CHILD RIGHTS AND YOU

Cyber-safety of children during COVID-19 & beyond

Policy Brief

Authors
Japreet Grewal (Technical consultant)
Shreya Ghosh (CRY)
Priti Mahara (CRY)

Published by: Child Rights and You (CRY)
Address: 632, 2nd floor, Lane No.3
(Beside Delhi Haath & Rajasthan Emporium Shops),
Westend Marg (Saket Metro Stati on to Garden of Five Senses), Saiyad ul Ajaib, New Delhi,
Telephone: 011 2953 3451
Website: www.cry.org

Published First: September 2021

Citation: Child Rights and You (CRY), 2021, ‘Cyber-safety of Children during Covid-19 and Beyond’

Introduction

Internet has increasingly become an integral part of children's lives, as a major method for daily communication with a wide variety of individuals, and for exploring a wide range of interests. One third of Internet users globally are children, with the proportion of Internet users likely to be higher in lower income countries where the Internet is rapidly penetrating all spheres of public life[1]. This ubiquity, however, is raising many concerns for parents, guardians, educators, child rights organisations and legislators alike. In the last two decades, there has been a phenomenal growth of internet usage in India. Of the overall internet population in the country, 433 million are of the age of 12 years and above, and 71 million are in the age bracket of 5-11 years who access the internet on the devices of the family members. Mobile phones are the key device for accessing internet in both urban and rural India due to their affordability along with availability of cheap data plans[2].

Despite the significance of this medium in children's lives in India, what is lacking is robust and representative data documenting online experiences of the country's children. In the global north there is already a considerable body of theory, evidence and expertise regarding children's online experiences but it is important to acknowledge that this may not necessarily apply to children's experiences in the global south.[3] Children have often been heralded as 'digital natives' which is problematic because it treats all children as the same and it tends to exaggerate their ability and understanding of these spaces, thereby leaving them vulnerable to risks that adults may have not yet noticed.

Several small-scale studies indicate that disparities exist in internet access and use based on socioeconomic status, geography and gender. In contexts where children do have internet access, it is primarily through mobile phones; it often begins in late childhood; is gendered and may involve shared or community-ownership rather than personal ownership of devices. Few children have received much guidance from school or home. Too many have only basic functional skills, and there are particularly worrying gaps in their information and digital literacy skills. This situation becomes more worrisome in a country like India where adult's education/literacy is still a challenge and digital literacy is at its minimal stage especially in marginalised communities.

The risks and opportunities faced by children have stimulated the development of legislation, regulation and resources designed to support their well-being and rights in a digital age globally as

[1] Livingstone, S., Carr, J. and Byrne, J. (2016). One inThree: Internet Governance and Children's Rights. Innocenti Discussion Paper No.2016-01, UNICEF Office of Research, Florence https://www.unicef-irc.org/publications/pdf/idp_2016_01.pdf

[2] Internet and Mobile Association of India, Digital in India, 2019- Round 2 Report, https://cms.iamai.in/Content/ResearchPapers/2286f4d7-424f-4bde-be88-6415fe5021d5.pdf

[3] The application of knowledge from any one time, place or culture to another must be carefully considered and critically appraised, and researchers must remain open to continual revision.

well as in India. However, problems that children face in the digital age are neither new nor specific to the internet.

In recent years, various UN agencies and related bodies concerned with children's well-being have addressed the importance of the internet in relation to children's rights. The key challenge is to develop rights-based strategies to maximize online opportunities for children while protecting them from risks and possible harm. Efforts must be directed towards ensuring that children are not positioned solely as vulnerable victims, and there is a need to acknowledge their agency and rights to access, information, privacy and participation.

This policy brief aims to provide a conceptual understanding of the most pressing cyber-safety issues affecting children in India and makes recommendations for improving the current policy landscape in the country to more effectively address these problems. The objective here is not to take a position as favouring or opposing children's use of internet but to contribute to a better understanding of how this medium can be made a part of children's lives in a safer way. With children's lives increasingly turning virtual as a result of the COVID 19 pandemic measures whether it is learning or leisure, it is imperative that the significance of digital technologies is integrated in the policy priorities for children's safety.

Part 1 : Cyber Safety and Children – Perspectives

Cyber safety primarily refers to concerns about the physical and psychological well-being of children who use digital technologies.[4] As more and more families and communities are gaining internet access, online activities are becoming increasingly embedded in children's lives. It has thus become critical to understand how these changes in technology are also changing how children socialise, participate, learn and communicate. In this context it has become essential to understand when these spaces are likely to expose them to harm. This section presents key underlying ideas on cyber-safety that bridge the knowledge gap between child protection principles and characteristics of online spaces by answering some critical questions –

1. How do we decide what is harmful to children online and how is it harmful? For instance, is exposure to obscenity or pornography, receiving hostile or racist messages, visiting a self-harm chatroom, or having one's social networking profile trashed, harmful to a child? Opinions on these vary, for instance, there is no consensus on what exactly is the harm when a child is exposed to pornography - is it harmful because it upsets or shocks the child,

[4] Gasser, U., Maclay, C. M., & Palfrey, J. G. (2010). Working towards a deeper understanding of digital safety for children and young people in developing nations. *Berkman Center Research Publication*, (2010-7), 10-36.

or because it distorts her conception of sexuality, or because it puts pressure on girls to perform certain sexual acts?[5]

2. Where is the harm ultimately suffered by the child? Harm is always suffered in the real world for instance as, physical harm, emotional distress, or social exclusion. Thus, in order to understand online harm, it is useful to fall back on the understanding of offline harm to children in the child protection discipline.[6] In fact, other related issues about online harm such as extent of parental responsibility and moral issues about when exposure to the adult world is appropriate are not internet specific issues; they are related to how we conceive childhood and are familiar debates in the offline world. [7]

3. Some children appear to be more likely to encounter risk or when they do encounter risk, more likely to find it harmful. Those who encounter risks offline are also likely to encounter them online, and those who encounter one risk online are also likely to encounter other risks.[8] This variation in the risk of online harm can be attributed to factors that are age-related, biological (e.g. temperament), psychological (eg. thoughts, emotions) or socio-cultural (models of behaviour around the child – beliefs, ideology[9]).[10]

4. A child may take or encounter risks, but not experience abuse or harm. Many children, for example, may place personal information online, which many adults might characterize as risk-taking behaviour, but only a minority are likely to experience any consequential harm.[11] This reflects a gap between child and adult perceptions of what is risky or desirable online. It also reflects on the type and frequency of complaints filed related to online harm/abuse. Thus considering children's perspectives becomes critical to producing policy measures that are effective at mediating between adults and children. Online safety entails addressing online risk by trying to balance between limiting access to opportunities and the measures to protect those vulnerable to harm. Online opportunities that provide benefits for children, if restricted for some can result in the negative outcome of digital exclusion.

[5] Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy. *ZER: Journal of Communication Studies*, *18*(35), 13-28.

[6] Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy. *ZER: Journal of Communication Studies*, *18*(35), 13-28.

[7] Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy. *ZER: Journal of Communication Studies*, *18*(35), 13-28.; Byron, T. (2008). Safer children in a digital world: The report of the Byron Review: Be safe, be aware, have fun.

[8] Livingstone, S., & Palmer, T. (2012). Identifying vulnerable children online and what strategies can help them.

[9] Livingstone, S., Mascheroni, G., & Staksrud, E. (2015). Developing a framework for researching children's online risks and opportunities in Europe.; Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

[10] Byron, T. (2008). Safer children in a digital world: The report of the Byron Review: Be safe, be aware, have fun.

[11] (2012). Child Safety Online: Global challenges and strategies. Technical Report, *Innocenti Publications*

Part 2 : Cyber Safety of Children – Online Risks

Online risks can be subdivided into three categories-

1. **Content risks** which generally position the child as the recipient of mass produced content
2. **Contact risks** constitute adult-initiated online interactions which require the child to participate, possibly unwittingly or unwillingly
3. **Conduct risks** where the child is an actor or interactor within a wider peer-to-peer or networked interaction.

