

Safeguarding Children's Rights in the Digital Age: A Comparative Study of Sri Lanka, the EU, and the USA

N. Bopagamage, Arunoda
Ministry of Environment, Sri Lanka

Abstract

The rapid advancement of digital technologies has profoundly reshaped childhood experiences worldwide, offering both significant opportunities and unprecedented risks. The need for a more comprehensive legal framework that deals with digital rights and the online safety of children has been very apparent in Sri Lanka. This paper examines the emerging challenges faced by children in digital environments and critically looks at the extent to which the current law and policy regime of Sri Lanka is sufficient to protect those children against threats like exposure to inappropriate content, cyberbullying, privacy invasion, and limited digital literacy. Drawing on a comparative analysis of the European Union and United States legal regimes, the study highlights significant regulatory gaps in the Sri Lankan context. The research employs a doctrinal legal methodology, supplemented by children's rights theory and legal realism as its theoretical framework. It proposes targeted legal reforms, including the enactment of a dedicated Online Child Protection Act, enhancement of data protection laws, and integration of online safety provisions into national child protection policies. The study concludes by emphasizing the necessity of a dynamic, child-centered regulatory approach that ensures Sri Lankan children's safety and empowerment in the digital age.

Keywords: children's rights, digital environment, data privacy, online child protection, Sri Lanka

1. Introduction

1.1 Background

The advent of digital technology has radically transformed various facets of modern life, including the lives of children. With one-third of internet users under the age of 18, children are among the most active consumers of information and communications technologies (Livingstone & Thid, 2017). A rising body of evidence demonstrates that youngsters are active on the internet at ever younger ages (United Nations, 2018). Their “lifeworlds” are becoming more digitally connected, which has a big impact on how they can use their rights under the UN Convention on the Rights of the Child (CRC) and how those rights may be upheld or ignored (Third, 2014). The United Nations Committee on the Rights of the Child (CRC Committee) has adopted General Comment No. 25, which affirms that children's rights are equally applicable in the digital age and that the CRC is a flexible human rights instrument that can be reinterpreted in various contexts (UN Committee on the Rights of the Child, 2021).

In Sri Lanka, as in many other parts of the world, children are growing up in an environment that is increasingly shaped by digital tools and the internet. Digital technology offers unprecedented opportunities for children to access educational resources, communicate with peers, and explore creative outlets. However, it also presents significant risks, such as exposure to inappropriate content, cyberbullying, privacy violations, and online exploitation (Livingstone, 2013).

Protecting children's rights in this digital era is crucial to ensuring their overall well-being. As technology evolves, the risks children face online become more complex and challenging (Livingstone & Thid, 2017). Consequently, there is a pressing need to ensure that the legal frameworks in Sri Lanka are equipped to safeguard children in digital spaces while also allowing them to benefit from the positive aspects of technology. This paper aims to assess the current state of children's digital rights protection in Sri Lanka, comparing it with legal frameworks in the EU and the USA, and

proposing legal reforms that can better address the unique challenges children face online. Objectives of the study are to examine the emerging challenges and risks in the digital environment for children; to analyze the existing legal frameworks in Sri Lanka related to digital rights of children; and to recommend legal reforms to address the challenges and gaps in digital rights of children in Sri Lanka.

1.2 Research Methodology

This study is library-based desk research in nature, and the data is collected through primary means, including statutes, regulations, case decisions, and secondary sources, including journals, reports, and websites. This study is a comparative study of selected jurisdictions, namely, the European Union (EU), the United States of America (USA), and Sri Lanka. Legal research and comparative legal analysis of child rights in the digital age in selected jurisdictions have been carried out with the support of the doctrinal method.

A doctrine can be defined as 'a synthesis of various rules, principles, norms, interpretive guidelines and values' (Mann, 2010) and identifying connections between seemingly unrelated doctrinal threads, rigorous analysis and inventive synthesis, and the difficulty of making general principles from a rich quantity of original materials are all characteristics of excellent doctrinal research (Council of Australian Law Deans, 2015).

The research design adopts a qualitative approach, grounded in constructivism as the underlying epistemology. Recognizing that knowledge is socially constructed and subjective, this approach allows for the exploration of multiple perspectives and interpretations regarding patent laws and practices.

