation, and prosecution of children's rights, through the adoption of effective laws, policies, and mechanisms. India's domestic legal reforms as well as its engagement in the global effort to combat online child exploitation are examples of its commitments, as it has not joined all the conventions, like the Budapest Convention on cybercrime. (Manoj et al., 2025)

1.10 *UN Convention on the Rights of the Child (CRC)*

The most comprehensive international treaty on children's rights is the "United Nations Convention on the Rights of the Child" (CRC) adopted in 1989 including civil, political; economic; social, and cultural rights. Having ratified the CRC in 1992 India committed to preserve the principles set forth under the Convention including the right of every child to be protected from all forms of abuse, exploitation, and harmful practices. It will be shown that the CRC's broad definitions of child protection are relevant on the dark web as it is a tool to protect children from exploitation, even in the digital environment. Browse articles 34 and 35 of the CRC, which specifically binds state parties to protect children from all forms of sexual exploitation and abuse, including sexual exploitation of children in pornography and the trafficking of children.

In the Indian context, there has been a great influence of the CRC on domestic legislation such as the 'Protection of Children from Sexual Offences Act, 2012' (POCSO Act) and the 'Information Technology Act, 2000.' Cruelty reflects the CRC's guiding principles of criminalization of online grooming, CSAM production and distribution, and other forms of digital exploitation by these laws. Furthermore, the Supreme Court of India has also accepted

the influence of the CRC in its decisions.

Further, the CRC is a major source from which the Indian jurisprudence and policymaking have drawn the emphasis on the child's best interests as a primary consideration. Legislative reforms, judicial interpretations, and other administrative actions that intervene to protect children from dark web-related crimes are guided by this principle. The ROC does not include digital threats explicitly, however the broad mandate of CRC in child protection offers a legal, and moral basis, to act and combat emerging risks in the digital age. India's commitment to the adhesion of the CRC principles requires the constant updating of legal instruments and proactive measures to confront the problems and challenges offered by the dark web as technology evolves. (Caglar, 2021)

1.11 *Budapest Convention on Cybercrime (India as a Non-Signatory)*

The first international treaty concerning cybercrime was the "Budapest Convention on Cybercrime", adopted in 2001 by the Council of Europe. It aims at strengthening international cooperation, as well as harmonization of the national laws and efficient investigations and prosecutions of cybercrimes, which may include offenses relating to child exploitation. Although the convention is open to non-European countries, India is not a signatory to this convention. The non-membership has led the debates within India's legal and cybersecurity communities, as it can have a beneficial role to play in enhancing cross-border collaborations in tackling cyber crimes involving the dark web.

India, not being a party to the Budapest Convention, has taken part in the discussions and expressed interest in responding to the goals of the treaty, which refers to the significance of international cooperation in fighting interconnected cybercrimes. The Indian reluctance to sign the convention has had its origins in the concerns of the Indian government about sovereignty and the possibility of foreign jurisdictions exercising jurisdiction over the handling of cyber policies within the jurisdiction, as noted by the Indian government. Though, India has been engaged in bilateral and multilateral cybercrime arrangements, which include intervention in the INTERPOL, taking part in the Global Conference on Cyber Space, or under the Mutual Legal Assistance Treaty (MLAT) framework with other countries. (Kaur, 2022)

India's laws, for instance, the 'Information Technology Act, of 2000', contain certain principles that are in keeping with this Convention, like those of criminalizing unauthorized access to, breaches of, and offenses concerning child pornography. It is further, Indian law enforcement agencies like the Central Bureau of Investigation (CBI) and the Indian Computer Emergency Response Team (CERT-In) also act with international partners to investigate and

prosecute crimes related to the black web. Despite being not a Budapest Convention party to India, it has shown the capability to collaborate with other global agencies against dark web- based child exploitation network cases that found exposure.