High-speed internet connections, higher bandwidth, increased use of peer-to-peer networks, more sophisticated compression and encryption techniques to ease anonymous distribution, and new ways of accessing the internet through Wi-Fi on mobile phones or prepaid cards that reduce traceability have all contributed to the potential for online abusive and exploitative activity towards children[12].

This section describes sexual risks/abuse, aggression-related risks/abuse (cyberbullying) and commercial (privacy and personal data related) risks/abuse.

Sexual Risks/Abuse

Sexual risks particularly in context of online sexual abuse, grooming/sexual solicitation, sexting, exposure to pornography, production and circulation of child sexual abuse material have been studied widely in the global north[13]. However; the evidence on online sexual exploitation and abuse in South Asia is patchy. ECPAT's[14] report on Online Sexual Exploitation in South Asia provides a sense of how these risks are experienced in countries like India. As an example, the report highlights the prominence of gendered experience of sexual risks evident in widespread sexual harassment and extortion of girls caused by perpetrators who are generally known to the victims, often peers or adults in the circle of trust.[15] Sexual risks across varied abovementioned contexts are explained with an objective to provide some conceptual clarity.

[12] (2012). Child Safety Online: Global challenges and strategies. Technical Report, *Innocenti Publications*

[13] Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online.; (2017). Combatting the Sexual Exploitation of Children in South Asia: Evolving Trends, Existing Responses and Future Priorities, ECPAT; (2012). Child Safety Online: Global challenges and strategies. Technical Report, *Innocenti Publications;* Livingstone, Sonia and Smith, Peter K. (2014) Annual research review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. Journal of Child Psychology and Psychiatry, 55 (6). pp. 635-654.; Slavtcheva-Petkova, V., Nash, V. J., & Bulger, M. (2015). Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. *Information, Communication & Society*, *18*(1), 48-62.

[14] Find more about ECPAT's work here: https://www.ecpat.org/

[15] (2017). Combatting the Sexual Exploitation of Children in South Asia: Evolving Trends, Existing Responses and Future Priorities, ECPAT

Exposure to pornography

Viewing pornographic material (both wanted and unwanted exposure) is one of the most discussed and debated issues that is perceived to have harmful effects on children. The term ‘pornography’ itself, can refer to diverse kinds of sexual content ranging from partial nudity to graphic depictions of sexual intercourse to violent or illegal images of abuse. The Indian law unpacks its view of obscenity and pornography in its substantive laws.[16] Cyber obscenity and cyber pornography are included in Information Technology Act 2000[17]. As per section 67 of IT Act any material is obscene which is lascivious or appealing to the prurient interest of its viewers or if its effect is such as to tend to deprave and corrupt persons. Section 67A covers the offence of publishing or transmitting any material which contains sexually explicit act or conduct in electronic form. Further Section 67B of the Information Technology Act, 2000 (IT Act) covers child pornography and criminalises transmission and publication of any material in electronic form which depicts children engaged in sexually explicit act or conduct, collects, creates, browses, downloads, promotes, entices or induces children to online relationships (including having sexual connotations), facilitates online abuse, records own abuse or others abuse, etc. Although as per Indian laws personal viewing, downloading, and possessing such content is not punishable unless the victims are children. Also the publications proved to be justified as being for the public good, in the interest of science, literature, art, learning, used for bona fide heritage or religious purposes, etc. are kept outside the purview of the abovementioned offences.

Children’s exposure to pornography is often considered as inevitably harmful. In fact, exposing a child to pornographic material or sharing such material with him/her is criminalised under the Protection of Children from Sexual Offences Act (POCSO), 2012[18] and the IT Act, 2000[19]. Many children (especially children in late adolescence) may deliberately seek pornography or obscene content to access information about sexuality. This tendency in children may increase with the lack of opportunities and platforms (through (family, school, etc.) that provide information about sexual and reproductive health and behaviours.

An alternative view is that internet also ‘pushes’ pornography at those seeking informational or health related content, a phenomenon that can be called accidental exposure. Children cannot always know the harmful effects of such exposure, especially in the long term for instance, it may lead to developing unrealistic sexual values and beliefs[20] or a stronger belief in women being sex

[16] Sections 292, 293, 354A, of Indian penal Code, 1860 ;

[17] Section 67, 67A, 67B of the Information Technology Act, 2000

[18] Section 11 of the POCSO Act, 2012

[19] Section 67 and 67A of the IT Act, 2000

[20] Owens, E. W., Behun, R. J., Manning, J. C., & Reid, R. C. (2012). The impact of Internet pornography on adolescents: A review of the research. *Sexual Addiction & Compulsivity*, *19*(1-2), 99-122.; They find tentative evidence that “youth who consume pornography may develop unrealistic sexual values and beliefs.”

objects.[21] An urgent policy need is to distinguish harmful from harmless activity and potentially criminal from legal activity and also to take up the challenge of making sexual and reproductive health related information more accessible and free from any kind of prejudice.

Online sexual abuse and exploitation

Sexting

Sexting involves communication with sexual connotations – this can include a wide range of activities including, creating and sharing nude/partially nude pictures or videos among peers, chatroom conversations about sex (video/no video) or messaging between romantic partners[22]. The latter could range from consensual sex-chats to being coerced to share sexual material [23]. Children and young people may indulge in sexting either with people they know or strangers they meet online[24].

While the Indian law does not use the term sexting, it criminalises several activities that constitute sexting. For instance, under the POCSO Act, 2012 and the IT Act, 2000, enticing or coercing a child to participate in sexually explicit acts is a criminal offence.[25] Some of these sexually explicit acts under the law include sexual harassment, verbal acts, showing pornography, threatening to use depiction of a child in a sexual act and enticing a child for pornographic purposes. Further, such communication also falls within the scope of what Section 67 of the IT Act regards as criminal acts. This section uses the lens of obscenity (discussed earlier) to criminalise activities i.e. publication or transmission or any material that is considered 'lascivious' or 'prurient'. This technically includes consensual sexual chats between young people in a relationship or children sharing pornography with each other and could be considered a disproportionate reaction to such communication.[26] As with pornography, there is no clear line between acceptable sexual exploration between peers and inappropriate or abusive messaging.

[21] Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry*, *55*(6), 635-654; This study quotes Peter and Valkenburg (2009) who found that increased exposure to online pornography led to a stronger belief in women being sex objects

[22] Slavtcheva-Petkova, V., Nash, V. J., & Bulger, M. (2015). Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. *Information, Communication & Society*, *18*(1), 48-62.

[23] Slavtcheva-Petkova, V., Nash, V. J., & Bulger, M. (2015). Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. *Information, Communication & Society*, *18*(1), 48-62.

[24] Slavtcheva-Petkova, V., Nash, V. J., & Bulger, M. (2015). Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. *Information, Communication & Society*, *18*(1), 48-62.

[25] Section 11 of the POCSO Act; Section 67B of the Information Technology Act

[26] Section 67 - 'Whoever' transmits, publishes or causes to be transmitted or published, any material that is 'lascivious', or which appeals to the 'prurient interest' is punished under this section.

Online Grooming/ Sexual Solicitation

Online Grooming is a process of socialisation through which an adult engages with and manipulates a child or young person for the purpose of online sexual abuse (which may include offline aspects)[27]. Groomers' can pursue sexual solicitation online by using chatrooms focused on children's interests, personal websites, social networking sites, or e-mail and other online communication tools.[28] The abuse can subsequently take place through an online or an offline interaction or both. The online grooming process may involve various stages namely, friendship and relationship-forming stages, risk assessment, exclusivity/isolation, and the sexual stage where an offender is in contact with a child over a sustained period of time. The grooming process however may become sexual in just minutes, hours, or days, in many cases depending on the goals and desires of the particular offender.

