

# SAFEGUARDING DIGITAL CHILDHOOD: A CRITICAL ANALYSIS OF THE IT ACT, 2000 IN ADDRESSING CYBERBEGGING AND SHARENTING

*Satyam Mangal*<sup>1</sup>

## **Abstract**

*In the rapidly evolving digital age, the rights and safety of children in cyberspace are increasingly at risk. This article critically examines the Information Technology (IT) Act, 2000, in the context of protecting digital child rights, focusing on emerging concerns such as cyberbegging and sharenting. It highlights the inadequacies of the Act in addressing these issues, despite its role as a foundational framework for managing cybercrimes in India. Through an analysis of legislative gaps, judicial responses, and international practices, the paper underscores the urgent need for comprehensive reforms. Suggestions include introducing specific provisions to criminalize cyberbegging, establishing regulatory mechanisms for sharenting, and aligning India's digital laws with global standards like the GDPR. The article emphasizes the dual need for robust legal frameworks and societal awareness to safeguard children in the digital sphere. Strengthening digital child rights is essential to ensure a secure and equitable environment for the next generation.*

**Keywords:** digital child rights, cyberbegging, sharenting, IT Act 2000, digital privacy laws

---

<sup>1</sup> Satyam Mangal is a 3rd-year student of B.A. LL.B. (Hons.) at Maharashtra National Law University, Nagpur.

## Introduction

*“There can be no keener revelation of a society’s soul than the way in which it treats its children.”* (Mandela, 1995)

In his speech at the Launch of the Nelson Mandela Children’s Fund in Pretoria, South Africa, on May 8, 1995 Nelson Mandela has quoted these words very succinctly so as to iterate how society’s true progress is reflected in how well it protects its most vulnerable members, especially children, from the dangers from various issues. In this digital age it is our responsibility to protect and nurture them because they are the foundation of our future. In today’s world, technology has become a central part of our lives, and children are increasingly exposed to the risks that come with being online. It is easy to frame and implement laws for any vulnerable section of society who can understand their rights and duties but it is very difficult to frame and implement laws for a vulnerable section who cannot understand their rights and duties. Children, people of unsound mind are some of the example of those vulnerable groups who cannot understand their rights and duties. Additionally, various factors like social and demographic factors, lack of experience (Carcelén-García et al., 2023), limited critical thinking skills, inherent trust in others makes children digitally more vulnerable towards any cybercrime (Boston Consulting Group, 2022) or 4Cs which includes content risk, conduct risk, contract risk, contract risk (OECD, 2023).

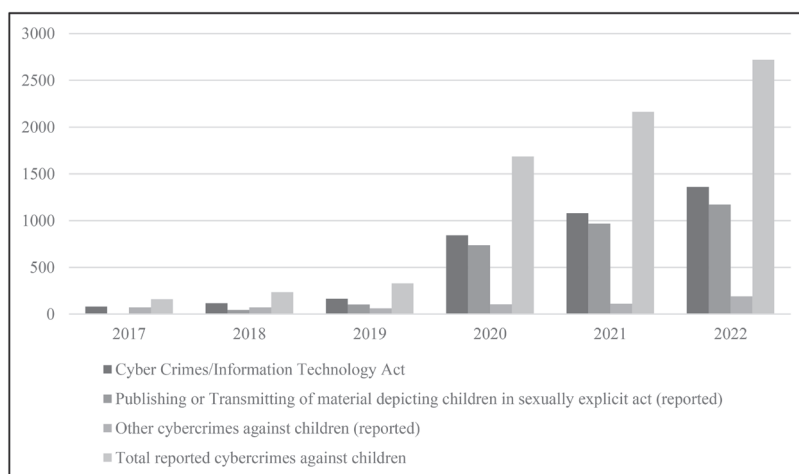
This research project, aims to looks at the gaps and limitations in the IT Act, 2000 when it comes to protecting digital child rights. It focuses on two main issues: cyberbegging, where children are exploited through digital platforms for begging; and sharenting, where parents share too much information about their children online, often without realizing the long-term effects. Furthermore, this article critically analyzes the efficiency and sufficiency of IT Act, 2000 to deal with these issues and to suggest some recommendations for filling the gaps of IT Act, 2000.