The absence of formal membership in the Budapest Convention introduces some difficulties, in particular when it comes to swift and easy data sharing and cooperation with signatory countries in the legal sphere. Yet, India is maintaining its advocacy for a more comprehensive, UN-led framework that accommodates the developing countries' reservations over cyber sovereignty and jurisdictional concerns. With cybercrimes progressing to the point of sophistication as well as their transnational nature, there is a discussion making its own about whether India should go back to reclaiming its stance on the Budapest Convention or look towards different international partnership schemes that could help India become more capable of fighting dark web crimes.

1.12 *Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography*

To protect children from sexual exploitation and abuse, the 'Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, child prostitution, and child pornography' (OPSC), however, was adopted in 2000 and supplements the CRC. India signed the OPSC in 2005, indicating its dedication to the fight against child trafficking, sexual exploitation, and the spread of child pornography, including through the dark web. It obliged state parties to criminalize the sale of children, child prostitution, and child pornography, as well as to adopt measures for the prevention, investigation, and prosecution of these crimes.

The OPSC being passed, together with the POCSO Act and amendments to the IT Act, has been a huge influence on the legal landscape of India. To this end, these laws correspond to the protocol's purposes by classifying in broad terms offenses relating to the exploitation of children sexually in all cases, including those traditional and on the Internet. For example, the IT Act provides that, "Section 67B" is an offense cognizable and PC in India and punishable under section 67B as 'whoever commits the offense of desecration as provided under section, is punishable under the relevant section criminal in nature', specifically criminalizes the offense of the online publication and transmission of material representing children in sexually explicit acts, which is both in tune with India's obligation under the OPSC. Moreover, the provisions on the use of children for pornographic purposes under the POCSO Act address all the issues raised in the protocol and add to the convention and law that Indian law covers both the physical and digital forms of exploitation.

Children's rights in India have gone beyond legal reform to include its policy and law enforcement efforts for fighting child exploitation. The country's holistic approach to child protection is evidenced by government programs such as the "National Plan of Action for Children", and public awareness campaigns that provide for children. Specialized training is provided to law enforcement agencies about cyber crime investigation, international organizations keep on sharing the knowledge and building the capacity to submit complaints against dark web-related offenses.

Though India has become a trailblazing example of law that lines up with the objectives of the OPSC, there are gaps to fill when dealing with the complex strategies of the perpetrators on the dark web. To fulfill the commitments under the protocol effectively, constant legal reform, technological innovation, and international cooperation are necessary. India's adherence to the OPSC's principles will have a significant bearing on how the country responds to the complex, transnational nature of cyber threats to children in the cyber age. (Guermouche, 2024)

TECHNOLOGICAL SAFEGUARDS FOR PROTECTING CHILDREN ON THE DARK WEB

Encrypted networks, the anonymous architecture of the dark web, and many secretive profiles make law enforcement agencies and policymakers fighting for child protection a difficult task. The undeniable presence of digital pedophiles and their countless horrors of trafficking, online grooming, child sexual abuse material, etc. emphasizes the urgent need for sufficient technological safeguards. While legal frameworks are important, they cannot keep up with the rapid rise of the type of technology used by offenders, allowing them to not be caught. For this reason, advanced technological tools are essential for complementing legal measures. The war against dark web child exploitation is a two-pronged battle, where both artificial intelligent (AI)-driven systems in detection, as well as combined efforts from governments, private contractors, and nongovernment organizations (NGOs), are being taken. This section looks at the technological aspects of safeguarding children, dealing with digital forensics, roles of internet service providers (ISPs), collaborative frameworks, and the use of ethical hacking to function as proactive dark web monitoring. (Chertoff, 2017)