While studies in the US[29] and Europe[30] have reported a small proportion of children being victimised by such encounters this minority nevertheless has had painful and even tragic experiences as analysis of cases reported to the UK children's helpline reveals[31]. Cases have also been reported in the South Asian travel and tourism markets of child sex offenders who groom children online and continue abusing offline, often returning to the same child over a period of time to gain his or her trust by giving gifts and offering support[32].

Although the crime statistics in India, do not disaggregate data on online grooming of children yet, the phenomenon is recognized and addressed in some detail by the IT Act, 2000. The term 'online grooming' is not used in the law, however, Section 67B of the IT Act defines the acts constituting online grooming i.e., whoever, -- ... (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or (d) facilitates abusing children online; or (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children.

[27] Livingstone S, Davidson J, Bryce J, Batool S, Haughton c, Nandi A. (2017). Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group. Department of Digital Culture, Media & Sport. London School of Economics

[28] (2017). Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review, International Center for Missing & Exploited Children

[29] Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry*, *55*(6), 635-654; Youth Internet Safety Survey, Finkelhor - The three waves of the nationally representative Youth Internet Safety Survey, conducted among US 10-17 year olds in 2000, 2005 and 2010; Wolak, Mitchell & Finkelhor, 2006; for wave 3, see Jones, Mitchell & Finkelhor, 2012

[30] Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online.

[31] Livingstone, Sonia and Smith, Peter K. (2014) Annual research review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. Journal of Child Psychology and Psychiatry, 55 (6). pp. 635-654.

[32] (2017). Combatting the Sexual Exploitation of Children in South Asia: Evolving Trends, Existing Responses and Future Priorities, ECPAT

Children makes many contacts online with people they have not met face to face and hence it is very difficult for a child or parent or caregiver to determining which online contacts pose a threat especially given the complex technical and social tactics employed by sexual offenders

Facilitation of commercial sex work and trafficking

Internet has also facilitated prostitution and trafficking of children in South Asia.[33] The internet and mobile phones can be used to support prostitution activities, connecting pimps, clients and victims more efficiently thus managing the sex business beyond traditional brothels. It also helps trackers in both contacting potential victims and connecting with criminal networks. Both local and travelling child sex offenders rely on internet to network among themselves, share information about locations where children may be available, either in the country where they reside or abroad, and organise local or cross-border criminal activity.

The UNODC has analysed several trafficking case profiles[34] to describe how in internet based trafficking, traffickers operate across borders and in multiple locations at the same time, while physically exploiting the victims in a single location. Internet can thus be used to broadcast or livestream acts of exploitation, reaching a large base of consumers in different locations throughout different regions of the world. Victims are often held and coerced into video performances, allowing the offenders to connect with potential clients (also offenders) living abroad. This type of trafficking typically relies on the availability of video equipment and digital recording devices to broadcast victims' exploitation. The way internet technologies are used to commit trafficking in persons changes according to the profile, group size and level of cyber expertise of the traffickers themselves.

Trafficking thrives on the internet in varied forms - spanning from simple advertisements of victims online to using communication platforms to broadcast exploitation abroad, to interacting with potential victims or transferring money between trafficking group members. The use of different online spaces/platforms by traffickers to recruit potential victims appears to relate with the age profile of the victims. Children and teenagers are often courted by traffickers on social media platforms and they appear to be susceptible to deceptive ploys in the search for acceptance, attention or friendship or love relationship or marriage.

[33] (2017). Combatting the Sexual Exploitation of Children in South Asia: Evolving Trends, Existing Responses and Future Priorities, ECPAT

[34] (2020). Global Report on Trafficking in Persons 2020, United Nations Office of Drugs and Crime.

Child Sexual Abuse Material

CSAM emerges as an area of special concern in India where evidence suggests that distribution of images is widespread[35]. CSAM includes, at a minimum, the visual representation or depiction of a child engaged in a (real or simulated) sexual display, act, or performance. With the advent of new technologies, it is imperative that the law acknowledges all the forms CSAM can take, all the ways CSAM can be distributed and all the ways in which CSAM can be possessed[36]. It overlaps with grooming as some offenders expose children to child pornography during the grooming process and make videos and images of offline sexual acts with children, or ask children to take sexual pictures of themselves.

It is a particularly alarming issue because it involves pictures and movies that are a record of a sexual assault on a child. Even when victims are successfully rescued and protected from further abusive acts, their victimisation is repeated in perpetuity as once the images are on the internet, they can easily be transmitted to other websites, downloaded onto mobile phones or distributed to an unknown number of recipients via email without requiring the knowledge or consent of the individual depicted.[37]

Each time CSAM is viewed by an adult, it makes the idea of sexual relations with children by adults acceptable.[38] In much of the research on CSAM, the main context for the abuse appears to be domestic, and the relationships between those producing the images and the children are familial or of social proximity. [39]

CSAM is criminalized in the IT Act, 2000 and the POCSO Act, 2012. Although not explicitly mentioned in the IT Act, CSAM could fall under its section 67B, which among other actions criminalises the creation of text or digital images and material in any electronic format that depict children in an obscene or sexually explicit manner. Further, Section 14 of the POCSO Act, 2012 criminalizes the use of children for pornographic purposes in any form of media, including the portrayal of child's sexual organs, the participation of a child in real or simulated sexual activities and the indecent or inappropriate portrayal of a child. Under Section 15 of the POCSO Act, 2012,

[35] (2020). Cybertipline Report. National Center for Missing and Exploited Children; The National Centre for Missing & Exploited Children (NCMEC) in the USA released some figures for the reports of online child sexual abuse material (CSAM) that they received in 2019. The highest number of uploads of suspected CSAM was from India as per geographical indicators related to the content. The figure reported is a sobering 1,987,430 pieces of content

[36] (2018). Model Legislation & Global Review on CSAM. International Centre for Missing and Exploited Children.

[37] New technological options, such as cloud storing facilities and the Darknet help with constant availability of new products, but also more effective escape routes to act with impunity; Dark Web is a collection of thousands of websites that use anonymity tools like Tor and I2P to hide their IP address. While it's most famously been used for black market drug sales and even child pornography, the Dark Web also enables anonymous whistleblowing and protects users from surveillance and censorship. You can read more about dark web at: Finklea, Kristin. (2017). *Dark Web* . Congressional Research Service.

[38] (2008). Enhancing Child Safety and Online Technologies. Final Report. Internet Safety Technical Taskforce. Berkman Center for Internet & Society. Harvard University

[39] (2012). Child Safety Online: Global challenges and strategies. Technical Report, Innocenti Publications

the storage of child pornographic material including for commercial purposes is also criminalized. Cyber Crimes related to transmitting of material depicting children in sexually explicit acts increased from 7 cases in 2017 to 44 in 2018 and 102 in 2019 (NCRB 2019). Highlights of a virtual conference on Child Sexual Abuse Material (CSAM) organized by the National Human Rights Commission state that there has been about 120% increase in the demand of pornographic material related to children during the lockdown induced by the Covid-19 pandemic. The document also mentions that in the year 2020, India received around 25,000 reports regarding the use and circulation of CSAM from the National Centre for Missing and Exploited Children (NCMEC) which is an agency that helps tracking websites that contain CSAM[40].

While content is criminal and needs to be taken down as they may potentially be put within reach of consumers of CSAM, the fact remains that not everyone who produces and sends CSAM is necessarily a criminal. Some of them are children themselves who may be indulging in sexting and maybe just taking a nude photo of themselves. Hence online code of conduct and online legal literacy amongst children is very much the need of the hour.

