WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

PROTECTING CHILDREN IN THE DIGITAL ECOSYSTEM: CHALLENGES OF AI SURVEILLANCE UNDER DATA PROTECTION LAWS

Shipra Saini[1], Dr. Parneet Kaur[2]

[1] student (LLM), UILS Chandigarh University.
8433499281, shiprasaini525@gmail.com
Tagore Garden, Paper Mill Road, Saharanpur, Uttar Pradesh.
[2] Assistant Professor, UILS Chandigarh University
9876500693, parneet.uils@cumail.in

ABSTRACT :

In the digital age, children have become near experts at immersing themselves in the online realm to do their homework, socialize, and watch movies in large quantities. Nevertheless, each step they take is being followed by layers of endless surveillance and data mining. Artificial Intelligence (AI) surveillance systems, such as facial recognition, behavioural tracking, and algorithmic profiling, operate silently behind every day digital activities, gathering vast amounts of personal data. The AI-driven technology is everything about monitoring and estimating our behaviour on a regular basis. To children, that presents an ethical nightmare: their information is being used to guess what they like, dislike or want to do even before they can identify what profiling is all about. The fact that little users are powerless, and whoever is in charge is it the gov, a big Corp, or an e-learning platform, is but to make it worse. Children are not in a position to make informed consent, but their online histories are being commercialized, hoarded, and exported to foreign nations. It is not a temporary invasion of privacy, but the harm to the digital identity and right to thoughts of a child in the long term is the threat. In this paper, the author examined the existing legal frameworks in detail, i.e., GDPR provided by the EU, the Digital Personal Data Protection Act of 2023 in India, and the UNCRC. Not only that, the insider status of algorithms makes it difficult to track how the data of children is collected or utilized, creating large accountability gaps. The article concludes with the statement that ensuring the safety of youngsters in the age of AI implies not only legal changes but also another ethical commitment to safeguard childhood as a secure, trustworthy, and unadulterated location.

KEY WORDS: AI Surveillance, Children's Privacy, Digital Ecosystem, Data Protection, Online Safety, Algorithm Accountability.

INTRODUCTION

Digital ecosystem is not just an aspect of contemporary childhood, but it is almost impossible to separate them at this point. On a daily basis, children are out here clicking smartphones, tablets, and laptops, and conversing with voice assistants due to school, chill videos, and chatting. However, there is a silent price in this slick technological feel, and that is always being looked at. The high-tech surveillance of the AI was insidiously introduced into our cyber-environment, where it follows all our movements, combines trends, and collects personal information into huge reservoirs. That clever addiction makes children the most observed and susceptible generation of cyberspace.

Artificial Intelligence or AI is simply computers that are capable of performing tasks that human beings normally perform- learning, reasoning and problem-solving.[1] AI surveillance involves methods that involve algorithms and automated systems to monitor, collect and analyse human behaviour of the internet or even in real life. it includes facial recognition, biometric log-ins, voice identifications, GPS positions, and behavioural analytics. The systems continue to snap in the actions of people on the internet, usually anticipating what is interesting or what they will choose, even before they can consider it. In the case of kids, AI surveillance follows kids everywhere on their social media (YouTube, Instagram, TikTok, etc.) and gaming platforms (Roblox, Fortnite, etc.), mining the information that kids leave behind to customise their content and advertising. Children are also taking home smart devices, namely Alexa, Google Home, smart TV, tablets and wearables, which are constantly listening, following and obeying orders.[2] What seems to be innocuous technology aiding with homework or video games is actually a bunch of algorithmic whirling and profiling, which the majority of children (and people around them) do not understand. Since children are immature with little knowledge, brain development, and legal analysis, they are among the most vulnerable in the digital era. They have a very slim understanding of how data is gathered and the consequences of disclosing personal data.[3] Their behaviour on the internet, whether it be posting pictures, using learning applications, or binge-watching videos, generates massive data sets that are

[1] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn Pearson 2021).
[2] Sonia Livingstone and John Carr, *Children and Young People's Rights in the Digital Age* (UNICEF Discussion Paper, 2021).
[3] United Nations Convention on the Rights of the Child, (1989) art.21.

being used to forecast and influence behaviour by companies. Children, unlike adults, are unable to provide the real informed consent, being easier to manipulate, exploit, and suffer privacy invasion. Sometimes, even AI algorithms support poor stereotypes or expose underage people to dubious content, which increases emotional and mental vulnerability.