## Critical Analysis of the Efficiency and Sufficiency of the Information Technology Act, 2000

Technological advancements have made our life both easy and difficult at the same time. If we take a simple example of our phone then it makes our life easier in clicking our pictures, messaging our friends, keeping our documents

etc. but at the same time there is always a risk that your pictures, messages or documents got leaked and misused by someone else to make your life difficult. This misuse of technology which affects society at large is termed as cybercrimes in general. Nowadays, almost all the crimes which were happening in our living space are got shifted on to virtual space because it is more efficient to commit crime where your identity is hidden. From 2019 to 2020 there was an increase 400% cybercrime against children (Economic Times, 2021) which is still persisting as shown by NCRB data (NCRB, 2017-2022):

Sr. No.	Year	Cyber Crimes/ Information Technology Act	Publishing or Transmitting of material depicting children in sexually explicit act	Other cybercrimes against children	Total reported cybercrimes against children
1.	2022	1360	1171	189	2720
2.	2021	1081	969	112	2162
3.	2020	842	738	104	1684
4.	2019	164	102	62	328
5.	2018	117	44	73	234
6.	2017	79	7	72	158



***Reported cybercrimes against children in India***

*Source: Based on data collected from NCRB Reports*

Furthermore, the Supreme Court of India in the case of *Just Rights for Children Alliance & Anr. vs. S. Harish & Ors.*, 2024 has recently reversed the

judgment of Madras High Court which held that watching child porn is not an offence. The supreme court has even shown its sensitivity towards the use of term ‘Child Pornography’ and held that this term has failed to capture the full extent of crime thus, gave the term ‘Child Sexual Exploitative and Abuse Material’ (CSEAM). The court also observed that Sec. 15 of POCSO Act penalizes storage or possession and that there is no requirement for the actual transmission of the material for the section to apply thus, it is the intention which is being punished and not the commission of any criminal act in the traditional sense.

The IT Act, 2000 is the foundational legal framework for managing cybercrimes and regulating electronic communication in India. However, its efficiency and sufficiency in addressing child rights, particularly in emerging issues like cyberbegging, sharenting, child pornography, and age restriction in social media usage by children, face several challenges. These are some of those issues which if happen in our living space then they are criminalized by statutes like Bhartiya Nyay Sanhita, 2023 (hereafter BNS, 2023), POCSO Act, 2012, Juvenile Justice (Care and Protection of Children) Act, 2015 (hereafter JJ Act, 2015) etc. but what if these issues are emerged on virtual space, does India have efficient and sufficient statutory mechanism to deal with these issues.

### **Begging v. Cyberbegging**

Begging is an act of gaining something from someone on the ground of sympathy and the supreme court of India recognized it “as a socioeconomic problem in which people are forced to beg for their livelihood due to lack of education and employment” (Hindustan Times, 2021). However, there are two categories of beggar, first category includes forced beggars on which honorable supreme court has put emphasis and the second category includes beggars by habit who are lazy and see begging as a way out (Aulia Simanungkalit & Pasaribu, 2023). The distinction between the first and second category is of choice. First category of beggars doesn’t have a choice therefore a ban on such begging wouldn’t be efficacious (Deccan Herald, 2021). However, the second category of beggars have a choice but consider begging as business therefore such ban on such begging would be efficacious.

The term ‘begging’ is defined under Sec. 2(8) of JJ Act, 2015 as “(i) soliciting or receiving alms in a public place or entering into any private premises