Live-Streaming of Child sexual abuse

One particularly insidious form of ICT-enabled child sexual exploitation constitutes the live streaming of sexual abuse, providing pay-per-view interactive content for perpetrators. Perpetrators often announce to their peer group (online and / or offline) regarding their intention to abuse a child on a set date and time. Those who wish to watch the live abuse arrange with the perpetrator to be online at that time. Viewers of live streaming child sexual abuse can be passive (i.e., pay to watch) or active by communicating with the child, the sexual abuser, and/or facilitator of the child sexual abuse and requesting specific physical acts (e.g., choking) and/or sexual acts to be performed on and/or performed by the child. Active participation on the part of the viewer is known as *child sexual abuse to order*, and can occur before or during the live streaming of child sexual abuse.[41] Payment may be in money or through bartering, such as exchanging images or drugs. Children may be lured into the perpetrator's house and sexually abused, and may or may not be aware that live transmission is occurring. Live images of abuse may also be recorded for future distribution in order to generate maximum profits[42].

[40] National Human Rights Commission (2020) https://nhrc.nic.in/sites/default/files/MinutesVirtualConference-OnlineChildSexualAbuse21072020.pdf

[41] UNODC, Module 12, Interpersonal Cybercrime, https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html

[42] UNODC (2015), Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf

Although live-distant child abuse has traditionally concentrated in South-East Asia, in particular in the Philippines, Europol has warned that it is spreading in other countries in South Asia especially among its lower socio-economic communities. [43] The key challenges in addressing CSAM are-

(1) Eliciting cooperation of the intermediaries[44] to proactively identify and remove CSAM and facilitate investigation through evidence sharing with law enforcement officials;
(2) Capacity building of local law enforcement officials to investigate CSAM related cases and appropriately handle evidence; and
(3) Understanding the tradeoffs between encryption and CSAM detection.[45]

A report released by the Rajya Sabha (upper house Government of India) in February 2020 on online child sexual abuse makes exhaustive technological and legislative recommendations, notably, mandatory reporting of CSAM by intermediaries to Indian authorities, and allowing legal backdoors to end to end encryption[46]. Further, draft amendments to Intermediary Liability Rules under the IT Act require platforms to use technological tools to proactively monitor content for taking down CSAM content, among other types of content[47]. Currently, most social media companies use PhotoDNA[48], as a primary tool used to detect child sexual abuse materials on digital communications platforms which is then reported to the National Center for Missing and Exploited Children (NCMEC)[49] in the USA. The underlying argument here is that with end-to-end encryption, social media platforms or messaging apps cannot be monitored at scale to scan for CSAM. This will also limit the evidence that law enforcement can access for investigations- this is because once the NCMEC receives CSAM reports, it alerts relevant national law enforcement authorities to take up

[43] ECPAT (2017) Regional Overview: Combating the sexual exploitation of children in South Asia. Evolving trends, existing responses and future priorities, https://www.ecpat.org/wp-content/uploads/2018/03/Regional-Overview_South-Asia.pdf

[44] Intermediaries under Section 2(w) of the Information Technology Act, 2000 are entities that provide services enabling the delivery of online content to the end-user – these involve ISPs, search engines, DNS providers, web hosts, interactive websites and cyber cafes. In February 2021, the Ministry of Electronics and Information Technology released the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 which have drastically altered the intermediary liability regime in India – they now regulate online intermediaries, as well as digital news organisations and OTT video streaming which are not intermediaries as per the parent legislation but act as publishers of information that goes beyond the authority of the parent legislation. Rule 4(4) of these new rules mandate a class of these intermediaries to deploy AI based content filtering technologies that proactively identify content such as rape or child sexual abuse, or other content that had previously been removed.

[45] (2017). Combatting the Sexual Exploitation of Children in South Asia: Evolving Trends, Existing Responses and Future Priorities, ECPAT; (2017). Child Online Protection in India. UNICEF India Country Office

[46] Parliament of India. (2020). Report of the Adhoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and its Effect on Children and Society as a whole. Rajya Sabha Secretariat. New Delhi.; https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf End-to-end encryption is a particularly robust form of encryption where third party intermediaries (such as a service provider) do not have keys to decrypt the communication; it is only readable by the two parties exchanging information.

[47] Ministry of Electronics & Information Technology. (2018). The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 at https://prsindia.org/files/bills_acts/bills_parliament/Draft_Intermediary_Amendment_2018.pdf

[48] PhotoDNA relies upon scanning every image that passes through a digital communications platform, assigning each image a unique hash, and then checking these hashes against the NCMEC database of illegal images; NCMEC explained below.

[49] An organization established by act of congress as a national resource center on missing and exploited children. In the USA it acts as the official clearinghouse for reporting of online child sex abuse materials.

those cases. At the same time, end-to-end encryption is critical to enabling people to communicate and ultimately be able to exercise their right to privacy and freedom of expression.

It is thus pertinent to explore if traceability of CSAM and perpetrators on end to end encrypted platforms is possible without breaking end to end encryption; and if there are effective alternatives to the enforcement of pro-active monitoring of content on platforms. It is necessary that we find a balance between protection of children from sexual exploitation and abuse and the potential privacy protections that the end-to-end encryption provides[50]. The Rajya Sabha Committee Report[51] discusses several technology solutions such as use of meta-data for investigation, installing backdoors for law enforcement access, compelled disclosure, device level (end-point) scanning of CSAM but measures need to be put in place to reduce risks to user privacy and ensure effective investigation.

Aggression-related risks

Cyberbullying/ Online Harassment/ Cyber-victimisation

Cyber bullying is often referred to as the intentional and repeated harm of others through the use of computers, cell phones, and other electronic devices.[52] It can take different forms, including threats and intimidation; harassment or cyberstalking, such as repeatedly sending unwanted texts or instant messages; vilification and defamation; exclusion or peer rejection; impersonation; unauthorized publication of private information or images; and manipulation. It is difficult to pinpoint how prevalent cyberbullying is as studies use varying definitions of cyber-bullying, but it is clear that this risk is the most common risk minors face online. Cyberbullying involves a range of actions (noted above) many among them may constitute a criminal offence under the IT Act, 2000 or the Indian Penal Code, 1860. For instance, disclosing a person's data, stalking, criminal intimidation, impersonation etc. are all punishable acts.

Cyber bullying is the element of imbalance of power that is critical to distinguishing bullying from other forms of aggression i.e. the victim finds it difficult to defend herself. In some cases imbalance can be seen in better skills demonstrated by the perpetrator than the victim such as the ability to impersonate and maintain anonymity. However, in cases where the victim knows the perpetrator, then the conventional criteria of physical/psychological strength and peer group popularity may

[50] Kardefelt-Winther, D., Day, E., Berman, G., Witting, S.K., and Bose, A., on behalf of UNICEF's cross-divisional task force on child online protection (2020). Encryption, Privacy and Children's Right to Protection from Harm. Innocenti Working Paper 2020-14. Florence: UNICEF Office of Research – Innocenti.

[51] Parliament of India. (2020). Report of the Adhoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and its Effect on Children and Society as a whole. Rajya Sabha Secretariat. New Delhi.; https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf

[52] Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant behavior*, *29*(2), 129-156.

come into play (i.e., a victim may fear retaliating against a popular and stronger pupil who can take further revenge offline).

Because offline bullying often involves physical intimidation or pain, it might be assumed that the severity of harm is greater than for cyberbullying. On the other hand, the affordances of online and mobile communication (such as anonymity, wide audience, difficulty of escaping) might make cyberbullying more harmful. However, research has pointed out that it is associated with a range of psychosocial problems, including affective disorders and behavioural problems including substance use. In order to address cyberbullying, efforts must be focused on addressing the psychosocial problems among children.

