UST LAW JOURNAL

THE OFFICIAL PUBLICATION OF THE UST GRADUATE SCHOOL OF LAW

VOLUME 3

DECEMBER 2025

UST LAW JOURNAL
Volume 3, Issue No. 3
December 2025

EDITORIAL BOARD

UST LAW JOURNAL (ISSN) is the official publication of the
UST Graduate School of Law Program

EDITORIAL OFFICE

4F Buenaventura García Paredes O.P. Building
University of Santo Tomas, España, Boulevard, Sampaloc
Manila 1008, Philippines

The UST Law Journal welcomes papers that explore pressing legal issues, address socio-economic and international topics with significant legal dimensions, and make meaningful contributions to these critical discussions. It is a peer-reviewed academic publication that aims to publish scholarly articles in its pursuit of legal scholarship and academic excellence. Papers are published through a double-blind peer review process undertaken by the Board of Editors and reviewers.

The Journal's mission is to cultivate an environment that values intellectual diversity, legal analytical precision, and the pursuit of impactful research. Each issue features contributions that bridge theoretical and practical approaches, drawing from comparative, international, and domestic perspectives. It presents legal scholarship that interrogates traditional doctrines, dissects contemporary legal challenges, and proposes innovative frameworks for understanding the complexities of law in an interconnected world.

The articles published in *The UST Law Journal* do not necessarily represent the views of the Board of Editors. The articles are representative of the views of the author/s alone, and the author/s are responsible for the views expressed therein.

EDITOR'S NOTE

Welcome to the 2025 3rd Volume, 3rd Edition of the UST Law Journal. This year's volume reflects our ongoing commitment to producing rigorous, forward-looking, and socially relevant legal scholarship that addresses the evolving challenges of our national, regional, and global legal landscape. We thank our contributors, reviewers, and readers for their trust and engagement as we usher in another year of meaningful discourse.

The digital world has become an integral part of childhood, shaping how children learn, communicate, and explore their identities. Yet the rapid expansion of social media platforms has also exposed young users to unprecedented risks. In response to these emerging threats, for this 3rd Volume, the 8th article, *"Social Media in Early Childhood: Adopting the U.S. Kids Online Safety Act in Protecting Children on Social Media"* offers a timely and much-needed contribution to contemporary discourse on child digital safety. The author examines the U.S. Kids Online Safety Act (KOSA) as a potential model for Philippine legislation, exploring how its core principles duty of care, algorithmic transparency, parental tools, and platform accountability could help safeguard young Filipino children navigating the online environment. The analysis is both global and local as it contextualizes KOSA within international child rights frameworks while critically assessing the Philippine legal landscape, including the Data Privacy Act, the Anti-Online Sexual Abuse and Exploitation of Children Act, and existing child welfare policies. By focusing on early childhood, the article highlights a stage where developmental vulnerability is at its peak and where digital harm can have long-lasting psychological, emotional, and cognitive effects. The proposed adoption of a KOSA-inspired framework underscores the need for proactive legal reform to strengthen parental empowerment, and implements protective measures prioritizing the best interests of the child.

IRENE D. VALONES
Editor-In-Chief

SOCIAL MEDIA IN EARLY CHILDHOOD: ADOPTING THE U.S. KIDS ONLINE SAFETY ACT IN PROTECTING CHILDREN ON SOCIAL MEDIA

By:

ATTY. LOVELY ROSE LIM UY

ABSTRACT

The increasing prominence of social media in everyday life has underscored the urgent need for mechanisms that safeguard the rights and welfare of vulnerable sectors, particularly children. This concern is especially relevant in the Philippines, a country widely regarded as one of the most active users of social media globally. Filipino children are introduced to platforms such as Facebook, TikTok, and online marketplaces at a very young age, which, while offering opportunities for connection and learning, simultaneously expose them to unprecedented digital risks and harms. Despite the existence of child protection laws in the Philippines, the current legal landscape remains inadequate in responding to the evolving threats posed by early social media exposure. The lack of clear statutory guidelines and regulatory oversight has resulted in significant gaps in enforcement, thereby compromising the country's ability to uphold its obligations to protect children's rights in the digital sphere.

In light of these concerns, this thesis conducts a comparative legal analysis between Philippine laws and the United States' proposed Kids Online Safety Act (KOSA), which advances a holistic, proactive, and child-centered framework for online safety. Through a qualitative, black letter law approach that examines existing statutes, jurisprudence, and legal doctrines, this article identifies critical areas for legal reform in the Philippine context. It argues for the incorporation of key KOSA principles, such as the "duty of care" imposed on digital service providers, to ensure that online platforms are held accountable for the protection of child users. This research also highlights the necessity of integrating digital literacy education for children, parents, and educators as a complementary protective measure. Such a multi-pronged approach, combining legislative reform with education and awareness, seeks to establish a safer, more responsible digital environment for Filipino children, in alignment with international best practices.

Keywords: Privacy, Social Media, Duty of Care, Early Childhood

I. INTRODUCTION

In recent years, social media has become an integral part of everyday life, profoundly shaping the way children interact with the world around them. The rapid expansion of platforms such as Facebook, Instagram, TikTok, and YouTube has not only broadened avenues for communication, entertainment, and learning but has also exposed minors to unprecedented online risks.

In the Philippines, studies[1] indicate that children as young as five years old engage with these platforms on a daily basis, often with minimal or no supervision. This early and frequent online exposure raises serious concerns about their safety, privacy, and overall well-being. A striking example of these challenges occurred in the Philippines when a two-year-old girl unintentionally purchased 60 packages from an e-commerce platform while playing on her mother's phone (GMA Public Affairs, 2023).

What began as an innocent interaction with a mobile device quickly escalated when the child, instead of merely tapping through games, navigated to the platform's "add to cart" feature and successfully completed the checkout process. Her parents were unaware of the transaction until the unexpected deliveries arrived at their doorstep, highlighting the ease with which young children can engage with digital platforms in unintended ways. This incident illustrates the rapid adaptability of children to technology and, more importantly, their vulnerability to online risks. While this case involved financial transactions, it underscores broader concerns about digital safety, including exposure to inappropriate content, data privacy risks, and the addictive design of online platforms. As children increasingly interact with digital spaces at younger ages, the need for stricter safeguards and more comprehensive regulatory frameworks becomes evident.