for the purpose of soliciting or receiving alms, under any pretense; (ii) exposing or exhibiting with the object of obtaining or extorting alms, any sore, wound, injury, deformity or disease, whether of himself or of any other person or of an animal”. Furthermore, Sec. 76 of JJ Act, 2015 and Sec. 139 of BNS, 2023 provides stringent provisions of punishment for offender who employ/kidnap/maim/objectify/use children for begging. Judiciary has also taken stricter stances against both offenders and governments for preventing the instances of child begging in living space. Recently, in the case of *Yatharatha Foundation v. Union of India, 2023* the Delhi High Court ordered Delhi government to rehabilitate the children rescued from child begging. The Calcutta High Court has also taken a *suo moto* cognizance in 2020 for the violation of child rights in child abuse cases which includes child labor, child begging etc. and held that, “The State must also take steps to ensure that all the JJBs and CWCs in the State have proper video-conferencing facilities and other infrastructural facilities and a report to that effect should be filed in terms of this order” (In re Court on Its Own Motion, 2020). Child begging of such kind is prohibited by both legislature and Judiciary in living space but when it comes to virtual space, none of them have taken any positive to curb such instances.

Cyberbegging refers to the act of begging on social media which has increased due to pandemic in many countries (Aulia Simanungkalit & Pasaribu, 2023). Its instances ranges from urgent medical donation to systematic long-term donations (Shrinidhi, 2007). The situation become worse when people started employing/ kidnapping/ maiming/ objectifying/ exploiting children online by forcing or manipulating them into begging through digital platforms. It is a phenomenon which happens with us on daily basis but we either ignore it or if support it don't look into the veracity of fact. For example, there are various news article websites in which between the article they show images/videos of a disabled child asking for help for its treatment, on social media platforms like Tiktok (Raisha Shahana et al., 2023), WhatsApp, Facebook, Twitter on regular basis we came across various posts, news, images, videos which objectifies/ maims a child. Although in the case of *Avnish Bajaj v. State, 2008* the court held that, “intermediaries (like websites) should be vigilant in ensuring that exploitative content involving children is not uploaded or circulated.” But the IT Act lacks specific provisions addressing cyberbegging. Existing sections on obscene content or illegal activities online, like Sec. 66 and Sec. 67, may be

invoked in extreme cases of exploitation, but they do not directly address the nature of cyberbegging. Furthermore, enforcement mechanisms within the IT Act are poorly equipped to track and penalize cyberbegging. Law enforcement agencies may struggle to monitor and identify online exploitation efficiently, especially when content may not overtly appear criminal. Therefore, there is a need of a regulatory mechanism to deal with this issue.

### **Parenting v. Sharenting**

Parenting in its traditional sense involves nurturing, guiding, and protecting children as they grow into responsible and independent adults. It includes making decisions that ensure the child's well-being, development, and safety. In today's digital world, however, a new concept has emerged: sharenting. Sharenting refers to the practice of parents or guardians sharing excessive amounts of information about their children on social media platforms often including photos, videos, and personal details (Ugwudike et al., 2024). Sharenting expert Stacey Steinberg defines sharenting as, "what parents do when they talk about their children outside the family circle, A post on social media with a picture, a blog post about their child, a video through a messaging platform like WhatsApp, etc" (UNICEF, 2025).

While parents share these moments out of pride or to connect with family and friends, sharenting can lead to significant privacy risks for the children. These risks include exposure to identity theft, online predators, and misuse of personal data. The practice also raises ethical questions about children's right to privacy and how their digital footprints, often created without their consent, could affect their future (Ugwudike et al., 2024). In this context, IT Act, 2000 which is India's key legislation for regulating cyber activities comes under scrutiny. While it addresses several aspects of digital privacy and security, it lacks specific provisions to protect children from potential harms caused by sharenting. This gap necessitates a closer look at how the law can be strengthened to balance parental sharing with the protection of children's privacy in the digital age.

The IT Act, 2000, currently lacks any specific provisions that regulate how much personal information parents can share about their children on social media platforms. While Sec. 43 and 72 offer some general privacy protections, they don't apply to situations where parents, rather than strangers

or hackers, expose their child's private information. This means that if a parent overshares their child's details, such as their full name, school location, or daily activities, without considering long-term privacy concerns, the law doesn't step in to protect the child. Unlike in Europe, where the General Data Protection Regulation (here after GDPR) grants children the right to privacy and the right to be forgotten, India's IT Act does not offer similar safeguards for minors.