Privacy-related risks

The introduction of internet and digital technologies has raised privacy concerns related to the collection and disclosure of personal information of online users including children (also referred to as dataveillance)[53] at varying degrees of user's knowledge and consent. Children are increasingly becoming objects of surveillance through mobile media, wearable devices, social media platforms and educational software. These technologies are being used for recording and sorting various attributes of children such as growth, development, health, social relationships, moods, behavior and educational achievements and effectively turning them into data. Children may engage in these practices themselves, or other actors may do so on their behalf, including their parents, caregivers, friends, teachers and healthcare providers, commercial entities seeking to capitalise on and profit from children's personal information. This is problematic because relying principally on data gathered in this way when making important inferences about children may risk amplifying certain features and/or neglecting certain others. As a result, this might restrict what can be known about them and how they might be treated.

In order to understand what children know and expect about different types of data following are the terms coined in this regard[54]

(a) **Data given** i.e. the data contributed by individuals (about themselves or about others), usually knowingly though not necessarily intentionally, during their participation online;

(b) **Data traces** – the data left, mostly unknowingly– by participation online and captured via data-tracking technologies such as cookies, web beacons or device/browser fingerprinting, location data and other metadata; and

[53] Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, *19*(5), 780-794.

54 Typology coined by a privacy lawyer Simone van der Hof

(c) **Inferred data** i.e. the data derived from analysing data given and data traces, often by algorithms (also referred to as 'profiling').

The different types of data therefore represent different degrees of invasiveness. There are also varying contexts of privacy namely, (i) interpersonal privacy (how my 'data self' is created, accessed and multiplied through my online social connections); (ii) institutional privacy (how public agencies like government, educational and health institutions gather and handle data about me); and (iii) commercial privacy (how my personal data is harvested and used for business and marketing purposes).[55] Children most often and instinctively think of privacy in terms of interpersonal relationships.

Children actively use various privacy protection strategies such as defining their use of a platform based on the platform privacy policy; withholding information; providing fake information, removing content, tags or withdrawing from the internet, customising privacy settings or social circles. They manage the use of communication apps/services based on the nature of their social connections and content of their communication. Other efforts management activities may involve active management of audiences and boundaries, for example, by segmenting friend groups within services and between them or removing and blocking people.

These efforts are more focused on the interpersonal domain and it appears that similar abilities to negotiate their interests in commercial or institutional contexts are limited. This is because their understanding of privacy is less focused on risks related to data mining, profiling or identity theft. In absence of a sufficient critical understanding of how commercial enterprises function, why certain apps/platforms would be interested in them, they will continue to think of data primarily as data given and privacy in interpersonal terms.

Section 43 and Section 66 of IT Act imposes civil and criminal liability for various offences related to data theft and breach of data privacy related offences. These provisions are applicable to body corporate (i.e. organization) or any person.

Children cannot be expected to understand many of the ways in which their data is used, or for what exactly their consent is formally required by an online provider for multiple reasons: complexity of digital interfaces (complex language and little attention to privacy by design); having no meaningful choice to provide personal information (take it or leave it kind of arrangement); and have little understanding of the commercial eco-system (i.e. range of services such as data brokers and profilers that the data collector caters to).

[55] Stoilova, M., Livingstone, S., & Nandagiri, R. (2019). Children's data and privacy online: growing up in a digital age: research findings.

Children have different capacities to understand privacy and different needs which cannot be explained entirely by age. In every age group, there are children with different needs and cognition. In fact, developmental psychology and, indeed, the UN Convention on the Rights of the Child (UNCRC), provides that children must be treated based on their evolving capacities as individuals, taking into account their specific needs, understandings and circumstances. Thus with growing concerns over children's privacy and the commercial uses of their data, it is vital that children's understandings of the digital environment, their digital skills and their capacity to consent are taken into account in designing services, regulation and policy.

The new Personal Data Protection Bill, 2019 (PDP Bill), India, emphasises that children need specific protection regarding their personal data (following similar explicit acknowledgement under the GDPR). The PDP Bill explains when and how consent should be provided for the processing of data, who can provide such consent as well as specific types of processing that will not be permitted in relation to children's personal data. The PDP bill also assigns responsibilities to service providers who collect and process children's data (data fiduciaries)[56] – they are required to verify the age of the child, and ensure that consent is obtained from the parent or guardian[57]. It also distinguishes between service providers who operate online services directed at children, or process large volumes of personal data of children and service providers whose consumers are adults as well as children.

It is pertinent to note that keeping a high age threshold for children's consent may not always be effective. This is because parents are often not familiar with the digital environment; they lack knowledge or skills; or they are simply not interested. Thus, making decisions about children's data for instance, until they are 15 years old would put too much responsibility in the hands of parents. They may also experience serious difficulties in understanding the complexity of modern data processing practices. Additionally, parental consent may result in excessive parental oversight and interference with the lives of children, which could also constitute a breach of children's right to privacy.

With schools moving online due to the pandemic, children's school data has become available across ed-tech apps and communication platforms. Revealing names, home addresses, behaviors, and other personal details about children can potentially be vulnerable to misuse. In May 2020, an Indian edtech service suffered from a data breach - the stolen personal information of millions of users, including that of minor students was put up for sale on Dark Web. Information including user names, passwords, joining date for the programme, last login date, location, email addresses,

[56] Personal Data Protection Bill, 2019 defines "data fiduciary" as any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data

[57] *ibid*

account status (active/inactive), etc, was compromised.[58] Another case of data breach resulted in compromising medical records, photos, passport scans belonging to over 50 thousand students, their parents and teachers[59].

In India, where the legal framework that governs the appropriate uses and disclosures of such data is still in the pipeline (PDP Bill), being mindful of the knowledge and skill gaps of children, parents and teachers – selection of online learning services and establishing their accountability for handling children's data has become critical. The National Education Policy, 2020 (NEP) acknowledges these privacy and data protection needs in use of education technologies however a clear road map of the modalities is not laid down yet (either through the subordinate legislation under PDP Bill or through separate notifications).

Internet Addiction

UNICEF India refers to internet addiction as "excessive use of mobile phones, internet and social networking sites that lead to harmful consequences to a person's physical and mental health and social life."[60] Although people can develop an addiction to these technologies irrespective of their age, this has been a growing concern among teenagers. There is currently no international consensus regarding the conceptualisation and diagnosis of internet addiction. Various terms have been used to name the condition, including compulsive computer use, internet dependency, pathological internet use, problematic internet use, virtual addiction, and internet addiction disorder.[61]

Existing global evidence on prevalence of internet addiction is divided.[62] Some scholars suggest that there is a difference between addictions on the Internet and addictions to the Internet. In other words, whether the problem under discussion is regarding the use of internet as a medium to fuel other addictions or is it addiction to specific online activities (which have their own behavioral addiction patterns ascertained). Several socio-demographic, internet-use related, psychosocial and comorbid factors have been found to be associated with internet addiction. To name a few, family income, gender, age of first exposure to internet, length and frequency of internet use, purpose

[58] Ahaskar, A. (2020 May, 06). Millions of Unacademy user accounts exposed in data breach. *Mint*. Available at https://www.livemint.com/technology/tech-news/over-20-mn-unacademy-user-accounts-exposed-in-data-breach-report-11588775083410.html

[59] Rawat, A. (2020 March 04). Exclusive: Edtech Startup Leaks Data Of Over 50K School Children, Govt Officials. *Inc42*. https://inc42.com/buzz/exclusive-edtech-startup-leaks-data-of-over-50k-indian-children/

[60] UNICEF (2017). Child Online Protection in India. UNICEF India Country Office

[61] J Kuss, D., D Griffiths, M., Karila, L., & Billieux, J. (2014). Internet addiction: A systematic review of epidemiological research for the last decade. *Current pharmaceutical design*, *20*(25), 4026-4052.