1.3 Significance of the Study

The issue addressed in this study, protection for children in the digital environment, is important in light of the growing significance of child rights. Globally, digital environment-related child rights protection can be

recognized as a moving subject, given the recent developments in the EU and the USA legal regimes. But the issue of protection for children in the digital environment has been relatively neglected by both academia and policymakers in Sri Lanka.

The overall aim of the study is to comparatively evaluate Sri Lanka, EU, and USA legal approaches to the protection of children in the digital environment, and to propose legal reforms to Sri Lanka based on such evaluation. Hence, the researcher intends to shed light on the grey area of legal scholarship in Sri Lanka.

1.4 Scope and Limitations

Although the objective of this study is to offer a thorough examination of protection for children in digital environments in the USA, the EU, and Sri Lanka, there are a few limitations that should be noted. Firstly, the scope of the study is limited to the above three jurisdictions, which may restrict the applicability of the findings to other jurisdictions with various laws on protection for children in digital environments. Furthermore, it might be difficult to capture all the developments within the study due to the complexity of child protection laws as well as the dynamic nature of protection for children in a digital environment.

2. Theoretical Framework

The legal theoretical framework for this research is rooted in several legal theories, with a focus on children's rights theory and legal realism. These frameworks will provide the basis for analyzing Sri Lanka's current legal structure regarding children's rights in the digital environment and offer insight for possible reforms.

2.1 Children's Rights Theory

The primary legal framework underpinning this research is children's rights theory, which is based on the recognition of children as independent rights holders. Michael Freeman (2002) describes children's rights as 'just claims

or entitlements that derive from moral and/or legal rules,' and argues that rights, in particular children's rights, are important: 'if we have rights we are entitled to respect and dignity' (Freeman & Veerman, 1992).

This theory is encapsulated in the United Nations Convention on the Rights of the Child (UNCRC) (United Nations, 1989), an international human rights instrument that sets out the parties' commitments as far as protection and fulfilment of children's rights are concerned. Particularly under the UNCRC, children possess certain rights which are particularly relevant in the digital age; the rights to privacy, as well as the rights to access information and protection from injurious information.

A child has the right to privacy as per Article 16 of the UNCRC; however, children cannot fully comprehend the information they are giving when it is collected online. Thus, children's data are often violated on the internet, which can lead to further consequences, including identity theft, or grooming. Thus, only using protection of children's digital privacy will ensure the protection of their rights and freedoms.

Article 17 emphasizes children's right to access information from a variety of sources. This provision becomes contentious in the era of internet whereby children must have a right to access to computer-generated media and information as well as to be protected from materials that are considered negative, vile, immoral and unlawful, including pornography, extremist content and other undesirable media information.

Article 19 of the UNCRC obliges states to protect children from all forms of abuse. This provision is vital in catering for risks that are often manifested through the internet such as, bullying, harassment and exploitation. Due to the changes in technology, the concepts guiding the UNCRC have to be implemented and interpreted under new conditions created by the technological change.

This framework helps highlight the need for Sri Lanka to bring its legal system in line with international obligations under the UNCRC to protect children's rights in the digital realm.

2.2 Legal Realism

Legal realism offers a lens through which to examine the enforcement of children's digital rights in Sri Lanka. Drawing on the assumption that laws must be understood and used within realistic frameworks, this theory challenges the existence of formalistic approaches to legal provisions, which lack understanding of realistic conditions for legal norms application. Legal realism is particularly useful in evaluating whether Sri Lanka's legal framework adequately addresses the real challenges children face in the digital age (Frank, 1930).

Legal realism calls for considering the experience of the laws governing child protection in connection with the internet, including what law in its practical application of its goals of protection. This includes examining what resources are available to law enforcement, the training of police in cases of digital rights abuse, particularly as it relates to children, and the technical ability of the judiciary in a child-centered approach to addressing violations of their rights.

This legal theoretical framework, grounded in children's rights theory and legal realism, provides the foundation for a critical analysis of Sri Lanka's legal response to the challenges children face in the digital age. By drawing on comparative insights from the EU and US, the research identifies key areas where Sri Lanka can improve its legal protections for children, ensuring that they are both shielded from online harm and empowered to engage with digital technologies responsibly.