India has enacted Digital Personal Data Protection Act, 2023 (hereafter DPDP Act, 2023) which on the same lines of GDPR grants children as data principle the right to privacy and right to be forgotten under Sections 12(1) & (2), 9(2), 8(7) and 6(4) & (7) of DPDP Act, 2023. However, there is still a grey area where parents/guardians act both as data fiduciary and data principle for their children. Under DPDP Act, 2023, data principal is defined as "the individual to whom the personal data relates and where such individual is a child, includes the parents or lawful guardian of such a child" and data fiduciary is defined as, "any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data." In these types of situations, parents/guardians act on their whims and fancies, and do whatever they want with the personal data of their child sometimes knowingly and sometimes unknowingly. This shows that IT Act, 2000 was inherently inefficient to deal with the issue of sharenting and more specifically these types of situations. Furthermore, the new DPDP Act, 2023 is also not quite sufficient to deal with the issue at hand because it does not provide a regulatory mechanism for the situations where parents/guardians act both as data fiduciary and data principle for their children.

The study of Livingstone and Stoilova shows that "5-7 years old child has a sense of privacy rules but struggle to comprehend the consequences of their actions, privacy 8-11 years old child is governed more by rules than internalized personality and 12-17 years old child is aware of privacy risks, assess opportunities and risks but tend to focus on short-term benefits when making a decision." (Livingstone et al., 2019). This shows that an age-based consent model can be developed which has child centric approach that will help children in sharing their views, supporting their different experiences, and encourages a safer and inclusive online space. Additionally, parents/guardian should be seen as trustees of the data of children so as to minimize the misuse of children's data.



## **Suggestions for Addressing these Emerging Cyber Issues**

The IT Act, 2000 was initially created to handle issues related to cybersecurity, e-commerce, and online crimes. However, the rapid growth of digital platforms has led to new problems, especially for children, that the law does not adequately cover. One such issue is cyberbegging, where vulnerable children are exploited online to beg for money. According to the National Institute of Rural Development and Panchayat Raj in their working paper, “Improvised Beggary in India: A Case Study of Telangana State,” the causes of begging include destitution, lack of care for vulnerable groups, and the absence of institutional support (Sarap et al., 2021). Issues like cyberbegging and sharenting also found their relation to these three fundamental causes.

To effectively tackle these emerging issues, the IT Act needs to be updated and the following suggestions can be used to strengthen the legal protections of children in the digital age, ensuring their safety and well-being online. Article 39(f) of the Constitution of India mandates the state to provide children with opportunities and facilities to develop in a healthy manner. Article 12 of the United Nations Convention on the Rights of the Child suggests that weightage should be given to the views of children in accordance with the age and maturity. These provisions can be used as front runners to take legislative, executive and judicial steps for protecting the rights of children in this digital age. Following are some issue wise suggestions which are analyzed and derived from various legal reports, case law, and international practices to provide a more comprehensive approach to safeguarding children:

### **Begging v. Cyberbegging**

#### ***Legislative Reforms***

Specific provisions should be added to the IT Act to criminalize cyberbegging and the online exploitation of children. These provisions should clearly define online child labor and cyberbegging, making it easier for law enforcement to act against offenders. Also, central government should be given power to make rules and regulations to prohibit it. Furthermore, laws like children’s image rights (LAW No. 2024-120, 2024) can be implemented which aims to protect children’s privacy through the lens of right to their image. Cyberbegging should attract severe penalties, including imprisonment and



finer, similar to penalties for child labor and exploitation. The JJ Act, 2015 provides penalties for child labor, and similar rules can be applied for digital platforms (*Bachpan Bachao Andolan v. UOI*, 2011).

### ***Technological Interventions and Community Based Approach***

Digital tools like fact checkers, community notes should be implemented to monitor and flag activities (Drolsbach et al., 2024) that involve children being forced to beg or work online. Concerned authorities can cooperate with social media platforms and digital payment processors to track suspicious behavior.