[62] Griffiths, M. D., Kuss, D. J., Billieux, J., & Pontes, H. M. (2016). *The evolution of Internet addiction: A global perspective. Addictive Behaviors, 53, 193–195.*

and type of internet use, life-satisfaction and wellbeing levels, existing conditions such as substance use, social phobia etc. are found to be associated with addictive behavior related to the internet.[63]

In a sample of children in India who were recently studied by CRY[64], 34% young people exhibited signs of mild internet addiction, 14 % showed moderate internet addiction and 1 % were suffering from severe internet addiction. This study also observed various factors that were related with prevalence of internet addiction such as ownership of mobile phones, existence of social media accounts, lack of adult supervision of internet use and gender. It was found to have harmful consequences to a person's physical and mental health and social life. The study showed that young people struggled with lack of control over internet usage and anticipation of being online when they were not using their devices and recognized the need for more evidence on whether this was associated with the type of online content being consumed by them.

[63] Griffiths, M. D., Kuss, D. J., Billieux, J., & Pontes, H. M. (2016). *The evolution of Internet addiction: A global perspective. Addictive Behaviors, 53, 193–195.*

[64] Child Rights and You (CRY), 2020, "Online Safety and Internet Addiction (A Study Conducted Amongst Adolescents in Delhi-NCR)", February 2020; New Delhi; The study used Kimberly Young's Internet Addiction Test Instrument to estimate the prevalence of internet addiction.

Part 3 : Online Safety During the Pandemic

Measures to contain COVID-19 has led to widespread social isolation and concerns have been raised about children's development, safety and well-being. While there is little evidence collection on the impact of epidemic containment measures on online abuse and exploitation,[65] school closures have had serious implications for access (socio-economic and gender based inequalities), risks of privacy violation (children's data) and pedagogical challenges.

Online Sexual Exploitation and Abuse– CSAM, Trafficking and Online enticement

An INTERPOL report released late last year[66] provided an analysis about how the COVID-19 pandemic is currently affecting the trends and threats of child sexual exploitation and abuse offences around the world. Several measures taken to control COVID-19 spread in the past year has resulted in closure of schools and movement to virtual learning environments. Children also reportedly spent more time online for entertainment, social and educational purposes whilst not necessarily being aware of any associated risks. According to this report, offenders who usually operate online are likely to increase the amount of time they spend online and continue to adapt and change their online environments to avoid detection and to target platforms based on popularity with children. With restriction of international travel of foreign nationals due to COVID-19 it is anticipated that many may transition their offending to an online environment. Economic hardship of families from COVID-19 and limited access to community support and services that are instrumental in addressing child sexual exploitation, may render children more susceptible to being exploited online.

UNODC 2020 report on Trafficking in Persons[67], has concluded that COVID-19 measures around the world such as lockdowns and travel restrictions would likely drive human trafficking further underground and cause traffickers to adjust their business models especially through the use of the internet and modern communication technologies to advertise, recruit and exploit children. NCMEC has also reported a rise in the number of reports from cases of CSAM, child sex trafficking and online grooming in the last year as compared with pre-Covid times. CyberTipline figures revealed increase from 1.9 million to 2.7 million cases across these categories from India alone[68]. The Ministry of Home Affairs (MHA) has taken note of the situation and issued an advisory[69] to the states and union territories to strengthen facilities for vulnerable groups in particular, using several

[65] Bakrania, S., Chavez, C., Ipince, A., Rocca, M., Oliver, S., Stansfield, C., & Subrahmanian, R. (2020). Impacts of Pandemics and Epidemics on Child Protection: Lessons learned from a rapid review in the context of COVID-19.

[66] (2020). Threats and Trends Child Sexual Exploitation and Abuse, COVID-19 Impact, INTERPOL.

[67] (2020). Global Report on Trafficking in Persons 2020, United Nations Office of Drugs and Crime.

[68] Figures available at https://www.missingkids.org/gethelpnow/cybertipline

[69] Ministry of Home Affairs. Women Safety Division. (2021). Advisory on Protection of Vulnerable Sections of Society such as Women, Children, Senior Citizens etc. available at https://www.mha.gov.in/sites/default/files/advisory_21052021_0.pdf

National Crime Records Bureau (NCRB)' s digital tools like Crime Multi Centre Agency (Cri-MAC) to share inter-state information within the police network, Crime and Criminal Tracking Network & Systems (CCTNS) to track missing individuals and UNIFY, an automated photo matching web-based application, to search for images of missing persons and unidentified bodies. While this is a welcome measure, much needs to be done in cooperation with social media platforms and other internet and financial companies whose services are facilitating exploitative transactions.

Online Learning & Access

School closures have raised concerns regarding breaks in learning due to inadequate digital access, capacity and infrastructure challenges for teaching online effectively. Furthermore, there are increasing concerns regarding use of children's data especially by online communication services (like whatsapp) and education technology applications to facilitate online learning.

As a response to school closures, diverse e-learning and digital initiatives have been launched by Union and State governments. However these need to be studied against the backdrop of the most recent National Sample Survey (NSS Report)[70] which highlights that about 23.8 per cent of Indian households have internet facilities: in rural areas only 14.9 per cent of households have access to internet facilities, while in urban areas this is significantly higher at 42 per cent. Only one out of every five Indians are able to use the internet (20.1 per cent), with rural figures at a low 13 per cent compared to 37.1 per cent for urban citizens. Among mere 13% of people surveyed (aged above five) in rural areas just 8.5% of females could use the Internet. In fact, a recent NCERT study[71] reveals that 27 per cent of students do not have access to smartphones or laptops to attend online classes. Therefore, a transition to online learning has been reported to be particularly challenging for the lower socio-economic classes and rural areas in the country.[72]

Inadequate digital access has been attributed to poor connectivity, expensive mobile data, lack of smartphones, and lack of skills in using the internet. Research also points out that school closures hit more marginalized groups much harder in terms of lower learning outcomes and even dropouts – these groups included students with disabilities, socio-economically disadvantaged students, or those in remote locations with limited access to basic services and infrastructure). In underprivileged families, in comparison to boys, girls have decreased access to gadgets is gendered

[70] National Sample Survey (2019) Key Indicators of Household Social Consumption on Education in India 2017-18, Ministry of Statistics and Programme Implementation, Government of India.

[71] National Council of Educational Research and Training (2020) 'Students' Learning Enhancement Guidelines', New Delhi: Ministry of Human Resource Development, Government of India.

[72] Favara, M., Freund, R., Porter, C., Sánchez, A., Scott, D. Young lives, interrupted: Short-term effects of the COVID-19 pandemic on adolescents in low- and middle-income countries. *Covid Economics* 2021, 67:172-198.

and this is likely to reduce the involvement in digital platforms of education and makes them more vulnerable to dropping out.[73]

The success of online education is dependent on the infrastructure available and teachers' familiarity with distance learning tools already in place. The NEP, 2020, recognises the importance of technology in aiding teachers, creating digital libraries and ensuring greater access to education. It envisages the development of digital infrastructure, digital content and capacity building to supervise the e-education needs of both school and higher education. In fact the MHRD has taken measures to establish platforms like Diksha for learning from content created by CBSE, NCERT and states/UTs for students as well as teachers. Similar platforms such as Swayam serve both high school and higher education students with close to 1900 courses across multiple disciplines. Further, these platforms are available not only across digital devices (laptop/mobile/desktop/tablets, TV and radio) but also across TV channels (for Swayam content) thus facilitating coherence of access and learning experience.[74]

While the NEP notes the existence of limited or no access to exclusive digital devices/ internet/ or even electricity it is imperative that these concerted efforts are supplemented with access to basic services such as power supply as well as awareness about the use of digital technology. All teaching-learning transactions must be within the framework of robust child protection policies which includes a component on cyber-safety of children and responsive grievance redress mechanisms. Further, given the existing digital infrastructure and the needs of marginalized students, emphasis must be placed on using low-tech solutions such as radio/television and distributing printed materials where digital penetration is limited.