Supporting this narrative, research[2] shows that one in ten minor children has made accidental online purchases, and six out of ten are already familiar with online shopping platforms. Beyond inadvertent transactions, children's limited understanding of online risks can lead them to unknowingly share personal information, including their location or full name, which heightens their susceptibility to exploitation and cyber threats. While social media platforms can enrich children's learning and creativity, they also introduce complex risks such as cyberbullying, data privacy breaches, and exposure to inappropriate content. The rapid growth of these platforms has far outpaced the development of effective legal protections, particularly in the Philippines, where existing laws do not sufficiently address the unique vulnerabilities of children in digital spaces. In contrast, the United States has introduced the Kids Online Safety Act[3] (KOSA), a major legislative initiative aimed at safeguarding children's well-being on social media through content moderation and privacy controls. KOSA was introduced to the U.S Senate by Senators Richard Blumenthal and Marsha Blackburn on February 16, 2022. The bill was prompted by a significant event in 2021 when Frances Haugen, a former data scientist at Facebook, leaked internal documents to "The Wall Street Journal". These files revealed the harmful impact Instagram had on minors' mental health, among other issues.[4]

---

[1] Kemp, S. (2024). *Digital 2024: The Philippines*. DataReportal, Available at: https://datareportal.com/reports/digital-2024-philippines (Accessed on September 3, 2024)

[2] Lim, A. R. (2015, July 14) Childnet. Available at: https://www.childnet.com/blog/1-in-10-young-people-accidentally-spent-money-on-in-app-purchases-survey-shows/ (Accessed on September 3 2024)

[3] The Kids Online Safety and Privacy Act (KOSPA) (S. 2073), commonly known as the Kids Online Safety Act (KOSA) (H.R. 7891), is a proposed legislation first introduced in Congress in 2022. The bill seeks to protect minors from harmful content on social media platforms by imposing a duty of care on covered platforms and requiring them to disable design features deemed "addictive" for minors.

[4] Sorkin (2022). *Child Safety is the New Tech Battleground.* Available at: https://www.nytimes.com/2022/02/17/business/dealbook/children-online-safety-bill.html (Accessed on February 26, 2025)

The leak triggered a Congressional investigation into Big Tech's failure to safeguard young users, leading to Instagram CEO Adam Mosseri testifying before Congress in December 2021.[5] Senator Blumenthal, referencing the leaked Facebook data, clarified that the bill's goal was not to dismantle tech platforms, but to engage them in a collective effort to achieve the shared goal of protecting children, to wit:

> *"not to burn the internet to the ground, not to destroy tech platforms or the internet or these sites; it is simply to enlist the social media platforms in this joint effort to achieve what should be a common goal – protecting children."*
> *– Senator Blumenthal, 2022.*

This statement emphasizes that the goal of the proposed legislation (likely KOSA) is not to dismantle or severely restrict the internet, social media platforms, or tech companies. Instead, it aims to make these platforms active participants in protecting children online. The Senate Commerce Committee thus advanced the bill in July 2022 alongside COPPA 2.0, an updated version of the Children's Online Privacy Protection Act (COPPA), which will be further discussed in the subsequent sections of this article. Both were expected to pass as part of larger legislation in the 117th Congress but ultimately failed. Still, former U.S. President Joe Biden endorsed KOSA when it was reintroduced in 2023 and urged Congress to pass child online safety legislation in his State of the Union address.[6] He emphasized the need to make social media companies accountable and to impose stricter limits on collection of the personal data;

> *"Second, let's do more on mental health, especially for our children. When millions of young people are struggling with bullying, violence, trauma, we owe them greater access to mental health care at school.*
>
> ***We must finally hold social media companies accountable for the experiment they are running on our children for profit.***
>
> *And it's time to pass bipartisan legislation to stop Big Tech from collecting personal data on kids and teenagers online, ban targeted advertising to children, and* ***impose stricter limits on the personal data these companies collect on all of us****."*[7] (emphasis added)

This led Senators Blackburn and Blumenthal to reintroduce the bill on May 2, 2023. Congress and President Joe Biden have emphasized that protecting children online is a top priority, with KOSA emerging as a leading legislative measure in this effort.[8] The bill has garnered strong bipartisan backing, securing over 25 co-sponsors. An earlier version passed unanimously in the Senate

[5] Ibid.
[6] 2023 State of the Union Address
[7] Transcript: President Biden's 2023 State of the Union Address, Available at: https://www.voanews.com/a/transcript-president-biden-s-2023-state-of-the-union-address/6953032.html (Accessed on February 26, 2025)
[8] Feiner, L. (2023) Lawmakers update Kids Online Safety Act to address potential harms, but fail to appease some activists, industry groups. Available at: https://www.cnbc.com/2023/05/02/updated-kids-online-safety-act-aims-to-fix-unintended-consequences.html (Accessed on February 26, 2025)

Commerce Committee, and the revised bill continues to gain support from various advocacy groups.[9] Tech companies argue that they already adhere to numerous federal regulations designed to protect children online and have taken proactive steps in response to public concerns and international policies. They emphasize that existing frameworks, such as the Children's Online Privacy Protection Act (COPPA) in the U.S. and various data protection laws abroad, impose strict compliance obligations on digital platforms to safeguard minors.[10]

"Protecting young people online is a broadly shared goal. But it would contradict the goals of bills such as this to impose compliance obligations that undermine the privacy and safety of teens," said Matt Schruers, president of the Computer & Communications Industry Association, whose members include Amazon, Google, Meta, and Twitter (now X). *"Governments should avoid compliance requirements that would compel digital services to collect more personal information about their users – such as geolocation information and a government-issued identification – particularly when responsible companies are instituting measures to collect and store less data on customers."*[11]

In November 2023, whistleblower and former Meta engineering director Arturo Beja testified before a Senate subcommittee on social media's impact on teen mental health, renewing momentum for the bill.[12] A January 2024 Senate hearing with the CEOs of Meta, TikTok, Snap Inc., Discord, and Twitter further amplified calls for action. By February, the bill had enough Senate support to ensure passage, though no companion bill had been introduced in the House.[13]

In May 2024, an attempt was made to attach KOSA to the FAA Reauthorization Act. Later, the Senate combined KOSA, COPPA 2.0, and the Filter Bubble Transparency Act into the Kids Online Safety and Privacy Act (S. 2073). Introduced by Chuck Schumer as an amendment on July 23, 2024, the bill passed the Senate with a 91–3 vote on July 30, 2024.[14]