### **Parenting v. Sharenting**

#### ***Legislative Reforms***

New child data protection law should be introduced to specifically address the issue of sharenting and deal with the grey area of DPDP Act, 2023. These laws should require parents to seek age-appropriate consent from their children before sharing personal information online. If the child is too young to give consent, parents should be guided by strict privacy standards and there should be an authority to look into all the matters which are related to use of personal data of children.

#### ***Policy Measures***

The government should implement educational campaigns and instructive courses aimed at parents, making them aware of the risks associated with oversharing their children's data online. This can be modeled on campaigns related to child safety. *Justice K.S. Puttaswamy v. Union of India* (2017) case established that every individual, including children, has a fundamental right to privacy. This ruling opens the door to argue that sharenting may infringe on a child's right to privacy, potentially extending to the Right to Be Forgotten once the child reaches an age where they can understand the implications of their data being shared online (*Justice B.N. Srikrishna Committee*, 2018).

### **Conclusion**

Law and society are dynamic in nature and the evolution of one inevitably leads or should potentially lead to the evolution of the other. Whenever there is a particular issue then it can be dealt either with the evolution of society or with the evolution of law. Evolution of society is something which can't be done/

happen abruptly, while on the other hand evolution of law is something which can be done overnight if it justifies the public interest. Therefore, to tackle contemporary issues such as cyberbegging and sharenting both legal reform as well as social awareness is necessary. The strength of a society lies in how well it safeguards the rights and dignity of its children, especially in the unseen spaces of the digital world.

In this light, one of the major concerns discussed above is cyberbegging, where children are exploited on digital platforms, manipulated into begging online. Unfortunately, IT Act, 2000 lacks specific provisions to criminalize such activities, making it difficult for law enforcement agencies to take effective action. To address this, new laws focusing specifically on online child exploitation are urgently needed. These laws should work in coordination with digital platforms to monitor and flag suspicious activities while imposing strict penalties on those who exploit children in the online space. Similarly, the rising issue of sharenting, where parents unknowingly compromise their children's privacy by oversharing personal information on social media, is another area of concern. The current IT Act does not regulate how much personal information parents can share, leaving children vulnerable to privacy breaches. To protect children's digital rights, new regulations should require parents to obtain appropriate consent before posting sensitive information about their children. Along with legal measures, awareness campaigns are essential to educate parents about the potential long-term impacts of oversharing in the digital space.

The IT Act, 2000 laid the groundwork for regulating cyberspace; it needs significant updates to address the evolving digital threats children face today. Although the DPDP Act, 2023 is enacted to deal with many of the issues but as proven in the project, there are still lacunas in it. Thus, the various offences and penalties provided under IT Act, 2000 are not efficient and sufficient for dealing with the contemporary digital child rights issues. Therefore, by implementing stronger legal measures and raising awareness, we can create a safer, more secure digital environment that not only protects children but empowers them to navigate the digital world responsibly. Only through these efforts can we ensure that children's rights and dignity are upheld in this fast-changing technological landscape.

## References

- Aulia Simanungkalit, D., & Pasaribu, I. (2023). Legal review of regulations regarding online begging on social media based on the Siyasah Fiqh perspective. *Law Development Journal*, 5(3), 334-343. Retrieved from <https://wsj.westscience-press.com/index.php/wsis/article/download/199/223/1161>
- Avnish Bajaj v. State (2008). *150 DLT 769*.
- Bachpan Bachao Andolan v. Union of India (2011). *AIR 2011 SC 3361*.
- Bhartiya Nyaya Sanhita, 2023, § 139 (India).
- Boston Consulting Group. (2022). Why children are unsafe in cyberspace. Retrieved from <https://web-assets.bcg.com/ec/76/4d06204a4f8e9f90428a3d992373/bcg-why-children-are-unsafe-in-cyberspace-sep-2022.pdf>
- Carcelén-García, S., Narros-González, M. J., & Galmes-Cerezo, M. (2023). Digital vulnerability in young people: Gender, age and online participation patterns. *International Journal of Adolescence and Youth*, 28(1). <https://doi.org/10.1080/02673843.2023.2287115>
- Chiara Patricia Drolsbach, Solovev, K., & Pröllochs, N. (2024). Community notes increase trust in fact-checking on social media. *PNAS Nexus*, 3(7), 217. <https://doi.org/10.1093/pnasnexus/pgae217>
- Deccan Herald. (2021). A ban on begging is no solution. Retrieved from <https://www.deccanherald.com/opinion/editorial/a-ban-on-begging-is-no-solution-1016319.html>
- Digital Personal Data Protection Act, 2023, §§ 12, 9, 8, 6, 2 (India).
- Economic Times. (2021). Over 400% rise in cyber crime cases committed against children in 2020: NCRB data. Retrieved from <https://economictimes.indiatimes.com/news/india/over-400-rise-in-cyber-crime-cases-committed-against-children-in-2020-ncrb-data/articleshow/87696995.cms>
- General Data Protection Regulation, 2016, Art. 17 (Europe).
- Hindustan Times. (2024). The Supreme Court is right on begging. Retrieved from <https://www.hindustantimes.com/editorials/the-supreme-court-is-right-on-begging-101627471711972.html>
- Information Technology Act, 2000, §§ 43, 66, 67, 72 (India).
- In re Court on Its Own Motion (2020). *2020 SCC OnLine Cal 2376*.