Privacy Risks

Increased use of communication and ed-tech apps for online learning has also raised concerns about personal data of students (discussed briefly in an earlier section) - who has access to the data, how it is being used and whether it is being kept safe. Many apps include learning analytics that helps track student progress and this data could be identifiable. These technologies have previously posed privacy problems.[75] Certain documented data practices include

[73] Oxfam India. (2020). *Status Report – Government and private schools during COVID-19, 'Findings of rapid surveys*; Kumar, A., Nayar, K. R., & Bhat, L. D. (2020). Debate: COVID- 19 and children in India. *Child and adolescent mental health*, *25*(3), 165-166.; Favara, M., Freund, R., Porter, C., Sánchez, A., Scott, D. Young lives, interrupted: Short-term effects of the COVID-19 pandemic on adolescents in low- and middle-income countries. *Covid Economics* 2021, 67:172-198.

[74] Ministry of Human Resource Development, Department of School Education & Literacy, (2020) India Report Digital Education: Remote Learning Initiatives across India at https://www.education.gov.in/sites/upload_files/mhrd/files/India_Report_Digital_Education_0.pdf

[75] Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education*, *16*(3), 263-279.; Regan, P. M., & Steeves, V. (2019). Education, privacy, and big data algorithms: Taking the persons out of personalized learning. *First Monday*.

corporate tracking of student activities both inside and outside of the classroom, discrimination against young people from marginalized communities, student loss of autonomy due to ongoing monitoring of their activities and sale of student data to third parties often for purposes of advertising to them.[76] It is noteworthy that schools are often not aware or skilled to understand the range of privacy implications of online learning and what makes matters worse is the complexity, length and vagueness of privacy notices and terms of service.

In India, there was no legislation specifically addressing children's data related privacy issues until the introduction of the PDP Bill, 2019. This PDP bill deals with children's data privacy, along with issues around children's use of online services including educational apps, the role of service providers[77] and restrictions on profiling of children's data. These service providers potentially include schools, and ed-tech companies. These institutions cannot profile, track or monitor the behavior or use targeted advertising on children under the bill. There are restrictions on processing children's data that causes significant harm and carries heavy penalties for violation. Further all technology companies which may not be directed at children but are used by them must process their data in their best interests. The bill creates ambiguity regarding understanding of best interests or what constitutes significant harm and such other terms for these provisions to be effectively implemented.

The National Human Rights Commission has published an advisory[78] to address these challenges with online learning which includes following the PRAGYATA Guidelines on online education, regulating ed-tech and other relevant digital platforms offering online classes, raising awareness among teachers and parents about online safety and privacy risks and related reporting and redressal mechanisms. NHRC advisory also directs the state governments to adopt a blended approach to education to ensure that the marginalised groups are not excluded from learning.

[76] Straus, V. (2019, August 20). Legislators ask 50-plus firms to explain how they use the 'vast amount of data' they collect on students. *Washington Post.*
https://www.washingtonpost.com/education/2019/08/20/legislators-ask-plus-firms-explain-how-they-use-vast-amount-data-they-collect-students-which-ones-facebook-google-blackboard-etc/

[77] Entities that operate commercial websites or online services directed at children or entities that process large volumes of personal data of children (called guardian data fiduciaries under the PDP Bill)

[78] (National Human Rights Commission, 2020 AND 2021)
https://nhrc.nic.in/sites/default/files/NHRC%20Advisory%20on%20Children%202.0.pdf ;
https://nhrc.nic.in/sites/default/files/NHRC%20Advisory%20on%20Children_0.pdf

Mental health and Online risks

Due to lockdown, limited opportunity for socialization may also affect the psychological state of children adversely. This may lead to increased loneliness, mood to conduct disorders, substance abuse or anxiety disorders. And they may be pre-disposed to using internet compulsively, accessing objectionable content or simply be more vulnerable to getting bullied or abused.[79] The quality and magnitude of impact of these measures on children is contingent on diverse factors like developmental age, educational status, pre-existing mental health conditions, economic status. The NHRC advisory suggests that state governments must develop human resources for providing emotional first aid at district level and make mental health services more accessible to all children with the help of local civil society organisations. In this regard, MHRD has developed an online repository of resources for children and their primary stakeholders to cope with mental health challenges resulting from the pandemic control measures.[80]

Protection Risks to children without parental care

The Covid pandemic has claimed close to 4 lakh lives in a little over one year, and the figures are still escalating with each new wave. Several children have lost either or both parents or been abandoned. This has led to a phenomenon of posting information about such children along with their identifiers on various social media platforms using various hastags related to children orphaned during the pandemic (like #covidorphans) along with adoption appeals. This poses threats to child protection in several ways- 1) the tag tends to label and stigmatise children who have been orphaned during this pandemic which could lead to long term emotional consequences for children, 2) It risks children's safety as the identifiers might enable traffickers and other perpetrators easy access to already vulnerable children, 3) many adoption appeals tend to reiterate caste, class and gender bias that exists across India's social fabric, 4) Most importantly, it is in complete violation of the existing law of the land.

The Ministry of Women and Child Development as well as the National Child Rights Commission has responded by issuing directives and guidelines to state governments on adhering to provisions of the Juvenile Justice (Care and Protection of Children) Act, 2015 and linking them with mechanisms available under the Integrated Child Protection Scheme. The Bal Swaraj- Covid Care portal especially aims at tracking the children affected by COVID-19 right from the production of children before the Child Welfare Committee (CWC) to the restoration of the children to their parent/guardian/relative and its subsequent follow-up.

[79] Kumar, A., Nayar, K. R., & Bhat, L. D. (2020). Debate: COVID- 19 and children in India. *Child and adolescent mental health*, *25*(3), 165-166.; Favara, M., Freund, R., Porter, C., Sánchez, A., Scott, D. Young lives, interrupted: Short-term effects of the COVID-19 pandemic on adolescents in low- and middle-income countries. *Covid Economics* 2021, 67:172-198.; Singh, S., Roy, M. D., Sinha, C. P. T. M. K., Parveen, C. P. T. M. S., Sharma, C. P. T. G., & Joshi, C. P. T. G. (2020). Impact of COVID-19 and lockdown on mental health of children and adolescents: A narrative review with recommendations. *Psychiatry research*, 113429.

[80] Manodarpan, a Ministry of Education initiative to provide psychological support at http://manodarpan.mhrd.gov.in/

Recommendations

The ultimate goal of building a protective online/offline environment for children must be to create the greatest possible opportunity, without marginalisation or exclusion of certain groups, to take advantage of the benefits offered by the online environment, while simultaneously minimising risks and potential harm in that environment. It requires understanding and addressing the risk of abuse that children across different age groups face. Key recommendations on cyber safety of children have been framed with this objective of achieving balance, preventing harm and strengthening redressal.

A. Addressing gaps in law and policy through cohesive policy discourse

There is a need for cohesion between forums for internet governance policy and child protection on the existing discourse on children's digital rights. The Ministry of Women and Child Development (MWCD) has a crucial role in facilitating this discourse. This will help in addressing the gaps in legislative and policy measures on several cyber safety issues such as criminalization of cyberbullying and sexting among peers and categorisation of self-generated images as CSAM.

Additionally, measures to resolve the circulation of CSAM is primarily regarded as a content regulation issue (MEITY) and/or a cybercrime issue (Ministry of Home Affairs). While addressing the CSAM issue through these lens is necessary, it is critical to prioritise the underlying sexual abuse and the urgency to identify and rescue the child victim of such abuse which is often sidelined in this debate as well as the resulting re-victimisation. This latter aspect underscores the need for contribution from the child protection stakeholders (such as Police, NCPCR and MWCD) to decide policy measures that facilitate disclosure and reporting, as well as ensure victim support and rehabilitation in accordance with the best interests of the child victim.