By July 2024, however, the House had yet to pass its version. A scheduled markup session in June was abruptly canceled, reportedly due to disagreements among House Republicans over a separate privacy bill. In August, Punchbowl News reported that House Republican leadership would not advance KOSA due to internal concerns.[15]

On September 18, 2024, the House Energy and Commerce subcommittee advanced the bill with last-minute amendments to its "duty of care" provisions, widening the gap between House and Senate versions. This led some lawmakers

---

[9] Ibid
[10] Ibid.
[11] Ibid.
[12] Klar (2023). *Meta Whistleblower to testify in Senate Hearing on Child Safety Social Media.* Available at: https://thehill.com/policy/technology/4292397-meta-whistleblower-to-testify-in-senate-hearing-on-child-safety-social-media/ (Accessed on February 26, 2025)
[13] . Wong (2024). Senate passes the most significant child online safety bills in decades. Available at: https://www.nbcnews.com/politics/congress/senate-poised-pass-significant-child-online-safety-bills-decades-rcna164259 (Accessed on February 26, 2025)
[14] Ibid
[15] Nazzaro (2024). House panel advances Kids Online Safety Act despite pushback. Available at: https://thehill.com/policy/technology/4886978-house-panel-advances-kosa/ (Accessed on February 20, 2025)

to withdraw support. No further action was taken before the 118th Congress ended, nullifying its progress.[16]

Senator Blumenthal intends to reintroduce the bill in the 119th Congress. He is eager to bring back KOSA. He admits that the point of the bill is to suppress content he dislikes. He believes by providing a comprehensive framework that focuses on children's digital well-being and privacy, KOSA exemplifies the global movement toward stronger regulations for children's online activities.[17]

> *"The dangers of social media are no less now than they were in the last session, and we need to pass the Kids Online Safety Act to give parents tools and young people control so that addictive, destructive content on bullying, eating disorders, and self-harm can be stopped,"* Blumenthal said.

In other words, the bill does not seek to ban or heavily regulate social media to the point of rendering it unusable. Rather, it aims to create reasonable safeguards that encourage tech companies or social media platforms to take responsibility for reducing harm to minors, such as limiting exposure to harmful content and addictive design features. While KOSA has faced legislative hurdles, its bipartisan support and ongoing revisions reflect a global recognition of the urgent need for stronger digital safeguards for children. This thesis explores how the Philippines can address similar challenges by adopting key provisions from KOSA to enhance its legal framework for child online safety.

By analyzing KOSA's core principles such as platform accountability, risk mitigation measures, and the duty of care alongside current Philippine regulations, this research seeks to identify legal gaps and propose policy reforms that would better protect children in the digital space. Ultimately, strengthening online safety measures is not about restricting technological progress, but about ensuring that digital platforms become responsible allies in safeguarding the well-being of young users.

The internet's origins can be traced back to the 1960s, when the U.S. Department of Defense set out to develop a secure and dependable communication network for wartime contingency. The Advanced Research Projects Agency Network (ARPANET), developed in 1969,[18] was the first fully network to utilize packet-switching technology. It allowed multiple computers to communicate on a single network, laying the groundwork for the modern internet.[19]

---

[16] Ibid

[17] Masnick (2025). Blumenthal So Eager to Bring Back KOSA, He admits its purpose is Censorship. Available at: https://www.techdirt.com/2025/01/09/blumenthal-so-eager-to-bring-back-kosa-he-admits-its-purpose-is-censorship/ (Accessed on February 20, 2025)

[18] ARPANET, established in the late 1960s by the Advanced Research Projects Agency (ARPA, now DARPA) of the U.S. Department of Defense, was developed as the first wide-area packet-switched network to support distributed control and became one of the earliest networks to implement the TCP/IP protocol suite. The goal of ARPANET was to create a resilient communication network for researchers and military installations, designed to maintain connections even in the event of system failures.

[19] History Tools. (n.d.). The complete guide to ARPANET: The groundbreaking computer network that led to the Internet. Available at: https://www.historytools.org/concepts/arpanet-complete-guide#google_vignette (Accessed on September 3, 2024)

Over the next decades, the internet evolved from a military tool to a research and academic platform, driven by universities and technological innovations like Transmission Control Protocol/Internet Protocol ("TCP/IP") in the 1970s.[20] The 1980s and 1990s marked the commercialization of the internet, with the emergence of web browsers such as Mosaic and Netscape, thereby popularizing the World Wide Web.[21] This period also experienced the emergence of countless websites and online services, greatly broadening internet accessibility for the general public.[22] The late 1990s and early 2000s witnessed an explosion in internet usage, fueled by the advent of high-speed internet connections, the rise of social media platforms, and the proliferation of mobile devices. This period saw the emergence of online communities, businesses, and content-sharing sites that transformed the way people interacted and consumed information online.

Social media platforms were the driving force behind this transformation. MySpace, launched in 2003, gained immense popularity, particularly among younger users, by allowing them to create personalized profiles, connect with friends, and share various forms of media. MySpace's success paved the way for future platforms and demonstrated the power of social networking.[23] Facebook, launched in 2004, quickly became the dominant social media platform, attracting a broader audience with its user-friendly interface and emphasis on real-world connections. Its exponential growth solidified its position as the go-to platform for social networking.[24] Other platforms like Twitter (now X), with its microblogging format, facilitated real-time communication and became a powerful tool for news dissemination and public discourse. The social web also revolutionized media consumption and creation through platforms like YouTube. Launched in 2005, YouTube empowered individuals to become content creators, sharing their videos with a global audience. This democratization of media led to the rise of "YouTubers" and significantly impacted culture, entertainment, and media.[25]

The mid-2000s marked a significant turning point with the rise of these platforms, fundamentally changing how people connected and communicated online. They fostered social interaction on an unprecedented scale, allowing users to share updates, photos, videos, and thoughts with friends and family across the globe. By the late 2000s and early 2010s, visually-driven platforms like Instagram (2010) and TikTok (2016), gained immense popularity, particularly among younger audiences. These platforms, with their emphasis on visual content and short-form videos, further increased children's engagement with digital tools and online communities. This trend underscored the growing influence of social media in shaping the digital experiences of younger generations. However, the trajectory of online interaction underwent a dramatic

[20] The origins of the internet can be traced back to the late 1960s, during the height of the Cold War. The United States Department of Defense, seeking to create a decentralized communication system that could withstand potential attacks, funded a research project that led to the development of ARPANET
[21] Valeria, H. (2024) History of World Wide Web. Available at: https://gloriathemes.com/the-history-of-the-world-wide-web/ (Accessed on February 25, 2025)
[22] Internet History of the 1970s. (n.d.). *Internet History*. Computer History Museum. Available at: https://www.computerhistory.org/internethistory/1970s/ (Accessed on September 3, 2024)
[23] Ibid.
[24] Ibid.
[25] Ibid.