- Justice B.N. Srikrishna Committee. (2018). A free and fair digital economy: Protecting privacy, empowering Indians. *Ministry of Electronics and Information Technology*. Retrieved from [https://www.meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report.pdf](https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf)
- Justice K.S. Puttaswamy v. Union of India (2017). *AIR 2017 SC 4161*.
- Just Rights for Children Alliance & Anr. vs. S. Harish & Ors. (2024). *2024 INSC 716*.
- Juvenile Justice (Care and Protection of Children) Act, 2015, § 2, 76 (India).
- LAW No. 2024-120 of February 19, 2024. (France)
- Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online: Growing up in a digital age. *London School of Economics and Political Science*. Retrieved from [https://eprints.lse.ac.uk/101283/1/Livingstone\\_childrens\\_data\\_and\\_privacy\\_online\\_evidence\\_review\\_published.pdf](https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf)
- Mandela, N. (1995). Address at the launch of the Nelson Mandela Children's Fund. *Nelson Mandela Foundation*. Retrieved from [http://www.mandela.gov.za/mandela\\_speeches/1995/950508\\_nmcf.htm](http://www.mandela.gov.za/mandela_speeches/1995/950508_nmcf.htm)
- NCRB. (2017-2022). *Crimes in India* (Vol. I).
- OECD. (2023). *21st Century children: Digital risks and resilience*. Retrieved from <https://www.oecd.org/content/dam/oecd/en/about/projects/edu/21st-century-children/21st-century-children-digital-risks-and-resilience.pdf>
- Protection of Children from Sexual Offences (POCSO) Act, 2012, § 15 (India).
- Raisha Shahana, Indriani, M. K., & Wiryany, D. (2023). Analysis of online begging phenomena in TikTok: Case study of changes in the structure of social problems about online beggars. *West Science Interdisciplinary Studies*, 1(6), 346-352.
- Sarap, K., Manikandan, A. D., & Sahu, P. P. (2021). Impoverished beggary in India: A case study of Telangana State. *National Institute of Rural Development and Panchayat Raj*. Retrieved from [https://nirdpr.org.in/nird\\_docs/srsc/srsc290621.pdf](https://nirdpr.org.in/nird_docs/srsc/srsc290621.pdf)
- Shrinidhi, H. (2007). Cyber begging—Ask money for anything and everything. Retrieved from <https://www.enidhi.net/2007/09/cyber-begging-ask-money-for-anything.html>
- Ugwudike, P., Lavorgna, A., & Tartari, M. (2024). Sharenting in digital society: Exploring the prospects of an emerging moral panic. *Deviant Behavior*, 45(4), 503-520. <https://doi.org/10.1080/01639625.2023.2254446>
- UNICEF. (2025). Sharenting. Retrieved from <https://www.unicef.org/parenting/child-care/sharenting>
- Yatharatha Foundation v. Union of India (2023). *SCC OnLine Del 5639*.