1.13 *Digital Forensics and Tracking Tools*

While these are being pursued through traditional law enforcement efforts, digital forensics has provided crime fighters and law enforcement agencies with a critical tool, allowing them to investigate and eventually ensure that offenders take their punishment in court. AI-based
CSAM detection is one such technology in this space with PhotoDNA leading the way toward a much more transformative technology in this area. The CSAM images have been developed by Microsoft using robust hashing algorithms to detect and mark known CSAM images even if it has been modified to avoid identification. Digital signatures convert images into code, and systems and law enforcement can quickly keep the harmful content out on platforms. Furthermore, the detection of grooming behaviors has been revolutionized by AI classifiers who have automated this process with machine learning algorithms to identify the pattern indicating abuse material or grooming behaviors. Rapid analysis of these data allows these tools to discover exploitation networks contained within the encrypted layers of the dark web. Meanwhile, blockchain technology is being used in new child protection themes. Despite the fact blockchain is typically linked to cryptocurrencies, its unalterable and transparent ledger system provides us with unique tools to fight online child exploitation. Reported CSAM can be secured through the use of blockchain to create secure databases of flagged material so that once alerted, the material will not be tampered with and can not circulate undetected. Furthermore, blockchain platforms have smart contracts that can automate the reporting mechanisms, which alerts the authorities in real-time to take action against suspicious activities that they are detecting. They also rely on cryptographic tracing methods, as transactions on the dark web are usually made with the use of cryptocurrencies like Bitcoin. Investigations using advanced cryptographic analysis have allowed investigators to trace the digital money trail, and untangle tangled networks of offenders and financiers involved in the trafficking and distribution of CSAM.
These technologies have been important in landmark cases such as takedowns of the dark web marketplace 'Welcome to Video' by which blockchain analysis helped to trace Bitcoin transactions to individuals engaged in CSAM activities. In this case, the dark web provides anonymity to perpetrators, but digital forensics working with international cooperation allows for the breaking of this anonymity. Such technologies are now being adopted in India on a gradual scale and cybercrime units are provided with sophisticated forensic tools as a part of the Cyber Crime Prevention against Women and Children (CCPWC) scheme. While much of the world is rapidly embracing these technological advancements for their ability to help detect and prosecute offenders, equally essential is the use of these same tools in victim identification and rescue, as they have to be used to protect children from online harm. (Gupta et al., 2023)

1.14 *Role of Internet Service Providers (ISPs) and Social Media Platforms*

Internet Service Providers (ISPs) and social media platforms are key stakeholders in the
ecosystem of child protection on the dark web. Their hugely extensive infrastructure and implicit control over the flow of data puts them in a distinctive class to be the first line of defense against online exploitation. Today, given the number of CSAM and other illicit content-related websites available on the Internet, ISP-level filtering and monitoring mechanisms are being deployed to block access to such websites. Isps can use a technological technique like Deep Packet Inspection (DPI) to inspect the network traffic in real-time and identify questionable activity that may lead to the dark web or pose as online child exploitation. Regulations on safeguarding minors from harmful content on the web mean that ISPs operating in jurisdictions like the UK are legally obliged to implement such filtering systems. About India, while it does not have a parallel legal mandate, the promise has been successfully demonstrated in collaborative efforts between ISPs and law enforcement agencies especially in cases where the illegal material is disseminated quickly.
They also contribute significantly to detecting and mitigating online grooming as a common measure leading to more serious exploitation over dark web channels. Such age verification systems that leverage AI and biometric technologies are also being created to keep minors away from restricted platforms or in front of potential predators. Currently, the use of natural language processing and behavioral analysis for grooming detection through AI moderation tools involves the automatic flagging of discussions showing red flags that correspond to manipulation or coercion. For example, Facebook and Instagram with their platforms are using algorithms that tweet for the grooming behaviors and warn those who could become the targets and also report any suspicious accounts to relevant authorities.
On the other hand, end-to-end encryption is becoming more prevalent and it becomes challenging to monitor and intercept harmful content. Encryption is important for user privacy, but it also establishes sanctuaries for offenders to talk, fearlessly. The encryption vs safety debate is becoming contentious as governments around the world push tech companies to develop lawful access means that can permeate and intercept cases of serious criminal activity. However, the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" that force digital platforms to track down the source of harmful content have been subject to legal scrutiny due to privacy concerns in India. Safeguarding user privacy and fulfilling child safety is a tricky cycle of legal and ethical challenges that are continuously lobbying the policymaker, the technology company, and civil society.