shift with the onset of the COVID-19 pandemic in early 2020. The pandemic brought about unprecedented changes to daily life across the globe, disrupting almost every aspect of human activity, including education.[26] In response to the escalating COVID-19 pandemic, the Philippine government implemented a series of measures to curb the spread of the virus. Initial actions included contact tracing and travel bans on foreign nationals from affected countries. However, these measures proved insufficient as the number of cases continued to rise.[27] The government then imposed community quarantines, starting with Metro Manila and eventually extending to the entire island of Luzon. These quarantines involved social distancing measures, class suspensions, travel restrictions, and the closure of non-essential businesses. These restrictions, while necessary, led to panic and disruptions in daily life. To further control the spread, enhanced community quarantines were implemented, including strict home quarantines, suspension of public transportation, and heightened enforcement of quarantine procedures. These measures aimed to limit movement and interaction, ultimately leading to the widespread closure of schools, playgrounds, and recreational facilities.

In line with the aforementioned information, these stringent measures resulted in a fundamental shift in children's lives, with physical gatherings and in-person activities restricted, and many aspects of their daily routines moving online.[28] The abrupt shift from traditional classroom learning to remote education stands as one of the most transformative changes in recent educational history. Schools rapidly embraced online learning platforms, which swiftly became the dominant mode of instruction. According to Atty. Felson Dalaguete's 2021 article:

> *"The COVID-19 Pandemic has changed the landscape of a lot of industries and sectors. The education sector is not an exception. With several restrictions on the conduct of face-to-face classes imposed by various governments around the globe, schools have resorted to different modes of learning delivery. One of these modes is online delivery of learning."*[29]

This unprecedented transition forced children, including those in preschool, to drastically increase their screen time, engaging in virtual classes, completing assignments, and interacting with educators and peers through digital interfaces. Instead of traditional face-to-face learning, young children had to adapt to virtual classrooms, where lessons were conducted through video calls, digital learning apps, and interactive platforms.

Beyond attending online classes, they also had to complete assignments using educational software, submit tasks through learning management systems, and rely on digital tools for assessments.[30] This sudden adaptation not only altered the physical space of learning but also redefined the very nature of

---

[26] The Philippines in the time of COVID-19: Early experiences and challenges of a resource-limited country. Available at: https://ojs.wpro.who.int/ojs/public/journals/1/covid19/wpsar.2020.11.5.005Amit.pdf (Accessed on February 25, 2025)
[27] Ibid
[28] Senate Economic Planning Office. (2022). COVID-19 School Closures: Lessons from Disrupted Learning. p. 6.
[29] *The Sufficiency of our Data Privacy Laws to Protect Children's Personal Data in the Midst of Online Learning*. Dalaguete (2021) page 126
[30] *Ibid*., p. 8

educational engagement, raising concerns about screen time, digital equity, and the long-term impact on students' social and academic development.[31]

The COVID-19 pandemic has created the largest disruption of education systems in history, affecting nearly 1.6 billion learners in more than 190 countries and all continents. Ninety-four percent (94%) of the world's student population have been affected by the closure of schools and other learning spaces, while 99% of affected learners in low and lower-middle income countries.[32] This education crisis has stimulated innovations within the education sector through distance learning solutions that support education continuity.[33]

In the Philippines, 25.08 million school-age children enrolled in public schools and private schools nationwide for Academic Year (A.Y.) 2020-2021. This is a 10% drop in enrollment, considering that in A.Y. 2019-2020, the total enrollment nationwide is 27.7 million.[34] Seven hundred forty-eight (748) out of 14,485 private educational institutions suspended operations, affecting 3,233 teachers and 40,345 learners.[35] The Department of Education (DepEd) launched the Basic Education-Learning Continuity Plan (BE-LCP) to help teachers and students cope with the challenges of remote learning. The BE-LCP calls for schools to use "blended" approach to teaching based on a mix of "modular" learning and online classes.[36] The adoption of distance or remote learning through online classes means that various platforms, software programs, applications, and learning management systems (LMS) would become a regular part of a learner's education. This has raised a lot of data privacy concerns on how all this technology will be collecting, storing, and using student's personal information.[37]

In her 2022 book, Rhuperdia Crowe-Clay emphasizes that online learning will continue to be an integral part of classroom culture even after the pandemic. Consequently, schools are partnering with educational technology companies to enhance access to digital tools, ensuring that technology is both accessible and relevant to all learners. This evolution marks a significant shift in the mindset of the broader educational community.[38]

With the advent of blended learning, conducting a "make-up class" due to severe weather is now a thing of the past. Modern lesson plans in the 21st century incorporate both asynchronous modules and synchronous sessions using platforms like Zoom. Suffice it to say, online learning is a highly viable solution

---

[31] Senate Economic Planning Office. (2022, December). COVID-19 School Closures: Lessons from Disrupted Learning. p. 11

[32] United Nations (August 2020). *Policy Brief: Education during COVID-19 and Beyond.* United Nations.

[33] *Ibid.*

[34] Hernando-Malipot, Merlina (1 Oct 2020). *DepEd Reports over 24M Enrollees this School Year. https://mb.com.ph/2020/10/01/deped-reports-over-24-m-enrollees-this-school-year/.*

[35] CNN Philippines (9 Sep 2020). Available at: *748 Private Schools suspend operations, this school year, DepEd says. https://www.cnnphilippines.com/news/2020/9/9/Private-schools-temporary-closure-DepEd-html.*

[36] Economics Policy Research Institute, UNICEF, UNDP (December 2020). *Final Report: The Impact of the COVID-19 Crisis on Households in the National Capital Region of the Philippines.* EPRI, UNICEF, UNDP

[37] Herold, B. (11 Aug 2020). *School Reopening Bring Wave of COVID-19 Student-Data Privacy Concerns.* Education Week. Available at: https://www.edweek.org/technology/school-reopenings-bring-wave-of-covid-19-student-data-privacy-concerns/2020/08 (Accessed on February 25, 2025)

[38] Crowe-Clay, R. (2022). In C. J. Bonk & M. Zhu (Eds.), Transformative Teaching Around the World: Stories of Cultural Impact, Technology Integration and Innovative Pedagogy (p. 252).

for unplanned teacher absences, whether due to natural calamities or another global pandemic.[39]

The transition to online learning, born out of necessity, has fundamentally reshaped children's relationship with the digital world, extending their online presence far beyond the virtual classroom. This new reality has normalized prolonged screen time, not just for academic pursuits but also for social interaction and entertainment. The limitations imposed by social distancing measures, which curtailed traditional in-person gatherings, propelled children toward social media platforms as a primary means of maintaining and fostering connections.