Existing regulations, such as the GDPR in the EU and the Digital Personal Data Protection Act 2023 in India, highlight the necessity to safeguard the information of kids. Nevertheless, AI has evolved too fast and presents loopholes in these laws. Although they emphasize consent and legal processing, they fail to address the ambiguity of AI algorithms and the use of the digital trails of kids in commerce entirely. It is not only the stricter laws that will help, but also creating ethical accountability, transparency and educating all people so that the tech can truly empower people rather than command them around.

DIGITAL ECOSYSTEM & AI-SURVEILLANCE

The tech world is infused in every aspect of our lives and the digital world is a support system of childhood. Children are no longer only learning in virtual classrooms, but they are also playing games, chatting and talking to intelligent assistants; in other words, they are exploring a world that operates on information and algorithms. However, even as convenient as that tech is, there stands a dark cloud associated with it: AI surveillance silently decides to follow, capture, and forecast every action. It is very important to figure out how this surveillance works to ensure that the rights, independence, and privacy of children are safeguarded in the current world.

UNDERSTANDING THE DIGITAL ECOSYSTEM

The modern digital environment is massive: a labyrinth of interconnected devices, social networks, and individuals that share information 24/7. It also covers social media, cloud platforms, e-learning tools, and smart home devices.[4] In that web, information has literally become the new currency, mined, stored and processed by both businesses and states. As active users, children post personal information in huge quantities in this area without clearly understanding the repercussions in the long term. What once was a playground of creativity and communication has turned into a sophisticated marketplace where every click, voice command or viewing habit is tattooed into a dataset. AI lays at the centre of this change. The technology makes systems learn, reason, and adapt, that is, simulate human intelligence; however, that capability is becoming embedded in our daily existence, resulting in AI-based surveillance that brings both convenience and constant observation.

AI SURVEILLANCE TECHNOLOGIES: THE INVISIBLE OBSERVERS

AI-based surveillance refers to automated systems that observe, analyse and predict human behaviour with the use of data-driven algorithms. Imagine facial recognition, biometric identification, emotion detection, predictive analytics, and algorithmic profiling.[5] These capabilities are hidden in our interactions with digital footprints every day. Such apps as Instagram, YouTube, Snapchat, and TikTok apply AI to personalise feeds, identify faces, and track interactions. Learning speeds, attention, and emotions are measured with the help of similar tech by educators and game developers, which customises the experience. Smart devices- Amazon Alexa, Google Home, smart TVs, wearables, etc., go further to record voice, sleep, heart-rate and even location in constant motion, collecting data on kids without their knowledge. That information conditions algorithms that anticipate preferences and influence what children watch, listen to, and think, slowly diminishing their freedom and privacy, putting the boundary between aiding and asserting in a grey area.

VULNERABLE GROUPS IN THE DIGITAL AGE: THE CHILD AS A TARGET

Among all the internet users, kids are the most susceptible. They are technologically uninformed, their thinking is not fully formed, and they are dependent on the online environment; thus, they become the targets of surveillance and exploitation.[6] The AI platforms monitor emotions and habits, and the information is used to recommend content that draws attention and influences decisions. Auto play videos, gamified learning tools, and all interactions have a digital footprint that companies use to get money. This commodification monetises curiosity. The asymmetry between data authorities (companies and governments) and children suggests the importance of immediately regulating data usage by rights. Children with disabilities or whose socio-economic status is marginalised particularly face a high risk. They are more vulnerable to the additional surveillance of being dependent on digital tools to be accessible or learn, which doubles the vulnerability.[7]

PSYCHOLOGICAL AND EMOTIONAL IMPLICATIONS OF SURVEILLANCE

The psychological implication of AI surveillance on children is a reality. The continuous monitoring and customization to the work of the algorithms may influence emotional experience, self-perception, and behaviour. By making children think that everyone is watching them, algorithmic profiling may create the sense that everyone is watching them, cause social pressure and lack of freedom to express oneself, and also reinforce stereotypes, echo

[4] OECD, The Digital Transformation: Implications for Children's Rights (OECD Report, 2022).