1.15 *Government and Private Sector Collaborations*

The effort to end child exploitation on the dark web has been done so far not by governments,
but in partnership with these public institutions, private sector, and multinational companies. In this regard, one of the most obvious examples of such collaboration is with INTERPOL and its laudable international attempts to fight cybercrime, notably crimes against children. The INTERPOL Crimes Against Children Unit is among such initiatives that help law enforcement agencies in the world to share intelligence and forensic data on offenders whose activities are beyond the borders. This global network gives India, as an active member of INTERPOL, the opportunity to participate in joint operations and in capacity-building programs to build the capacity to investigate cybercrime.
Within India, the Indian government has put in place several measures under the rubric of Digital India to strengthen cybersecurity infrastructure and guard against the online vulnerability of vulnerable populations. This way, states can set up Cyber Crime Coordination Centres (I4C) to coordinate on issues of cybercrimes including those touching on the issues of the dark web. The specialized units at these centers enable them to carry out their work on child protection, use advanced analytical tools to monitor online activities, and assist investigations. Its National Cyber Crime Reporting Portal also serves as a platform for the general public to report incidents of online child exploitation and thus the involvement of the general public in these efforts is increased.
Just as important is cooperation with the private sector, particularly by tech companies, cybersecurity companies, NGOs, and other institutions. Tools and policies for fighting CSAM have been developed by tech giants like Google, Microsoft, and Facebook specifically to fight it and help law enforcement. The Internet Watch Foundation (IWF), India's own Childline India Foundation, and other NGOs work closely with both governmental and non- governmental organizations to treat, remove harmful content, offer victim support, and secure tougher legalities. Often acting as intermediaries, these organizations help victims, law enforcement, and technology suppliers to pass information on to each other.
Many cases have seen successful interventions between government initiatives and private sector innovations. In 2021, when Indian cybercrime units and international law enforcement teams teamed up with tech companies, they busted a dark web child pornography ring, with arrests and the rescue of some victims. In the real world, we see the application of this case involves real-time sharing of information, interoperability of technological innovation, and cooperation between jurisdictions. The constant evolution of the digital landscape will mean that we need to continue cultivating strong partnerships between the public and private sectors to tackle the wide array of threats associated with the dark web.

1.16 *Dark Web Monitoring and Ethical Hacking for Child Safety*

In the arsenal of law enforcement agencies combating online child exploitation dark web monitoring and ethical hacking are as indispensable as can be. Because the dark web depends on encryption and anonymity to prevent those activities from getting flagged by traditional investigative methods, many traditional investigative techniques do not work here. Darknet intelligence and cyber patrol play a role here. Darknet intelligence consists of systematically monitoring children's exploitation activities on hidden websites, forums, and marketplaces. These hidden networks can be probed with specialized software tools that will crawl through the (virtually) empty nets and flag keywords, patterns, and metadata that indicate illegal activities. Trained officers and cyber analysts, put together into cyber patrolling units, are used to actively infiltrate dark web communities in controlled environments and gather evidence, identify perpetrators, and break cybercriminal networks. (Adel & Norouzifard, 2024)
These efforts are supported by ethical hacking also referred to as white hat hacking. Dark web infrastructures are simulated to be attacked by ethical hackers working with law enforcement to discover the vulnerability of such structures. They take advantage of these weaknesses by accessing hidden servers, tracing the IP addresses, and trying to penetrate encrypted data which can then lead to their identification and prosecution. Ethical hacking is legally sanctioned in several countries; India being among them, whenever it is allowed to be carried out with proper authorization, it is a powerful mechanism to prevent crimes on the dark web from happening. These techniques have proven themselves successful with the case studies provided for successful intervention. It is important to point out that one such example was the dismantling of the notorious dark web platform 'Playpen' which played an integral role in the marketing and distribution of massive amounts of CSAM. Using an ethical hacker, law enforcement agencies developed a technique known as the Network Investigative Technique (NIT) which enabled them to trace anonymous users. As a result, hundreds were arrested worldwide, and many child victims were safely rescued. Much like in India, cybercrime units have begun using this approach of darknet monitoring and ethical hacking to expose trafficking rings and CSAM networks. The proactive measure is not only helpful in bringing the offenders to court but also discourages them from engaging in such crime as even on the hidden web, their acts can be traced and prosecuted. Now, with technology moving forward, ethical hacking as well as monitoring on the dark web will become a major part of the law enforcement details that will help protect children from the dangers of the digital underworld.