The digital landscape of children's social lives underwent a rapid transformation, with platforms like Zoom, WhatsApp, Instagram, and TikTok becoming indispensable tools for connection and interaction. These platforms served as virtual hubs, allowing children to maintain friendships, share experiences, and participate in group activities despite the limitations of physical distancing. Notably, TikTok experienced a surge in popularity, providing a creative outlet through short-form video creation and enabling participation in viral challenges. This platform, in particular, became a crucial means for children to preserve a sense of community and shared experience, effectively mitigating the feelings of isolation imposed by physical separation. The widespread adoption of these technologies underscored their vital role in sustaining social connections and fostering a sense of belonging during a period of unprecedented social change.

While many children exhibit remarkable proficiency in using technology for communication and entertainment, a significant gap often exists in their understanding of essential digital literacy skills. This disparity creates a vulnerability, as children may lack the knowledge and awareness to navigate the online world safely and responsibly. Concepts such as managing privacy settings, recognizing suspicious behavior, understanding the permanence of online actions, and knowing how to respond to inappropriate content are often unfamiliar to them. This knowledge gap leaves children more susceptible to online risks, including scams, phishing attempts, cyberbullying, and exposure to harmful or inappropriate content. The absence of these crucial digital literacy skills underscores the need for comprehensive education and guidance to empower children to become informed and responsible digital citizens.

The blending of educational and social activities online[40] blurred the lines between structured learning time and free browsing, often leading to unstructured and unsupervised use of social media. This blurring effect has resulted in a significant amount of unsupervised social media usage, as children navigate a digital environment where educational platforms and social media networks often coexist and overlap. The extended time spent online, while facilitating learning and social connection, has also raised valid concerns about

[39] Ibid.
[40] Senate Economic Planning Office. (2022, December). COVID-19 School Closures: Lessons from Disrupted Learning. p. 6.

children's exposure to potentially inappropriate content.[41] This 24/7 access to digital platforms heightened children's vulnerability. Unlike the oversight typically available in physical environments like schools, parents found it challenging to keep track of their children's online activities. The pandemic's sudden shift to digital life not only made social media a staple in children's daily routines but also revealed gaps in digital safety and well-being that require urgent attention.[42] At the same time, the surge in online activity coincided with a rise in misinformation, especially around topics like health and the pandemic. Children, who may lack the critical thinking skills necessary to identify credible sources, were particularly vulnerable to being misled by false or harmful information. This exposure not only distorted their understanding of the world but also posed risks to their mental and emotional well-being.[43] The reduced level of parental supervision during this period presented significant risks. Many children explored the internet with less guidance, increasing their exposure to online dangers, including potential interactions with predators in chat rooms, gaming platforms, and social media sites. These predators often masked their intentions behind seemingly friendly interactions, making it easier to exploit children increased online presence.[44]

The convergence of reduced parental oversight, increased time online, and limited digital literacy during the pandemic created a precarious situation for children navigating the digital world. This echoes the early days of the internet, where a lack of understanding and regulation led to unforeseen consequences. Just as the internet's rapid expansion in the 1990s and 2000s brought about challenges related to privacy, security, and misinformation, the pandemic-induced surge in children's online activity exposed vulnerabilities in digital safety.

The internet's history is a testament to the rapid pace of technological advancement, often leaving ethical considerations and safeguards struggling to catch up. This pattern was glaringly apparent during the COVID-19 pandemic, as children's increased online presence exposed vulnerabilities in their digital safety.

Looking back, the early internet was a Wild West, with limited regulation and understanding of its potential impact. Issues like cyberbullying, privacy breaches, and exposure to harmful and inappropriate content emerged as the internet grew, prompting reactive measures to address these challenges. Similarly, the pandemic forced a sudden shift to online learning and social interaction for children, without adequate preparation or comprehensive safety measures in place. This historical context underscores the need for a proactive approach to child online safety. By learning from the past and anticipating future challenges, a digital environment can be fostered where children can thrive without compromising their well-being. This necessitates a collective effort from policymakers, tech companies, educators, and parents to prioritize child online

[41] Saini, N., & Mir, S. (2023, August). Social Media: Usage And The Impact On Education. *Journal of Namibian Studies*, *33*(i),p. 4677.
[42] Ibid., p.4683
[43] Ibid., p.4686
[44] Mintz, S. (2004). Huck's raft: A history of American childhood. Belknap Press. p.4685

safety and ensure that technological progress aligns with ethical considerations and safeguards.

II. CONTEXT

The pandemic revealed that while the internet can be a powerful tool for connection and learning, it also exposes minors to a range of dangers, from cyber threats to mental health issues. As discussed, while online platforms provided a way to stay connected during isolation, it also introduced new challenges in maintaining children's digital safety and well-being.

Despite these risks, the Philippines lacks a comprehensive regulatory framework specifically designed to safeguard children in online spaces. Existing laws primarily address cybercrime and general child protection but fail to provide targeted safeguards against social media risks, such as algorithm-driven content exposure, exploitative data practices, and the absence of platform accountability. Without concrete policies that hold online platforms responsible for ensuring child safety, Filipino children remain vulnerable to a digital ecosystem that prioritizes engagement and profit over their well-being. This lack of regulation makes children particularly vulnerable to inappropriate content, such as pornography, explicit materials, and violent content, which may be detrimental to their development.

Discussions on protecting children online through acts like the U.S. Kids Online Safety Act gained more attention as policymakers recognized the heightened risks during COVID-19. Meanwhile, in the Philippines, several laws have been enacted to safeguard the rights and welfare of minor children across various settings, including social media. The growing prevalence of social media use among minors underscores the urgent need for targeted, up-to-date regulations—such as those in the U.S. Kids Online Safety Act—that directly addresses the risks children face in the digital age. This article aims to examine the extent to which the U.S. framework for protecting children online—recognized for its comprehensive and structured approach—aligns with the objectives of ensuring social media safety for children. At the same time, it will assess whether existing Philippine laws, while offering some degree of protection, adequately address the unique threats children face in digital environments. Philippine regulations provide a general framework for safeguarding children online, but they often integrate digital threats within broader child protection or cybercrime laws rather than focusing specifically on social media safety. By analyzing these differences, this article seeks to determine whether adopting elements of the U.S. approach can enhance the effectiveness of child online protection laws in the Philippines. By examining the strengths of KOSA and comparing them with Philippine laws, this article aims to identify key areas for legal reform that can better protect Filipino children from online threats.