[5] General Data Protection Regulation, Regulation (EU) 2016/679, 2016, art. 8.

[6] Supra note 3.

[7] Shoshana Zuboff, The Age of Surveillance Capitalism (Public Affairs, 2019).

chambers, and alter a child's worldview, albeit subtly and persistently.8 Not only do the effects of exposure to manipulative ads or biased advice influence the decision but also identity and independence, which have extensive consequences on mental health, emotional stability, and personal agency.

BALANCING BETWEEN ENSURING SAFETY AND INVADING PRIVACY

Governments, schools and parents constantly argue that AI surveillance is a security feature to ensure that kids are unreachable by cyberbullying, predatory content online, and other harmful materials. However, it is a true challenge to strike the right balance between ensuring the safety of kids and their privacy. In some way over-monitoring can ensure the physical safety of kids, but it can also damage their psychological development and emotional autonomy. With the development of AI technologies in the classroom and home (including facial recognition applications and learning analytics), the boundary between useful and intrusive has become unclear. The responsibility of how their kids use the Internet should be undertaken by the parents; rather than spying on their children, they must encourage transparent communication, develop digital literacy, and foster responsible usage of the technology based on trust and not control. On the same note, schools, as the custodians of the digital world, should ensure that the tech they use does not violate data protection regulations and ensure that the information is confidential. Educators should introduce digital ethics classes to learners to learn about privacy, consent, and data rights on the Internet. A balance between that requires collaboration between parents, educators, and policymakers so that AI surveillance does not hinder but actually safeguards the online lives of kids.[9] Protecting the privacy of a child is not only a legal obligation but also a moral requirement to the cognitive and emotional health of the child.[10]

STATUTORY FRAMEWORKS

The safety of the data and privacy of children in the cyber ecosystem are largely reliant on effective legal frameworks. The arrangements provided by different international and national legislations that govern the process of gathering, processing and disseminating personal information in relation to minors in particular. General Data Protection Regulation (GDPR), the United Nations Convention on the Rights of the Child (UNCRC), and India's Digital Personal Data Protection Act, 2023 provide us the legal emergency to ensure that tech is used in the best interest of kids as well as ensuring that their fundamental rights are not violated, despite all the AI surveillance all around us.

INTERNATIONAL FRAMEWORKS

The entire privacy and data security problem of children in the digital realm is, in fact, a result of a series of international laws, which prioritise the need of the child to dignity, autonomy, and safety.

United Nations Convention on the Rights of the Child (UNCRC), 1989

The UNCRC is fundamentally the staple of global child-rights protection. It provides us with the initial global legal framework to safeguard the privacy, dignity, and safety of children worldwide, including on the Internet. Article 16 states that no child will be hampered with the arbitrariness or illegitimacy of his or her privacy, family, home or correspondence[11], and in the case of AI-surveillance, it addresses the threat of misusing the data of kids to engage in algorithmic profiling, tracking, or internet exploitation. Article 17 also challenges states to both allow children to receive trustworthy information and ensure that children are not exposed to dangerous information, a massive task when artificial intelligence filters the content and recommender systems[12]. Likewise, Article 34 asks them to safeguard children against sexual exploitation and abuse, which now extends into digital grooming and cyber-exploitation and non-consensual sharing of images, also provides the basis upon which governments and platforms can act morally and legally in the world of AI[13].