JUDICIAL APPROACH AND CASE LAW ANALYSIS

Indian judiciary is a vital stakeholder in shaping the law of children's rights, particularly against the new type of threats using the dark web to exploit children. But while they have the statutory framework, i.e., the "Protection of Children from Sexual Offences Act, 2012" (POCSO Act) or the "Information Technology Act, 2000", the judiciary is the actual agent of enforcement through interpretation and application. This repository of the ninth report is highly important as it indicates that courts in India have forthrightly looked at children's rights and have been taking proactive programs not just for offenders, but protecting, rehabilitating, as well as caring and felicitating victims. This is an evolving stance of the judiciary during the endeavor of evolving with technological advancements and the complexity of cybercrimes about children. There have also been landmark judgments on key issues like the admissibility of electronic evidence, the role of intermediaries, and the need for victim-centric justice in cases of online abuse. The following part is an insight into the most pivotal judgments of the Supreme Court that impelled India to deal with the menace of online child exploitation.

1.17 *Landmark Indian Cases on Online Child Exploitation*

(*Bachpan Bachao Andolan v. Union of India*, 2011) was one of the landmark cases that presented the Indian judiciary's determination to take care of the problem in the internet space related to online child exploitation. Though not entirely concerning the dark web, the case stood out as the State's responsibility to prevent all kinds of abuse on the Internet, which paved the way for severe measures for such online crimes. Indirectly the Court has influenced how online abuse cases are dealt with today by directing the government to amend existing laws, strengthen investigation mechanisms, and expedite cases against people who exploit children.

The "*In Re: Exploitation of Children in Orphanages in the State of Tamil Nadu*"[1] suit, where the Supreme Court took suo motu cognizance about reports of rampant abuse of children including on digital platforms is another. Moreover, the Court's observations included how technology perpetuated and combatted child exploitation. The exercise emphasized the urgency of having robust cybersecurity protocols and a system that would ensure law enforcement agencies and internet service providers would be able to track and stop online abuse. It enabled advocates for the reforms of data monitoring, and the accountability of digital platforms' goal of preventing the spread of child sexual abuse material (CSAM).

Not only that, but the (*Shreya Singhal v. Union of India*, 2015) also brought a change with its

[1] (2002) 3 SCC 31.

far-reaching implications in online content regulation but the entire case was about freedom of speech. While the Supreme Court has struck down "Section 66A" of the IT Act as unconstitutional, it has allowed the government the right to ban content by 'Section 69A', as long as due process is followed. Indirectly, this ruling reinforced the mechanism for preventing harmful online content, including CSAM, by way of the legal framework of removal of harmful online content. It sought to make the legislative intervention balance between the safeguarding of constitutional rights, and the state's ability to forbid the online dissemination of illegal material.

The landmark cases also show how the Indian judiciary has evolved its policy toward handling the difficulties brought by online child exploitation. Tracing the efforts of all courts in upholding the importance of having robust legal frameworks, technological advancements, and stakeholder cooperation to fight out these crimes has enabled them to be well. The judiciary has also gone a long way in ensuring that any infringement of children's rights is not left unattended, even in the most complex and hidden nook of the digital world, by interpreting existing laws in light of the new technological reality. Indian courts' proactivity spreads into legislative reform, public policy, and law enforcement in line with safeguarding children from the dark web's evolving threats.