This article holds significant value in shaping the future of child protection in digital spaces. This analysis allows for the identification of critical gaps and areas for improvement, particularly in establishing a clear duty-of-care framework for online platforms. By highlighting these areas, the research aims to

influence legislative reforms and promote the adoption of more robust child protection measures in the digital sphere.

Beyond its legal implications, this article also holds significant implications for the legal profession, particularly in shaping the evolution of technology law and child protection policies in the Philippines. By critically analyzing existing legislation and comparing it with international best practices, legal practitioners, policymakers, and scholars can gain a deeper understanding of the gaps in current regulations.

This research provides a strong legal foundation for drafting new policies, guiding judicial interpretations, and advocating for stronger enforcement mechanisms. Furthermore, it equips legal professionals with the knowledge and tools necessary to navigate emerging legal challenges in the digital age, ensuring that children's rights remain protected amidst rapid technological advancements.

As technology continues to advance, the need for proactive and adaptive legal frameworks becomes even more pressing. This research emphasizes that protecting children online is not just about addressing current risks—it is about establishing a foundation for future generations to navigate the digital world safely. Future generations deserve an online environment where they can explore, learn, and connect without being exposed to harmful content, data exploitation, or manipulative algorithms. This article advocates for laws that will make online platforms active partners in child protection, ensuring they uphold their responsibility in fostering a secure and age-appropriate digital space.

By advocating for proactive and adaptive legal mechanisms that prioritize child welfare, this article aspires to drive meaningful policy changes that will ensure a more secure and child-friendly digital landscape in the Philippines. Ultimately, it seeks to contribute to ongoing efforts to protect children's rights and well-being in the ever-expanding digital world.

III. THE DILEMMA

The rise of social media usage among children highlights a significant gap in legal protections in the Philippines. Existing laws, such as but not limited to the Data Privacy Act and the Anti-Child Pornography Act, provide general protections but fall short in addressing the nuances of social media use by children. These laws do not contain specific provisions for protecting children's data, monitoring the content they encounter, or regulating the algorithms that may expose them to harmful material.

Meanwhile, the U.S. Kids Online Safety Act mandates that platforms provide safe settings for children and transparency for their guardians, demonstrating a more comprehensive approach to protecting young users. This thesis explores how Philippine laws can adapt and evolve to offer children the same level of protection. To this end, this thesis seeks to analyze and answer the following questions:

1. How do existing Philippine laws and jurisprudence protect children from online activities?
2. How does the U.S. Kids Online Safety Act regulate children's use of online platforms?
3. How can Philippine legislation incorporate best practices, such as the "duty of care" principle, to effectively address the need for protecting children from harmful content on social media platforms?

IV. WHY CHILDREN?

During childhood, a child requires continuous attention, guidance, nourishment, comfort, and opportunities for enjoyment. These fundamental needs shape not only a child's well-being but also their overall development into a self-sufficient individual.[45] According to Kant in 1997, because children are brought into the world involuntarily, parents bear a moral duty to ensure conditions that nurture their growth, equipping them with the necessary skills and values to navigate life. This principle of parental responsibility is echoed in the preamble of the United Nations Convention on the Rights of the Child (UNCRC):

> *"Recognizing that the child, for the full and harmonious development of his or her personality, should grow up in a family environment, in an atmosphere of happiness, love, and understanding."*[46]

This statement underscores the importance of a supportive and nurturing environment in fostering a child's emotional, cognitive, and social development. The role of parents and guardians extends beyond merely providing for basic needs; it involves actively shaping the child's capacity for self-determination, decision-making, and personal agency.[47]

As children mature, they progressively develop their ability to exercise autonomy. However, during their formative years, they rely on their parents or guardians to act in their best interests, making decisions that ensure their safety, security, and well-being.[48] While children possess a negative right to liberty—meaning they should be free from undue interference—their positive liberty, which involves the ability to make informed choices and participate meaningfully in society, must be cultivated under the guidance of their caregivers.[49] In this context, parents and guardians act as intermediaries, approximating the child's best interests while gradually preparing them for independent decision-making.[50] It is crucial to distinguish between positive liberty and positive rights to avoid conflating the two. Child protection policies

---

[45] Professional Child Protection and the Child's Freedom of Expression," in *Professional Practice in Child Protection and the Child's Right to Participate*, eds. A. Falch-Eriksen & K. Toros (Routledge, 2021), p.41.
[46] *UN 1989, p. 1*
[47] Brighouse, H. (2002). *School choice and social justice.*
[48] *Ibid.*
[49] MacMullen, I. (2015). *Faith in schools? Autonomy, Citizenship, and Religious Education in the Liberal State.*
[50] *Ibid.*

primarily focus on preserving the negative rights of children—ensuring they are free from harm, abuse, exploitation, and neglect—while also addressing the nuanced balance between restriction and empowerment.[51]

Positive liberty, meanwhile, pertains to the child's ability to exercise freedom effectively within society, engage in meaningful participation, and develop the necessary competencies to assert their rights as individuals.[52] While social and welfare rights contribute to a child's well-being, they form a distinct category that falls beyond the immediate scope of this discussion.

In essence, childhood is a critical period in which the foundations for future autonomy and self-governance are laid. Parental guidance must strike a balance between protection and gradual empowerment, ensuring that children not only grow up in an environment of care and support but also acquire the skills and confidence necessary to exercise their freedoms responsibly in adulthood.[53]

EARLY EXPOSURE TO SOCIAL MEDIA

Before children even take their first steps, their digital footprints are already being established—often beginning before birth. Parents utilize fertility apps, participate in trending maternity photo shoots, share ultrasound images, and post newborn photos online. AI-powered baby monitors, cloud-stored baby pictures, and digital records of medical checkups further contribute to their expanding digital presence, creating a data trail that begins in infancy and continues to grow over time.