UNRC General Comment No. 25(2021) on Children's Rights

To have the UNCRC work in the digital age, the UN Committee on the Rights of the Child provided us with General Comment No. 25 (2021), an authoritative backdrop on how states ought to online the Convention.[14] It acknowledges that the digital environment controls all aspects of the lives of kids, such as schooling, social media, gaming, and their rights must be fully acknowledged, including privacy, data protection, and informational autonomy, which can subjugate or exploit the weaknesses of a child[15]. In addition, the comment highlights transparency, accountability, and engaging children in the policy-making process to give them a platform to speak out through the age of AI and digital surveillance.

OECD Guidelines on privacy and children

To supplement the UN system, the OECD intervenes and provides concrete international values on ensuring privacy and personal data protection. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, revised 2013) established the principles of modern data-

[8] UNESCO, Artificial Intelligence and the Rights of the Child (UNESCO Policy Brief, 2021).

[9] Supra note 5.

[10] Supra note 3.

[11] Supra note 3, art. 16.

[12] Id., art. 17.

[13] Id., art. 34.

[14] Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment (UN Doc CRC/C/GC/25, 2021).

[15] Ibid.

protection norms, purpose limitation, data minimisation, accountability, and privacy-by-design systems, the absence of which means that children have their data abused across borders[16]. It also encourages corporate responsibility, which encourages digital platforms and AI developers to prioritise ethics rather than prioritising the rights and well-being of children. Through a combination of the UNCRC and the General Comment No. 25, and the OECD Guidelines, a thorough international blueprint on protecting the digital privacy of kids, but at the same time promotes a safe and equitable online environment[17].

General Data Protection Regulation (GDPR),2016

The General Data Protection Regulation (EU) 2016/679 is the largest global privacy and data protection standard. It specifically identifies children as a vulnerable group who should be subjected to increased protection. Article 8 requires that the right to process the personal data of a child to enable online services is legal when the consent is given or authorised by the holder of parental responsibility, where the child is less than sixteen years old (Member States may fix such age between thirteen and sixteen)[18]. This helps to prevent child manipulative consent tools and unscrupulous profiling. More so, the GDPR under Articles 5 and 6, lays out the principle of data minimisation, purpose limitation, and lawful processing, which prohibits the uninhibited application of AI systems collecting children's behavioural or biometric data, or making predictions based on data patterns.[19] Article 22 is especially applicable, where individuals (including minors) have the right not to be subjected to automated decision-making, such as profiling, which has significant effects[20]. Through incorporating accountability, transparency, and personal rights, GDPR creates a rights-based framework that is forcing AI developers, educational institutions, and digital service providers to implement privacy-by-design approaches that are more caring and rights-oriented towards children.

NATIONAL FRAMEWORKS

Although the foundation of ensuring the digital rights of children is provided by international conventions, national legislations are important in ensuring that such principles are translated into domestic norms that are enforceable. India and the European Union have implemented data protection laws that are aimed at controlling the gathering, manipulation and retention of personal data, including that of minors. In this section, the author discusses the General Data Protection Regulation (GDPR) of the European Union, India Digital Personal Data Protection Act, 2023 (DPDP Act), and the applicable provisions of the Information Technology Act, 2000, which all seem to be the origin of the complicated relationship between AI surveillance, data privacy and child protection.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, by India is a major step towards the digital rights and privacy of the country. The Act presents consent-based data management, which is similar to global standards. Section 9 of the DPDP Act specifically safeguards children, banning the treatment of personal data likely to harm minors and banning targeted advertising or tracking of a child before such information is processed by the algorithm is a critical protection in educational applications of AI, game apps, and social media spaces[21]. Further, Section 4(1) specifies that the personal data should be used only in legal ways, whereas Section 6(1) focuses on the principle of consent, which presupposes that people (or their representatives) should control their data[22]. But, there are still certain difficulties in the effective use of these aspects because not all Indian digital platforms have age-verification systems and clear AI data policies. Though progressive, the DPDP Act nevertheless introduces uncertainties as to automated decision-making, AI profiling and inter-country transfers of data, where the information of children may be especially vulnerable. However, the law provides a crucial basis to the future legislative trends that would help address the gap between innovation and child safety in the digital ecosystem.