CONCLUSION

Child protection efforts are up against a formidable foe in the dark web, which cannot be sneaked out behind the bushes, as it provides anonymity through which crimes of child exploitation, trafficking, and distribution of child sexual abuse material (CSAM) are carried out. Even with legal and technological safeguards in place, the offenders are still able to leverage encryption to evade being tracked and prosecuted by police. Having an Indian legal framework based on constitutional provisions as well as 'The Protection of Children from Sexual Offences Act, 2012' (POCSO Act), 'The Information Technology Act, 2000' and "Bharatiya Nyaya Sanhita" (BNS), India intends to tackle these challenges through criminalizing the online child exploitation, bettering the capacity of cyber forensic and collaborating between countries. Cyber risks evolve and hence, legal concepts also need to, new enforcement mechanisms need to be put in place as well as advanced digital tools for battling the rising threat of child exploitation on the dark web. Also, India maintains its commitment to global child protection issues through international cooperation, under such frameworks as the UN Convention on the Rights of the Child (CRC) and the Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography (OPSC).

In fighting dark web crimes against children, technology will never be so important as it plays a role in defining offenders using digital forensics, AI-powered CSAM detection, and blockchain analysis and identifying offenders. There is collaboration between the government and private sector in terms of partnerships with internet service providers (ISPs), and social media platforms among others that have enabled policing mechanisms to become faster in doing away with harmful content. In addition, ethical hacking, dark net intelligence, and cyber patrolling have become important for tracking offenders and dismantling criminal networks. However, end-to-end encryption is widespread today and thus presents a significant challenge because it means a balanced approach between privacy and child safety is needed. A watchword of it is that online child protection policies in India have relied hugely on the Indian judiciary, evident from some landmark cases including (*Bachpan Bachao Andolan v. Union of India*, 2011), where the importance of digital evidence and digital platform accountability in preventing online exploitation have been struck.

The implementation of a multi-pronged approach to improve the success of child protection measures on the dark web must be moved forward. Addressing the difficulties of cyber-enabled child exploitation will require strengthening legal frameworks, investing in the most advanced forensic tools available, and increasing international cooperation. Continuous training needs to be provided to law enforcement agencies too on cybercrime investigation, and technology companies should take effect to implement stricter age verification and content moderation systems. Care must be taken in crafting the ethical implications of digital surveillance and legally requiring access to encrypted data to have the child safety outcome without compromising the individual privacy. Through the development of a collaborative ecosystem around legal, technological, and policy solutions, India can remain committed to protecting the rights of children in the context of the digital age, where even the darkest edges would become safe havens for perpetrators of child exploitation.

BIBLIOGRAPHY

1. Adel, A., & Norouzifard, M. (2024). Weaponization of the growing cybercrimes inside the dark net: The question of detection and application. *Big Data and Cognitive Computing, 8*(8), 91. https://doi.org/10.3390/bdcc8080091