As they mature, their daily activities are increasingly monitored through daycare updates, school cafeteria payment systems, electronic health records, and surveillance technologies. These digital records collectively form a comprehensive profile that follows them into adulthood, shaping their online identity long before they have the ability to manage it themselves. Unknowingly, parents, educators, and other trusted adults contribute to this extensive data trail, often without considering its long-term implications. These digital records, once shared, may become permanently accessible to friends, employers, corporations, and even law enforcement.

Leah Plunkett, in *Sharenthood: Why We Should Think Before We Talk About Our Kids Online*,[54] explores how the widespread practice of sharing children's data—whether through social media, educational platforms, or digital monitoring—poses significant privacy risks. She examines how well-intentioned

[51] Berlin, I. (1958). *Two concepts of liberty*
[52] Feinberg, J. (1980). *The child's right to an open future.*
[53] Archard, D. (2020). *Children: Rights and childhood* (3rd ed.).
[54] Definition of *Sharenthood*: It refers to the widespread practice of parents, guardians, and other trusted adults sharing children's personal information—such as photos, milestones, and daily activities—on social media and digital platforms, often without considering the long-term privacy risks. Coined by Leah Plunkett, the term highlights how this form of digital exposure, while typically well-intentioned, contributes to the creation of a child's digital identity before they have the ability to control or consent to it. It raises concerns about data commodification, digital surveillance, and the potential lifelong consequences of early online exposure, emphasizing the need for stronger legal protections to safeguard children's privacy in an increasingly digital world. Leah A. Plunkett, *Sharenthood: Why We Should Think Before We Talk About Our Kids Online* (The MIT Press, 2019), Available at: https://doi.org/10.7551/mitpress/11756.001.0001. (Accessed on February 20, 2025)

but excessive data-sharing can lead to unintended consequences, shaping a child's digital identity long before they have the ability to control it.

Plunkett introduces the concept of sharenting—the practice of parents and guardians voluntarily sharing details of their children's lives on social media and other digital platforms. While often done with good intentions, this practice can have lasting consequences, including the commodification of children's personal data, exposure to digital surveillance, and the loss of control over their own narratives. She warns that the digital footprints created by parents today may follow children into adulthood, influencing their educational, professional, and personal opportunities.[55] This perspective is particularly relevant to discussions on legal frameworks designed to protect children online.

Plunkett critiques how existing laws, instead of imposing restrictions on excessive data-sharing practices, tend to reinforce a system where children's personal data becomes a commodity for corporations and digital platforms. She highlights the structural biases in legal regimes that implicitly encourage parental data-sharing, often under the guise of parental consent, without providing children with mechanisms to reclaim their digital privacy in the future.[56]

In the context of this thesis, this phenomenon highlights the urgent need for stronger legal protections to safeguard children's digital privacy. The Philippines' Data Privacy Act of 2012 (Republic Act No. 10173) establishes general principles of data protection, which will be examined in detail in succeeding sections. This thesis assesses whether the Act lacks specific provisions addressing children's online exposure and the risks associated with sharenting. Plunkett's work also highlights the broader societal implications of excessive digital exposure during childhood. She argues that sharenting is not merely a personal choice but a practice encouraged by corporate structures that thrive on data collection and targeted advertising.

Social media platforms are designed to promote oversharing, while governments often fail to implement policies that prioritize children's privacy over commercial interests. This raises an important question: *should the responsibility for protecting children's digital rights rest solely on parents, or should laws evolve to place greater accountability on digital platforms and regulatory bodies?*

As digital technology continues to evolve, the challenge remains: *how can legal frameworks ensure that children's rights to privacy and autonomy are preserved in a world where their digital identities are shaped before they even have the agency to understand or consent to it*? Plunkett's work serves as a crucial reference point in analyzing how existing laws, including those in the Philippines, can be re-examined and strengthened to provide clearer, more robust protections for children in the digital space. Addressing these gaps would allow policymakers to develop a legal framework that not only safeguards children from external threats but also considers the long-term consequences of parental and institutional data-sharing practices.

---

[55] *Ibid.*
[56] *Ibid.*

CHILREN'S RIGHTS IN INTERNATIONAL AND PHILIPPINE LAW

Franklin Delano Roosevelt once stated: *"We cannot always build the future for our youth, but we can build our youth for the future."* This principle is especially relevant in today's rapidly evolving digital landscape, where technology presents both opportunities and challenges. While digital innovations enhance education and engagement, they also introduce significant risks, necessitating stronger protective measures from all stakeholders.[57]

To maximize the advantages of technology and advance children's welfare, it is essential for policymakers, educators, and parents[58] to work together, ensuring that these innovations safeguard and empower children as they explore the digital world. Children are a nation's most valuable resource. Prioritizing their well-being and providing opportunities for meaningful lives is essential.[59] As early as 1974, the Philippine government recognized that its responsibility to protect children extends beyond meeting their basic needs such as education, healthcare, and safety. It also includes shielding them from the unique challenges while actively promoting their welfare in an evolving environment. Legal scholars like Jorge Coquia, in his book Human Rights, emphasizes the need for special protection and care for children due to their age and developmental stage. Philippine law defines children as individuals under 18, reflecting this commitment.[60] This principle is also central to the United Nations Convention on the Rights of the Child (UNCRC), adopted in 1989. [61]

The UNCRC is the most comprehensive international framework for children's rights. It encompasses provision and protection rights and affirms children's right to participate in society, especially in decisions affecting their lives.[62] It also serves as the global framework for child protection, establishing fundamental rights that all countries must uphold. These rights encompass a child's right to privacy, autonomy, and protection from exploitation, forming the basis for national policies and legal systems worldwide.[63] Article 3, paragraph 1 of the UNCRC provides:

> *"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."*[64]

---

[57] Crowe-Clay, R. (2022). *Transformative teaching around the world: Stories of cultural impact, technology integration, and innovative pedagogy*
[58] Article 13. Social and Emotional Growth, PD No. 603
[59] Presidential Decree No. 603, Child and Youth Welfare Code, December 10, 1974, Art. 1.
[60] Republic Act No. 6809, An Act Lowering the Age of Majority from Twenty-One to Eighteen Years, February 21, 1990.
[61] United Nations, Convention on the Rights of the Child, November 20, 1989, Treaty Series, vol. 1577, p. 3. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (February 20, 2025)
[62] Kosher, H., Ben-Arieh, A., & Hendelsman, Y. (2016). Children's Rights and Social Work.
[63] Falch-Eriksen, A. (2018). *Human rights in child protection: Implications for professional practice and policy*
[64] Committee on the Rights of the Child. (2013). General Comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration (Art. 3, Para. 1) (Comment No. 14).