3. Emerging Challenges in the Digital Environment for Children

The digital environment presents a double-edged sword for children. While they have access to valuable tools for education and self-expression, the dangers of the digital world cannot be overlooked (Davies & Eynon, 2013). Children are particularly vulnerable to the below-mentioned risks.

3.1 Exposure to Harmful Content

Children often encounter inappropriate content online, ranging from explicit material to content that promotes violence, racism, or extremism. Due to their developing cognitive abilities, children may have difficulty discerning harmful content from appropriate material, leading to long-term psychological harm.

3.2 Cyberbullying and Online Harassment

Cyberbullying refers to when a child is harassed, threatened, or embarrassed online (The Digital Environment, 2024). Cyberbullying is a growing concern in Sri Lanka, with children often subjected to harassment, threats, and defamation on social media and other online platforms (Livingstone, 2013). The anonymity provided by the internet exacerbates the problem, making it difficult to hold perpetrators accountable.

3.3 Privacy Violations

Many children unknowingly share personal information online, which can lead to privacy violations. Predators, hackers, and other malicious actors exploit children's naivety, often using their data for exploitative purposes, including identity theft and grooming for exploitation (Livingstone, 2013).

3.4 Limited Digital Literacy

Children often lack the necessary skills to navigate the internet safely. Without adequate digital literacy, they are ill-prepared to recognize online threats or protect their personal data (Livingstone, 2013).

These challenges underscore the urgent need for legal and regulatory frameworks that can adequately protect children's rights in the digital age. As the nature of these risks continues to evolve, so too must the laws and policies aimed at addressing them.

4. Legal Frameworks in Sri Lanka

Sri Lanka has made strides in addressing cybercrime and child protection. Several laws and regulations are relevant to safeguarding children in digital environments. This chapter presents a brief analysis of the existing legal framework to protect children from online violence in Sri Lanka, and its shortcomings.

4.1 Constitution of the Democratic Socialist Republic of Sri Lanka

Article 12 of the Constitution states that all persons are equal before the law and are entitled to equal protection of the law. This safeguard would cover children as well. Article 12(4) nevertheless takes a step further and permits specific legal provisions and subordinate laws or taking executive action to further the interests of children. This provision acknowledges the affirmative action is necessary for children as a unique group that requires defence.

Apart from fundamental rights, the Directive Principles of State Policy and Fundamental Duties (DPSP) mentioned in Chapter VI of the Constitution stipulates that the State is to promote with special care the interest of children and youth so as to ensure their full development, physical, mental, moral, religious and social, and to protect them from exploitation and discrimination (Article 27 (13)). However, as per Article 29, this is a non-justiciable right. This shortcoming has however been overcome in fundamental right cases, where DPSP set out in Article 27 (2)(h) has been used in conjunction with Articles 12 and 12 (4) to protect the rights of children (*Chandani De Soysa v. Minister of Education*).

4.2 Penal Code of Sri Lanka

The amendments to the Penal Code that were made by Acts Nos. 22 of 1995, 29 of 1998, and 16 of 2006 are crucial for the protection of children. The 1995 amendment to the penal code increased the severity of the existing offenses, added new ones pertaining to children, and reinterpreted others. Under Section 286A, obscene or indecent exhibitions, shows, films, or

photographs featuring children are now illegal. The new offense is called 'obscene publication and exhibition relating to children' and it applies to everyone under the age of eighteen. Therefore, this Act makes it illegal to make, produce, possess, import, or otherwise deal with any kind of obscene writings, drawings, prints, paintings, printed matter, pictures, posters, emblems, photographs, cinematograph films, or other obscene objects.

The Penal Code was amended in 1998 to include additional offenses pertaining to children. As a result, it became illegal to cause or procure children to beg, hire or engage children to act as procurers for sexual intercourse, or traffic in restricted places. The Code also requires photographers and filmmakers to disclose any indecent or obscene images or videos of children they come across while working. Failure to do so could result in a fine and/or two years in prison. In order to stop child sexual abuse, the Penal Code was further revised in 2006 by adding Section 286B, which extends the reporting obligation to anybody offering 'service by means of a computer,' such as cybercafés. In addition, the introduction of Section 286C into the Penal Code in 2006 made it illegal to store or distribute child pornography via the internet or by email.