2. *Anvar P.V. v. P.K. Basheer & Ors.*, AIR 2015 SC 180 (Supreme Court of India, September 18, 2014).
3. *Bachpan Bachao Andolan v. Union of India & Ors*, AIR 2011 SC 3361 (Supreme Court of India, April 18, 2011).
4. Caglar, C. (2021). Children's right to privacy and data protection: Does the article on conditions applicable to child's consent under the GDPR tackle the challenges of the digital era or create further confusion? *European Journal of Law and Technology, 12*(2). https://ejlt.org/index.php/ejlt/article/view/828
5. Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy, 2*(1), 26–38. https://doi.org/10.1080/23738871.2017.1298643
6. Crepax, T., Muntés-Mulero, V., Martinez, J., & Ruiz, A. (2022). Information technologies exposing children to privacy risks: Domains and children-specific technical controls. *Computer Standards & Interfaces, 82*, 103624. https://doi.org/10.1016/j.csi.2022.103624
7. Ferrara, P., Franceschini, G., Corsello, G., Mestrovic, J., Giardino, I., Vural, M., Pop, T. L., Namazova-Baranova, L., & Pettoello-Mantovani, M. (2021). The dark side of the web—A risk for children and adolescents challenged by isolation during the novel coronavirus 2019 pandemic. *The Journal of Pediatrics, 228*, 324–325.e2. https://doi.org/10.1016/j.jpeds.2020.10.008
8. Guermouche, F. Z. (2024). The international legal framework for protecting children from cybercrimes: Cyberbullying as a case study. *International Journal of Early Childhood Special Education, 16*(4), 1043–1057. https://www.int-jecse.net/article/The+International+Legal+Framework+for+Protecting+Children+from+Cybercrimes%253A+Cyberbullying+as+a+Case+Study_7187/?download=true&format=pdf
9. Gupta, S., Kumari, S., & Sugandh, U. (2023, November). Protecting children's data from cybersecurity attacks to prevent child sexual abuse: A techno-legal approach. In *2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)*. https://doi.org/10.1109/ICCSAI59793.2023.10421403
10. Gupta, V. (n.d.). *Protection of kids from cybercrimes: Role of technology contracts*. iPleaders. https://blog.ipleaders.in/protection-kids-cybercrimes-role-technology-contracts/
11. Kaur, G. (2022). Internet crimes against minors and legal framework in India. *Indian Journal of Public Administration, 68*(4), 705–718. https://doi.org/10.1177/00195561221091381
12. Knodel, M. (2024, February 23). *Children's rights at the centre of digital technology standards by design*. Expert Speak, Raisina Debates. https://www.orfonline.org/expert-speak/children-s-rights-at-the-centre-of-digital-technology-standards-by-design
13. Kokolaki, E., Daskalaki, E., Psaroudaki, K., Christodoulaki, M., & Fragopoulou, P. (2020). Investigating the dynamics of illegal online activity: The power of reporting, dark web, and related legislation. *Computer Law & Security Review, 38*, 105440. https://doi.org/10.1016/j.clsr.2020.105440
14. Kumar, R. (2023, September 25). *Protecting our kids from the dark web's menace!*. LinkedIn.https://www.linkedin.com/pulse/protecting-our-kids-from-dark-webs-menace-ranjit-kumar/
15. *Maneka Gandhi v. Union of India*, 1978 AIR 597, 1978 SCR (2) 621 (Supreme Court of India, January 25, 1978).
16. Manoj, D., James, R. I., Kumaran, S., Devnath, G. P., Varughese, B. T., Arakkal, A. L., & Johnson, L. R. (2025). Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation. *Child Protection and Practice, 4*, 100088. https://doi.org/10.1016/j.chipro.2024.100088
17. *Shreya Singhal v. Union of India*, AIR 2015 SC 1523 (Supreme Court of India, March 24, 2015).
18. Sorensen, S. (2020). Protecting children's right to privacy in the digital age: Parents as trustees of children's rights. *Children's Legal Rights Journal, 36*(3), 156–178. https://lawecommons.luc.edu/clrj/vol36/iss3/2
19. UNICEF. (n.d.). *Protecting and prioritizing children's rights and safety in digital environments: A call to action.* UNICEF. https://www.unicef.org/innovation/stories/protecting-childrens-rights-in-digital-environments
20. *Vishaka & Ors. v. State of Rajasthan & Ors.*, AIR 1997 SC 3011 (Supreme Court of India, August 13, 1997).
21. Vithalani, N. P. (2023). Cyber crimes and law in India: A critical analysis. *International Journal of Creative Research Thoughts, 11*(8), e942–e953. https://ijcrt.org/papers/IJCRT2308532.pdf