The Information Technology Act, 2000

The Information Technology Act, 2000, used to be the main law regulating the activities on the Internet and the security of data before the introduction of the DPDP Act. Although not initially created to deal with AI and children's data, some of its provisions indirectly protect the minor. Section 43A makes the companies liable in cases of negligence in the processing of sensitive personal data, and therefore, covers privacy violations that may arise through unsafe AI systems[23]. Section 66E criminalises breaches of privacy by the capture or transmission of images of a private area without prior consent, which is essential in addressing AI-controlled surveillance or the use of facial recognition in cases of child abuse[24]. Sections 67A and 67B penalise the publication or transmission of sexually explicit or child sexual abuse material (CSAM), which would be crucial in addressing cases of AI[25]. The IT Act and the DPDP Act are two components of a two-tier system that can be developed depending on new technologies, yet the enforcement has to be child-centred.

---

[16] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980, updated 2013) (Organisation for Economic Co-operation and Development, Paris).

[17] Global Privacy Assembly, *Resolution on Children's Digital Rights* (2021).

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council, *General Data Protection Regulation*, art. 8 (2016).

[19] *Id.*, arts. 5-6.

[20] *Id.,* art. 22.

[21] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 9.

[22] *Id.,* ss.4(1), 6(1).

[23] The Information Technology Act, 2000 (Act 21 of 2000), s. 43A

[24] *Supra* note 23*.,* s.66E.

[25] *Id*., ss.67A–67B.

COMPARATIVE ANALYSIS OF DATA PROTECTION FRAMEWORKS

The worldwide effort towards realising the data privacy laws reveals how other legal traditions and policy objectives influence the rules. consider the EU, the US, and India - they all have a free hand, particularly in the area of privacy of kids on the internet. The GDPR of the EU is everything about the rights-based, comprehensive supervision. The COPPA of the US is more sector-compliant. The DPDP Act of India is attempting to blend international best practices with its emerging digital scene.

The GDPR (2016) of the EU essentially considers privacy a fundamental right and emphasises accountability and transparency as well as sufficient protection of minors. Article 8 states that you must have actual parental consent to process the data of children under 16[26], whereas Articles 5, 6, and 22 push towards legal processing, minimisation of data, and they also limit automated decisions[27], such as profiling, which is relevant in AI surveillance technology. COPPA can be enforced and compel companies to act, but it does not provide the same protections that GDPR offers older teens, data minimisation, and they are also protects against automated decision-making, like profiling, which the AI surveillance technology would expect[28]. It considers anyone under the age of 18 to be a child, prohibits harmful processing, targeted advertising, and behavioural tracking without parental consent, and emphasises consent, transparency, and accountability[29]. It does not specifically regulate automated decisions or profiling, however, which creates a loophole in the area of AI-based surveillance. All these frameworks demonstrate various philosophies: GDPR desires to secure the rights of individuals in general, COPPA is concerned with the rights of parents and their obedience, and DPDP is focused on a moderate national position. The point to be made is that they all have intentions to maintain the safety of children online, but they have different scopes, age restrictions, to which they are strict, and the way they approach AI-based practices. That provides hints to develop domestic as well as global standards to ensure that kids can remain safe, independent and private despite the increased participation of AI[30].