4.3 Computer Crimes Act No. 24 of 2007

Computer crimes fall under two categories under the Computer Crimes Act, No. 24 of 2007: (a) committing crimes like fraud and theft; and (b) introducing viruses, worms, gaining unauthorized access, hacking, and character assassination. 'Any person who intentionally does any act, knowing or having reason to believe that he/she has no lawful authority to secure such access and with the intention of committing an offence under the Act or any other law,' as stated in Section 3, 'in order to secure for himself or for any other person access to (a) any computer; or (b) any information held in any computer'. The Act also lists as offenses the unlawful interception of data and the illegal disclosure of information necessary to get a service (Section 10). It is illegal, according to Section 7, for someone to take data from a computer or its storage device without authorization. It also makes downloading, uploading, and duplicating such

content that was obtained illegally. Even though the aforementioned provisions don't specifically target online violence against, they might be crucial in prosecuting those who commit online crimes against children (Fernando et al., 2021).

4.4 Obscene Publications Ordinance

The amended Section 2 of the Obscene Publications Ordinance makes it illegal to publish an offensive item online. Furthermore, when children under the age of eighteen are found in possession of cell phones containing pornographic material, or when children are given access to pornographic video films in internet cafes and other establishments, the police and other law enforcement authorities file charges under the Obscene Publications Ordinance (as amended by Act, No. 22 of 1995 and Act No. 29 of 1998). It is clear that the act's actual application can provide protection against OVAC acts (Fernando et al., 2021).

4.5 Children's Charter of Sri Lanka

Through the Children's Charter (CC), the Government of Sri Lanka incorporated the CRC into national Policy. The Charter, which serves as Sri Lanka's fundamental policy framework for children, reaffirms Sri Lanka's commitment to a range of international human rights instruments. These include the Geneva Declaration of the Rights of the Child (1924), the Declaration of the Rights of the Child (1959), the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (1976), particularly Articles 23 and 24, the International Covenant on Economic, Social and Cultural Rights (1976), specifically Article 10, and the foundational statutes and instruments of specialized agencies and international organizations concerned with the welfare and rights of children. Collectively, these instruments underscore the universal recognition of children's human rights and guide Sri Lanka's policy direction in safeguarding them.

The Preamble to the CRC acknowledges that Sri Lanka's indigenous traditions, as well as its socioeconomic and social policies, have always

placed a high priority on the concern, care, nurturing, growth, and development of children (Sri Lanka Charter on the Rights on the Child). It also states that in order to guarantee children's and youth's complete development and protection from discrimination and exploitation, the Constitution shall advance their interests (The Constitution of the Democratic Socialist Republic of Sri Lanka, 1978).

In addition, the Charter recognizes the right to children's privacy (Article 16), protection from abuse and neglect (Article 20), protection from sexual exploitation (Article 34), and the obligation of the state to set up suitable social programmes to prevent physical and mental violence, abuse, and exploitation, as well as to treat victims in the process of achieving these goals.

4.6 Policy Framework

The National Child Protection Authority (NCPA) of Sri Lanka is the principal body for the protection of children from all forms of abuse in Sri Lanka when it comes to assessing the current policy framework on online violence against children. Its responsibility is to advance children's interests and wellbeing on a nationwide scale. The NCPA's 'National Policy on Child Protection 2017–2027' lays out the broad objectives, guiding principles, and values, as well as the policy goals and primary tactics that can be used to guarantee that every child is shielded from abuse, neglect, and other types of maltreatment and harm. The policy's objectives, guiding principles, and values designate 'other forms of violence and harm and child protection' as an umbrella term that might apply to online violence against child. However, one significant flaw in the Policy is its omission of any mention of online violence against child (Fernando et al., 2021).

The 'Best Interest of the Child' principles are the cornerstone of every decision-making that impacts the lives of children, according to the Policy. A child's best interests shall be considered when evaluating the immediate and long-term risks to their development, safety, and well-being. When it comes to online violence against child, the best interest of the children

premise might be quite important. Article 3 of the CRC explicitly affirms that *“in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.”* Accordingly, parents, guardians, and all stakeholders responsible for children's digital experiences must ensure that robust protective measures are implemented to safeguard children from online risks while promoting a safe, empowering digital environment.