The data protection policy of the country must underscore the child protection principle of evolving capacities of a child and the decisional autonomy of late adolescents in the use of online services/platforms. In another instance where cohesion between child protection and data protection is critical – is in drawing a distinction between educational entities such as schools and ed-tech application providers for the purpose of clarifying where safeguards are needed for data collection and processing. On the other hand, policy discussions on child protection issues (for instance, child sexual abuse) are also not adequately informed about the implications of the increasing pervasiveness of internet in children's lives and how this evolves or amplifies the conventional/traditional/offline forms of child abuse.

There are also specific issues at the intersection of child protection, education and cybersafety. For example, there is urgent need to have clear guidelines and parameters for selection of online learning and communication applications to ensure that children's data is being collected and processed responsibly. The MHRD may develop these parameters in consultation with education boards, civil society stakeholders and technology experts. However, the MHRD may collaborate with MEITY in order to address the challenges in ensuring inclusive online learning in the country.

B. Addressing enforcement challenges through capacity building

Law enforcement

There is limited specialist expertise among local law enforcement officials to tackle online child abuse and exploitation in terms of reporting, investigation, evidence handling and child sensitivity. While officers who are likely to investigate or respond to crimes against children undergo mandatory training for child protection laws (POCSO 2012 and Juvenile Justice Act, 2015), they tend to divert all cases with an internet element to cyber cells which only have 1 or 2 officers who are likely to have overload of cases and resulting delays. This also has implications for centralisation of investigation skills to a few officials. There is inadequate training and technology for handling as well as ensuring admissibility of digital evidence. It is noteworthy that cybercrime police departments are often focused on fraud and organized crime and may therefore have little or no expertise, or professional interest, in child protection. Child online sexual exploitation for example is often seen as a cybercrime/organized crime by such officers which misrepresents the nature of offending. These trainings are necessary to decentralize the investigation of online offences against children and also deliver a child-centred response to these cases.

The Bureau of Police Research and Development (BPR&D) under the MHA is responsible for addressing the capacity needs of the law enforcement in the country to tackle crimes effectively and has taken some measures in this regard. However much needs to be done to scale up these capacity development measures at the district level.

Child protection functionaries

Child protection workforce that provides victim support such as helplines and functionaries appointed under the Integrated Child Protection Scheme (ICPS), village child protection committees, in the country, are best placed to help child victims of online abuse and exploitation. But they do not have access to adequate knowledge and training to support and rehabilitate such victims. Specialised facilities for counselling and rehabilitation that are available in the country have limited outreach (concentrated in urban areas). A few NGO initiatives respond to the needs of victims of child online abuse and exploitation, but this is barely sufficient. These actors can be trained and mobilized through interventions developed by the MWCD in collaboration with civil society organisations to address not only those online threats that translate into legal offences but also other aggressive and sexual risks that are not illegal but nevertheless have an adverse impact on children. These stakeholders can also play a critical role in prevention and awareness of online safety concerns.

C. Empowering children and their eco-systems - Education and Awareness

Parents and Teachers

There is limited understanding among caregivers, educators and society regarding children's experiences with ICTs and perceived risks that they face online. There is a need to help caregivers, educators and parents to understand what children should know so as to be able appropriately and responsibly and be able to guide them. The existing awareness building programmes lack common content focus, are fragmented and have limited outreach. There is a need for a coordinated approach for equipping children, caregivers, teachers and public with skills for safeguarding against online threats and being responsible digital citizens.

The MOE may develop the requisite policy interventions to address these knowledge and skills gaps. Interventions for capacity building of teachers must be developed to equip them with specialised knowledge and skills relating to internet and its intersections with child development, associated risks and opportunities and channels of redress and support. It is also imperative that these interventions are institutionalized. Cyber Safety focused curriculum must be made available to all the teachers as part of pre-service and in-service training programmes. Similarly, parenting programmes must also be developed that are directed at providing guidance to Indian parents to engage with their children and help them navigate this medium more effectively. Civil Society organizations can support government in the awareness generation and teacher training efforts.

Children

The assumption that children are digital natives bears little relation to the everyday experience of hundreds of millions of rural and/or working-class children in India. Thus, developing programs for children for age-appropriate life skills education which incorporate the understanding of problems in the online context would be more useful than digital literacy/citizenship interventions. At a policy level, there is a need for a clear mandate (that must be established by NCPCR and MOE in collaboration with civil society) to identify and develop the interests and concerns of children as stakeholders in the use of ICTs that will fill the cracks and bridge the existing disconnected policy dialogues. Children's life skill training programs must also include cyber literacy and cyber safety related issues.

D. Developing evidence base for informed policy and public awareness

The data on the extent, pattern and trends of children's usage of digital technologies in the country is patchy. Most of the research on children and young people's internet use and related risks is from the global north based on data about the lives of children living European childhoods. Studies are generally situated in densely mediatized North America, Europe, Australia-New Zealand, Japan, South Korea and materially well-off parts of Asia, Africa and Latin America. Often, several policies and programmes designed in the global south rely on this type of research. Access to the internet is increasing but the actual impact of internet on abuse & exploitation against children in the country remains unknown. There is research done on small samples by academic institutions that is indicative of certain trends in children's interface with internet keeping in mind class, caste, religion and gender context in the country. The MWCD, NHRC and NCPCR may take measures to develop a research agenda to explore various online safety issues in Indian context as well as children's experiences with internet and their perception of risks and harm related to their online activities.

E. Augmenting Budget for Children as a Proportion of Union Budget

The MWCD, MHA and MHRD may require development of effective budget plans to implement the aforementioned recommendations. It is critical that this budgeting exercise is undertaken in light of the changes in the share of the child budget (as a proportion of Union Budget) in the last few years. This year, the budgetary allocation for children is 0.38 % of GDP. As proportion of union budget it is the lowest in the last 10 years; it has reduced by 2.05 percentage points from 4.51% (2011-12 BE) to 2.46% (2021-22 BE). An analysis of component-wise allocations reveals that other than child health which saw an approximate increase of 15%, all other sectors including child protection have seen a decline. Allocations for child protection in fact, have taken the biggest hit with a drop of more than 40%. With increasing emphasis of online and blended models of education in a climate of growing safety concerns for children, government efforts can only be realized if backed by adequate budgetary allocations.

Conclusion

Internet has created another dimension for child protection issues thus online risks and harm must be understood within the context of larger child protection landscape in the country/region. This implies that the response and prevention strategies can be implemented with the existing child protection structures. There is thus a critical need to integrate our understanding of this new medium and what it brings to the child protection issues with existing ideas, capacities and resources. It is imperative that the approach to resolving child online safety issues effectively must be multi-stakeholder and multi-sectoral thus including a diversity of governmental and non-governmental actors across a range of spheres. The policy discourse on children's online safety in India is in its nascent stages in the internet governance as well as child protection policy forums. Technology solutions are no silver bullet to resolve online safety issues; they may reduce the prevalence of online harm but these solutions cannot create safe spaces without the right policies, upskilling of the existing child protection workforce and user empowerment.

There are however a few reasons for exercising caution with developing and implementing online safety policy in the country. For the policies to be effective they must be evidence-based, pointing to the urgent need to do so, in order for policies to be relevant to India. Child cyber safety policies tend to be based on adults' perception of risks and harm and consequently tend to become paternalistic, preachy and ineffective. Evidence gathering efforts must include and encourage child participation so that policies can truly reflect and respond to children's perspectives of their lives online and what they perceive as risky. This should cover children perspectives from various sections i.e. privileged, vulnerable, rural, urban, male, female, etc.

Along with child centric and child friendly laws and policies what is very much important is supportive supervision and guidance from parents and caregivers at home in promoting opportunities and benefits and curbing risks and harms among the adolescents. Focus should be given on making them aware about cyber safety rules and the programmes should be developed to build their skills on safe cyber usage. Talking about sex and sexuality is still a taboo in our society. In small family conversations and school curriculum must have concepts on 'reproductive and sexual rights education' along with cyber-safety rules and life-skills education.