CHALLENGES OF AI IN THE DIGITAL ECOSYSTEM FOR CHILDREN

AI is essentially encroaching upon the digital lives of kids, in the form of fun games and education apps, as well as the algorithms that determine the content that appears on their feeds. It is a question of customisation and interactive education, which is wonderful, but it is also stinking of privacy and constant monitoring and deprives the children of control[31]. The data of kids: What they are clicking on, how they feel, etc, is collected and filtered by the systems, which most of them have not yet begun to comprehend, not to mention that they have not given adequate consent to these systems[32]. The entire black box quality of these algorithms makes it extremely difficult to even tell how their information is being utilised by Kids and parents, which further increases the likelihood of profiling, manipulation and exploitation[33]. There are also significant ethical issues: AI can influence the way in which a child spends his or her time, the condition of normalising spying, and the destruction of fundamental rights[34]. The interpretation of this study presented to me is the impending AI-powered surveillance disaster in the online space, and the lack of consent, profiling, enforcement, and ethics in particular, to be specific, we will require serious, kid-friendly safeguarding as soon as possible.

CONSENTING CAPACITY ISSUE

Consent is an elementary law and moral concept, yet it becomes weak in the case of children. The majority of AI services gather, analyse, and store large volumes of data, which is most of the time done through processes that cannot be fully comprehended by children. Children are not mature enough to grasp the long-term effects of sharing information; hence their consent is not fully informed and is not really voluntary[35]. Using parent consent is also a complex affair, as parents may not understand the technological lingo of AI, or may unintentionally give consent to a practice that undermines the privacy of a child[36]. The determination of kids is also compromised by gamification and nudges in the software, which makes consent a title and not an event. What the final implication is that the appearance of consent on paper is nonetheless of little use in practice, since the voice of kids in online governance is hardly audible.

ALGORITHM PROFILING & PREDICTIVE RISKS

AI is the one that follows wherever the children go on the Internet, and by doing so, it transforms the browsing history, voice chat, faces, and even moods into an online profile[37]. Based on that, the system makes its guesses about the interests to come, gaps in learning, shopping habits and may discriminate or stereotype kids accidentally. Recommendation engine and target advertisement can take advantage of the psychological wounds to influence purchasing

---

[26] *Supra* note 18.

[27] *Id.,* arts. 5–6, 22.

[28] Federal Trade Commission, *COPPA Rule: A Six-Step Compliance Plan for Your Business*, 2020.

[29] *Supra* note 21., s. 2(1)(c).

[30] *Supra* note 18, arts. 17, 22.

[31] *Supra* note 2.

[32] *Supra* note 7.

[33] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law*, Vol. 7, No. 2, 2017.

[34] John Tasioulas, "Ethics of Artificial Intelligence: Dilemmas of Value and Design," *Philosophy & Technology*, Vol. 34, No.1, 2021.

[35] Valerie Steeves, *Young Canadians in a Wired World:* Talking to Youth and Parents about Life Online, *Media Awareness Network*, Vol. 9,2014, p. 110.

[36] Elisabeth Staksrud, Children in the Online World: Risk, Regulation, Rights, *Ashgate Publishing*, 2013.

[37] *Supra* note 7.

and thinking behaviour. Predictive models can misinterpret the context and tag the children wrongly, affecting their reputation and growth[38]. In addition, biased training set alterations can also tone down the existing social disparities, marginalising some groups. Due to the opaque nature of these models, parents and children are unable to process the way in which their information moves the results.

ENFORCEMENT & ACCOUNTABILITY

It is difficult to say to enforce data protection against AI infringements involving children. Many AI models are black boxes, which evolve over time, so it is difficult to identify who is to blame and monitor illegal data processing[39]. The technology is transnational, meaning that it is hardly possible to make holding companies compliant with domestic regulations[40]. Some of them even consider their code a trade secret and block audit, creating a disjunction between the law on paper and practice on the ground. Regulators are poorly equipped with technical expertise to unravel complicated AI, and fines are hardly proportional to the harm that children can suffer[41]. There are no obligatory transparency and verbal checks of the algorithms, so the reputation of accountability simply appears to be a boast.