Sri Lanka has enacted a number of legislative and policies related to children's protection in the digital environment, yet it continues to have a number of challenges, with one of them being its ability to respond to the dynamics of cybersecurity threats. However, it's noted that new laws and specific provisions are required dedicated to address the issue of online violence against children though certain existing laws such as the Penal Code, Computer Crimes Act, and the National Policy on Child Protection offer some form of starting framework. Improving these frameworks to the standard enjoyed in developed countries may potentially increment the safety of children in the present digital age.

5. Comparative Analysis: EU and USA Legal Approaches

5.1 EU Legislative Developments

The EU has developed comprehensive legal frameworks to address the challenges and risks faced by children in the digital environment. These frameworks aim to strike a balance between protecting children's rights and enabling their access to digital opportunities. The EU's approach is grounded in various legislative instruments, strategies, and policy initiatives that safeguard children from online risks, ensure their privacy, and promote digital literacy. This chapter explores key aspects of these frameworks, highlighting the measures taken to create a safer digital space for children.

5.1.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), which came into effect in 2018, is one of the most significant legislative measures in the EU for protecting the privacy and personal data of individuals, including children. The GDPR explicitly recognizes the need for enhanced protection for children, especially in the digital world. It establishes specific provisions that focus on the rights of children, including the following:

- **Article 8 - Conditions Applicable to Child's Consent in Relation to Information Society Services:** Article 8 requires that for children under the age of 16, consent for processing their personal data must be obtained from their parent or guardian. EU Member States have the flexibility to lower this age limit to 13, but the emphasis remains on protecting younger users.
- **Right to Erasure (Article 17):** The GDPR also includes the 'right to be forgotten,' allowing individuals, including children, to request the deletion of their personal data when it is no longer needed for the purpose for which it was collected. This is especially important for children who may have posted or shared information online without fully understanding the implications.

The GDPR's focus on consent and data protection reflects the EU's commitment to safeguarding children's privacy online and ensuring that their personal information is not exploited by digital services (Article 17).

5.1.2 Audiovisual Media Services Directive (AVMSD)

The Audiovisual Media Services Directive (AVMSD) is another critical legal instrument in the EU aimed at protecting minors from harmful content in digital media. Revised in 2018, the AVMSD sets out rules for both traditional broadcasting and video-on-demand services, including online platforms like YouTube and streaming services (Directive (EU) 2018/1808, 2018). Key provisions related to children include:

- The AVMSD requires that content likely to impair the physical, mental, or moral development of minors be restricted and that parents or guardians have tools to control children's access to such content (Article 6a).
- The directive places responsibilities on video-sharing platforms to ensure that minors are protected from harmful content and to prevent the promotion of hate speech, violence, and child exploitation on their services (Article 28b).

The AVMSD helps establish a safer online environment by obligating digital platforms to implement measures that prevent children from accessing harmful material, thereby addressing issues like online harassment and exposure to inappropriate content (Article 28b).

5.1.3 EU Strategy for a Better Internet for Kids (BIK+)

The EU Strategy for a Better Internet for Kids (BIK+), first launched in 2012 and updated in 2022, is a comprehensive policy initiative designed to create a safer online environment for children (The European Strategy for a Better Internet for Kids (BIK+), 2022). The strategy focuses on four main areas:

- Encouraging the creation of high-quality, age-appropriate content that supports the positive development of children (The European Strategy for a Better Internet for Kids (BIK+), 2022).
- Promoting digital literacy among children, parents, and educators to ensure children can navigate online spaces safely and critically (The European Strategy for a Better Internet for Kids (BIK+), 2022).
- Enhancing measures to combat cyberbullying, child sexual abuse material, and other online risks, while also supporting mechanisms for reporting and removing harmful content (The European Strategy for a Better Internet for Kids (BIK+), 2022).
- Empowering children to have a voice in shaping online spaces and policies that affect them, ensuring that their views are considered in

the development of safer online environments (The European Strategy for a Better Internet for Kids (BIK+), 2022).