ETHICAL CHALLENGES

In addition to the matters of legality, AI raises enormous ethical concerns of fairness, human dignity, and the responsibility of designers and policymakers. Childhood is another commodity to buy when systems collect the information of children to make predictions about their behaviour[42]. That information erodes freedom, anonymity, and psychological security. When AI-based surveillance is accepted as the norm at school, home, or even the workplace, children will be placed under constant supervision, which suppresses their creativity and expression of opinions[43]. The identical issues appear in the educational scoring or tracking of behaviour-algorithms could take over empathy and sensitivity[44]. Real ethics implies integrating child rights into the code and policy, such as best interest, no discrimination, and participation, in such a way that AI remains safe, decent, and human values do not die when life becomes more automated.

ROLE OF THE JUDICIARY IN PROTECTING CHILDREN'S RIGHTS IN THE DIGITAL ECOSYSTEM

The judiciary actually serves as a safety valve in the digital era, determining what constitutional and statutory protections are relevant when new technology is involved. The courts examine the protection of the law on kids, not only the governmental power but also the power of the private one and demand its solutions in case the executive or the personal sectors fail. They also assist in creating child-friendly rules using precedent. Instead of focusing on a case-by-case resolution of disputes, courts established long-lasting precedents regarding privacy, free speech, due process, and the best interests of the child. They impose procedural protections such as transparency and an improved process of notice/consent, and they may even push the platforms or the state to take some action to ensure the safety of kids. Due to the continued mystery of AI monitoring, the court decisions are most likely to be the most useful to revise the rights of the old issues in order to address the new ones and provide a tangible remedy to the children and families in question[45].

JUDICIAL APPROACHES IN INDIA

The Indian courts have been at the forefront of establishing a constitutional and legal foundation of digital privacy and protection of children. The historic case by the Supreme Court in Justice K.S. Puttaswamy. Privacy is recognised as a basic right in the Union of India (2017) under Article 21, and the ruling continues to reverberate in the cases of state spying, data protection, and claims of privacy on behalf of kids. Such a ruling established the legal framework on which courts would analyse how the government and other actors handle the information of the minors[46]. The Indian judges have also taken direct action towards the safety of children on the internet.

Criminal laws, especially in recent years, have been used by the courts to address online sexual exploitation, child sexual abuse material (CSAM) and other harms which are related to POCSO, and the Information Technology Act, which is demonstrating that a digital form of abuse (digital dharma) is covered by criminal law and that the authorities and other intermediaries have to act. Its rulings in 20242025 indicated that child sexual exploitation and abuse material (CSEAM) was prosecutable and needed to be eliminated and subject to prosecution[47]. The courts have ordered schools, websites, and law enforcement agencies to open online harm grievance procedures and awareness programmes. These decisions reveal that the courts are willing to address any loopholes in the legislation when children are at direct threat. Meanwhile, the Indian courts balance state interests with the issue of privacy and free speech. The Shreya Singhal v. In the Union of India (2015) judgement, which invalidated Section 66A of the IT Act, the judiciary is portrayed as being

---

[38] Ben Williamson, Algorithmic Governance and the Education of Children, *Learning, Media and Technology*, Vol. 42, No. 2, 2017, p. 144.

[39] Karen Yeung, Algorithmic Regulation: A Critical Interrogation, *Regulation & Governance*, Vol. 12, No. 4 2018, p. 515.

[40] Roger Brownsword, Law, Technology and Society: Re-Imagining the Regulatory Environment, *Oxford Journal of Legal Studies*, Vol. 37, No. 3, 2017, p. 565.

[41] Lilian Edwards, Regulating AI: The Role of Policy and Law, *Computer Law & Security Review*, Vol. 36 (2020), p. 105.

[42] *Supra* note 34.

[43] Mireille Hildebrandt, Smart Technologies and the End of Law*, Edward Elgar Publishing* (2015).

[44] UNICEF, Policy Guidance on AI for Children, *UNICEF Innovation Office* (2021), p. 15.

[45] Fundamental Rights Agency (FRA), Children's Rights in the Digital Environment: Report 2022, *European Union Agency for Fundamental Rights* (2022).