The BIK+ strategy is significant in providing a holistic approach to child protection in the digital age, complementing legal measures with educational and awareness-raising initiatives (The European Strategy for a Better Internet for Kids (BIK+), 2022).

5.1.4 European Parliament's Resolution on Children's Rights in the Digital Environment

In March 2021, the European Parliament adopted a resolution on children's rights in the digital environment, which recognizes the need for a balanced approach that respects children's rights while ensuring their safety (Resolution on Children's Rights in the Digital Environment, 2021). It highlights several recommendations, including:

- Recommending that digital service providers adopt stronger measures to protect children's data and ensure transparency in data processing activities (Resolution on Children's Rights in the Digital Environment, 2021).
- Calling for enhanced efforts to address cyberbullying, online harassment, and other forms of violence against children online (Resolution on Children's Rights in the Digital Environment, 2021).
- Emphasizing the importance of digital literacy and online safety education in empowering children to use technology safely and responsibly (Resolution on Children's Rights in the Digital Environment, 2021).

This resolution reflects the EU's ongoing commitment to adapting its legal and policy frameworks to the evolving challenges of the digital age, recognizing the critical importance of children's rights in this context (Resolution on Children's Rights in the Digital Environment, 2021).

The EU's legal framework for safeguarding children's rights in the digital age is built on a combination of binding regulations like the GDPR and AVMSD, as well as policy initiatives like the BIK+ Strategy. These frameworks collectively address key aspects of child protection, including privacy, safety, and digital literacy. By continuously adapting its legislative and policy measures, the EU seeks to provide a balanced environment where children can benefit from digital opportunities while being protected from online risks. This serves as a model for other jurisdictions, including Sri Lanka, which can draw on the EU's experience to enhance its own digital child protection mechanisms.

5.2 USA Legislative Developments

The USA has developed a complex legal framework to address the unique challenges faced by children in the digital environment. This framework includes federal laws, state regulations, and guidelines that seek to protect children's privacy, ensure their safety, and regulate their interactions with online content. The emphasis is on balancing the protection of children with the preservation of their access to online educational and social resources. This chapter explores key aspects of these frameworks, highlighting the measures taken by the USA to create a safer digital space for children.

5.2.1 Children's Online Privacy Protection Act (COPPA)

The COPPA is one of the most critical pieces of federal legislation aimed at protecting children's privacy online. Enacted in 1998, COPPA is designed to regulate the collection, use, and disclosure of personal information from children under the age of 13 by websites and online services (COPPA, 1998). According to COPPA, websites and online services that collect personal information from children under 13 must obtain verifiable parental consent before collecting such data. This includes information such as a child's name, address, and contact information (15 USC § 6502(b)(1)(A)). Operators are required to provide a clear and comprehensive privacy policy that details their data collection practices and must notify parents directly about how they collect and use children's information (15 USC §

6502(b)(1)(A)(i)). Also, parents have the right to request the deletion of their child's personal information from a website's database (15 USC § 6502(b)(1)(B)).

COPPA is enforced by the Federal Trade Commission (FTC), which can impose penalties for non-compliance. The Act is significant because it sets clear standards for privacy protection in online spaces frequented by children (*Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, 2025). However, some critics argue that the law has limitations, such as its focus on children under 13, leaving older minors with less protection (Regan, 1995).

5.2.2 Children's Internet Protection Act (CIPA)

The CIPA of 2000 is another crucial federal law aimed at protecting children from harmful online content. CIPA requires that schools and libraries that receive federal funding for internet access or internal connections implement measures to block or filter internet content that is obscene, child pornography, or harmful to minors (Children's Internet Protection Act, 47 USC § 254 (2000)). Key components of CIPA include that schools and libraries must use technology protection measures to block access to visual depictions that are obscene or harmful to minors (47 USC § 254(h)(5)(C)) and CIPA also mandates that schools and libraries develop and adopt internet safety policies to monitor minors' online activities and educate students about appropriate online behaviour (47 USC § 254(h)(5)(C)).

CIPA focuses primarily on protecting children from harmful content in educational settings, ensuring that they have a safer browsing experience. While it has been effective in schools and libraries, critics argue that the scope of CIPA is limited as it does not extend to all online environments that children access.

5.2.3 State-Level Regulations and Initiatives

In addition to federal laws, individual states have enacted legislation to further safeguard children in digital spaces. Some states have implemented

more stringent privacy laws that extend protections to minors beyond what is provided under COPPA. Examples include:

- California Consumer Privacy Act (CCPA): While not exclusively for children, the CCPA provides enhanced privacy rights for California residents, including minors (California Consumer Privacy Act, Cal Civ Code § 1798.100 (2018)). It requires businesses to provide clear notice to consumers about data collection practices and offers individuals the right to access, delete, and opt-out of the sale of their personal information.
- California Age-Appropriate Design Code Act (CAADCA): Passed in 2022, this law aims to create a safer digital environment for children by requiring online platforms to prioritize the privacy and safety of users under 18. The CAADCA focuses on designing online services that take into account children's best interests (California Age-Appropriate Design Code Act, AB 2273 (2022)).

These state-level initiatives complement federal efforts and reflect a growing recognition of the need to adapt privacy and safety measures to the changing digital landscape.

The legal framework of the USA for protecting children in the digital age encompasses a blend of federal laws like COPPA and CIPA. These frameworks aim to address the diverse risks children face online, from privacy violations to exposure to harmful content and exploitation. While these efforts have made significant strides in enhancing child safety online, challenges remain in adapting laws to evolving digital threats and ensuring uniform protection across all states. The experience of the USA highlights the importance of continuous legislative adaptation and coordinated policy efforts to safeguard children's rights in an increasingly digital world.

6. Recommendations for Sri Lanka

Based on the comparative analysis, several recommendations can be made to strengthen the protection of children's rights in the digital environment in Sri Lanka:

6.1 Enact Specific Legislation for Online Child Protection

Sri Lanka has taken initial steps to protect children from online risks through its existing legal and policy frameworks, but significant gaps remain in adapting to the challenges of the digital age. By drawing on the approaches of the EU and USA, Sri Lanka can develop a more robust system for safeguarding children's rights in digital spaces.

Sri Lanka should consider enacting a dedicated Online Child Protection Act, similar to COPPA in the USA, to address the specific risks children face online. This law should include provisions for:

- Parental consent for data collection from minors.
- The right to erasure of personal information.
- Age verification mechanisms for accessing certain online services.

A separate section for online sexual exploitation and harassment, akin to provisions in the EU's AVMSD, should also be included to address digital threats.

6.2 Strengthen Data Protection for Children

Sri Lanka could adopt elements from the GDPR, such as the requirement for obtaining parental consent for processing personal data of minors. Establishing a 'right to be forgotten' would allow children and parents to request the removal of personal information from digital platforms.

Developing a comprehensive Data Protection Act that specifically addresses children's data privacy can ensure that online services are held accountable for how they handle minors' data.

6.3 Improve Institutional Capacity and Enforcement Mechanisms

The NCPA can be empowered with a dedicated unit focused on online safety and digital child protection. This unit could work in collaboration with law enforcement and the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) and SLCERT to monitor online activities that pose risks to children.

6.4 Integrate Online Safety into the National Policy on Child Protection

The current National Policy on Child Protection should be revised to explicitly include measures for protecting children from online violence and digital threats. This would align Sri Lanka's policy framework with international standards, such as those seen in the EU and the USA. Including specific goals related to online safety in the policy would ensure that resources are allocated for implementation, monitoring, and continuous improvement.

Implementing these recommendations will require legislative reforms, capacity building, and active collaboration with international partners. A comprehensive and adaptive approach will help create a safer digital environment for Sri Lankan children, allowing them to fully benefit from the opportunities of the digital age while minimizing potential risks.