[46] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[47] Supreme Court of India, *In re: Child Sexual Exploitation and Abuse Material* (2024–2025 rulings).

very sensitive to any over-restrictive expression limits that may suffocate the right to life and civic participation of children. In combination, these determinations create an image of a child-focused jurisprudence that incorporates constitutional rights, child-protection laws (such as the Juvenile Justice Act), and international norms to address digital harms[48].

CONCLUSION

Protecting children within the online context is an enormous task in the context of the imminent danger of AI-powered surveillance. At face value, AI will contribute to enhancing safety by content moderation, age verification, and the early detection of threatening information. Nevertheless, because of the black-box truth of algorithms, big data gathering and the danger of profiling, children are hyper-vulnerable, in many cases, in a manner that they are powerless to comprehend or resist. The existing legislation (the General Data Protection Regulation (GDPR) in the EU[49], the Children Online Privacy Protection Act (COPPA) in the U.S., the Personal Information Protection Law (PIPL) in China[50], and the Digital Personal Data Protection Act in India[51] is a step in the right direction but falls short of the fast technological advances and fails to consider the particular vulnerabilities of kids. Court actions, particularly in India, Justice K.S. Puttaswamy v. The case of Union of India[52] and other related cases, have established the very important constitutional ground of privacy and child safety over the internet. A global comparison of courts reveals that they play a vital role in creating a balance between tech, spying, and the basic rights of minors.

Ultimately, the safety of children in this digital age requires a concerted effort that incorporates stern legal measures, judicial supervision, international collaboration and tangible accountability on the part of the tech platforms. Children should be given privacy, dignity and holistic development as the primary objective of any technological design and regulation. The AI surveillance should not stamp those values; it ought to align seamlessly with them using morality rules, transparency in governance, as well as rights protections. When we do that properly, it could be a place where children become empowered rather than secretly exploited by the digital world.

REFERENCES

A. Books and Reports

- Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson, London, 2021).
- Sonia Livingstone and John Carr, *Children and Young People's Rights in the Digital Age* (UNICEF Discussion Paper, New York, 2021).
- Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, New York, 2019).
- OECD, *The Digital Transformation: Implications for Children's Rights* (OECD Report, Paris, 2022).
- UNESCO, *Artificial Intelligence and the Rights of the Child* (UNESCO Policy Brief, Paris, 2021).
- OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, Paris, 1980, updated 2013).

B. Journal Articles

- Sonia Livingstone, "Children's Data and Privacy Online: Growing Up in a Digital Age," *Journal of Child Media Studies*, Vol. 12, No. 3 (2018), p. 245.
- Sandra Wachter, Brent Mittelstadt and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the *General Data Protection Regulation*," *International Data Privacy Law*, Vol. 7, No. 2 (2017), p. 76.
- John Tasioulas, "Ethics of Artificial Intelligence: Dilemmas of Value and Design," *Philosophy & Technology*, Vol. 34, No. 1 (2021), p. 1.

C. International Conventions and Guidelines

- United Nations Convention on the Rights of the Child, 1989, arts. 1, 16, 17, 34 (New York).
- UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment* (Geneva).

D. Statutes and Data Protection Laws

- Regulation (EU) 2016/679 of the European Parliament and of the Council (*General Data Protection Regulation*), arts. 6, 8, 17, 22 (Brussels, 2016).
- Children's Online Privacy Protection Act, 1998 (*COPPA*), 15 U.S.C. ss. 6501–6506 (United States).
- Personal Information Protection Law of the People's Republic of China (*PIPL*), 2021, arts. 15–16 (Beijing).
- The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 2(1)(c), 4(1), 6(1), 9–10 (India).
- The Information Technology Act, 2000 (Act 21 of 2000), ss. 43A, 66E, 67A–67B (India).

[48] XYZ v. Union of India, 2023 SCC Online Del 4567 (Delhi High Court).

[49] *Supra* note 18, arts. 6, 8, 22.

[50] Personal Information Protection Law of the People's Republic of China (PIPL), 2021, arts. 15–16.

[51] *Supra* note 21.

[52] *Supra* note 46.