7. Conclusion

The protection of children in digital environments is a growing concern in the modern world of fast-paced digital models. This study has explored Sri Lanka's current legal frameworks for safeguarding children online, identifying strengths and weaknesses in comparison with established systems in the EU and the USA. Although Sri Lanka has made some progress with general child protection laws and with the activities of the NCPA, the law and the relevant regulations targeting online threats and privacy remain a significant gap. The EU and the USA, on the other hand, offer examples with particular regulations such as GDPR and COPPA

which deal with the specific exposures children face in the digital space. Such models prioritize data protection, online privacy and digital literacy, and are useful examples that Sri Lanka can learn. To fill its regulatory lapses, Sri Lanka must contemplate coming up with special legislation, reviewing the current legislation, improving the digital literacy initiatives and collaborating with international agencies to establish a secure internet space in which children can explore the internet. By adapting best practices from global examples to local needs, Sri Lanka can build a comprehensive framework that ensures children can safely engage with the digital world, benefiting from its opportunities while being protected from its risks.

Future research is needed to better understand how online technologies are used by Sri Lankan children and which of them are at risk of online harassment. The research studies on online behavior of children, the usefulness of school-based digital literacy programmes, and the effectiveness of law enforcement in response to the online abuse would be helpful in policymaking. It is also necessary to conduct research on the question of how the proposed legal changes can be implemented and how the international practices may be adjusted to the social and cultural environment of Sri Lanka.

References

California Age-Appropriate Design Code Act, AB 2273 (2022).

California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (2018).

Chandani De Soysa v. Minister of Education, SC/FR/2016/77 (Sri Lanka).

Children's Internet Protection Act, 47 U.S.C. § 254 (2000).

Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998).

Children's online privacy protection rule: A six-step compliance plan for your business. (2025, May 29). Federal Trade Commission. <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business>

Constitution of the Democratic Socialist Republic of Sri Lanka (1978).

Council of Australian Law Deans. (2015). *Statement on the nature of legal research*. <https://cald.asn.au/wp-content/uploads/2017/11/cald-statement-on-the-nature-of-legal-research-20051.pdf>

Davies, C., & Eynon, R. (2013). *Teenagers and technology*. Routledge. <https://doi.org/10.4324/9780203079270>

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 (Audiovisual Media Services Directive), OJ L 303/69.

European Commission. (2022). *European strategy for a better internet for kids (BIK+)*.

European Parliament. (2021). *Resolution on children's rights in the digital environment* (P9_TA(2021)0072).

Fernando, N., Hakeem, M. A. M., Seneviratne, W., De Silva, M., Cooray, J., State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services, Save the Children, & World Vision. (2021). *Online violence against children in Sri Lanka: A national research on incidence, nature and scope*. Social Policy Analysis and Research Centre (SPARC), University of Colombo. <https://sparc.cmb.ac.lk/wp-content/uploads/2021/04/ECVAC-Research-Summary-Report-Design.pdf>

Frank, J. (1930). *Law and the modern mind*. Transaction Publishers.

Freeman, M. (2002). *Human rights: An interdisciplinary approach*. Polity Press.

- Freeman, M., & Veerman, P. E. (1992). The limits of children's rights. In *The ideologies of children's rights: International studies in human rights*. Brill.
- Government of Sri Lanka. (n.d.). *Sri Lanka Charter on the Rights of the Child*.
- Livingstone, S. (2013). *Children and the internet*. John Wiley & Sons.
- Livingstone, S., Carr, J., & Byrne, J. (2015, November 2). *One in three: Internet governance and children's rights*. Centre for International Governance Innovation.
<https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights/>
- Livingstone, S., & Thid, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, 19(5), 657–670.
- Mann, T. (2010). *Australian law dictionary*. Oxford University Press.
<https://doi.org/10.1093/acref/9780195557558.001.0001>
- National Child Protection Authority. (2017). *National policy on child protection*.
- Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. University of North Carolina Press.
- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), OJ L 119/1 (2016).
- State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services. (2021). *Online violence against children in Sri Lanka: A national research on incidence, nature and scope*.

The digital environment. (2024, April 4). *Children's Rights*.
[https://www.coe.int/en/web/children/the-digital-environment#{%2212440617%22:\[8\]}](https://www.coe.int/en/web/children/the-digital-environment#{%2212440617%22:[8]})

Third, A. (2014). *Children's rights in the digital age: A download from children around the world*.

UN Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. UNICEF.
<https://www.unicef.org/bulgaria/en/media/10596/file>

United Nations. (1989). *Convention on the Rights of the Child*.
<https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>

United Nations. (2018). *State of the world's children 2017: Children in a digital world*. UNICEF.