Governments that have ratified the UNCRC are obligated to implement these rights in their legal frameworks, ensuring that children have not only theoretical protections but also practical mechanisms to enforce their rights. While the UNCRC mandates that children's rights be upheld in administrative and judicial proceedings,[65] it remains unclear whether digital platforms and parental data-sharing practices align with this obligation.

The UNCRC guarantees that children must be given a voice in matters that affect them, yet children often have little to no control over their digital presence, which is shaped by parents, corporations, and government policies without their consent. The practice of sharenting—where parents and guardians voluntarily share children's personal data on social media and other digital platforms—exemplifies this gap in child rights protection. Philippine Supreme Court Associate Justice Marvic Leonen has consistently emphasized the *"best interest of the child"* in his concurring and dissenting opinions across various cases, underscoring that children's welfare, emotional stability, and overall development should take precedence in legal proceedings. This principle extends beyond traditional legal matters and is especially relevant in the digital age.[66]

In 2021, the UN Committee on the Rights of the Child finally recognized that children's rights extend to the digital realm,[67] reinforcing the need for stronger protections against data exploitation and privacy violations. However, despite this recognition, children's digital rights are frequently undermined. Many lack awareness of their digital footprint, and even when they do, they have limited avenues to contest parental data-sharing practices or corporate data collection. This growing gap highlights the urgent need for legal frameworks that empower children to protect their digital identities and ensure their best interests remain safeguarded online.

CHALLENGES OF THE DIGITAL AGE

According to Atty. Dalaguete's article[68], technology has assumed an even more prominent role in children's lives since the COVID-19 pandemic took hold. Data-powered technologies have been used to track, trace, and control the infection rate, as well as continue the provision of education, health, and social services to children while government-imposed lockdowns are being implemented.[69]

In education, schools have shifted to technology-enabled remote learning. This shift required children to use online platforms to access education; thus, true consent is not possible - they must provide their personal data in exchange for accessing their fundamental right to education.[70] This situation falls squarely with the challenge of obtaining informed consent of children. Additionally, the

[65] *Ibid.*
[66] Briones v. Miguel, G.R. No. 156343 (2005) [as per J. Panganiban]
[67] *Committee on the Rights of the Child.* (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment.
[68] *The Sufficiency of our Data Privacy Laws to Protect Children's Personal Data in the Midst of Online Learning*. Dalaguete (2021) page 126
[69] Referee, Linda; Day, Emma; and Byrne Jasmina (August 2020). *COVID-19: A spotlight on child data governance gaps. United Nations Children's Fund* (UNICEF)
[70] *Ibid.*

utilization of online learning platforms places the burden of determining the acceptability of the platform or application's data protection and privacy policies to educators and school systems. Normally, teachers and school administrators do not have the knowledge, time, or capacity to review terms and conditions from privacy policies. Hence, the urgency has concentrated on bringing necessary services to children, and less attention has been paid to privacy and protection of data.[71] The shift to remote learning also increased children's use of social media and the internet. Children in many parts of the world are spending more time online to connect with friends or to keep themselves entertained. This increased use of the internet puts in the spotlight the issue of persistency of data.

Without regular supervision of their parents or legal guardians, children may unknowingly give consent to the processing of their information without being fully aware of the risks involved in the processing. The vast amount of children's data that can be collected and stored through this uninformed giving of consent can have a significant effect over the children's lifetime. In response, the Philippines has introduced and strengthened several laws to address critical online issues affecting minors, including data privacy, online exploitation, child pornography, and cyberbullying.

V. EXISTING PHILIPPINE LAWS

This section will provide an in-depth analysis of existing laws in the Philippines to protect minors in their online activities. Each law addresses specific aspects of online safety, targets a broad range of online crimes, including guaranteed privacy protection for children, and is expanded to include protections against cyberbullying, human trafficking, child pornography, and all forms of exploitation. Through this comprehensive analysis, insights are gained into how the Philippine legal system seeks to adapt to evolving digital risks. This will explore the purpose of these laws in practice, addressing both their successes and the challenges that remain in ensuring comprehensive protection for children in the digital age.

R.A. 9775 – Anti-Child Pornography Act of 2009

Child pornography in the Philippines poses a serious and growing threat, largely driven by the escalating levels of poverty. As a result, the country has become a global epicenter for the live-streaming[72] of child sexual abuse.[73] The Luxembourg Guidelines, which provide a standard terminology for discussing child sexual abuse and exploitation, emphasize the importance of using precise language in addressing such crimes, as terms like "child pornography" can trivialize and undermine the severity of the abuse.

---

[71] *Ibid.*

[72] *Republic Act No. 11930*, *Anti-Online Sexual Abuse or Exploitation of Children and Anti-Child Sexual Abuse or Exploitation Materials Act*, July 30, 2022. Streaming refers to the broadcasting or viewing through the use of ICT, whether the viewer is passively watching or actively directing the content. It is considered live-streaming when the broadcasting or viewing occurs in real-time.

[73] Anti-Money Laundering Council. (2020). *Child pornography in the Philippines: Post-2019 study using STR data. Page 3*

In light of this alarming trend, the Anti-Child Pornography Act (Republic Act No. 9775) serves a crucial role in safeguarding vulnerable minors from sexual exploitation and abuse. By prohibiting the use of children in any pornographic material whether for creation or production of any form, the law aims to protect children from being victimized and exploited in both digital and physical spaces.

> "Republic Act No. 9775, Anti-Child Pornography Act of 2009, Sec. 4 (a).Section 9. Duties of an Internet Service Provider (ISP). - All internet service providers (ISPs) shall notify the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility.
>
> Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person: Provided, That no ISP shall be held civilly liable for damages on account of any notice given in good faith in compliance with this section.
>
> Furthermore, an ISP shall preserve such evidence for purpose of investigation and prosecution by relevant authorities.
>
> An ISP shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address which contains any form of child pornography.
>
> All ISPs shall install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered.
>
> An ISP who shall knowingly, willfully and intentionally violate this provision shall be subject to the penalty provided under Section 15(k) of this Act.

The law's provisions requiring internet service providers (ISPs) to block access to websites featuring child pornography represent a proactive approach to child protection.[74] Likewise, the law's comprehensive scope extends to all forms of distribution, ensuring that children are not exploited for commercial gain through various media, including social media platforms and websites. Hosts must prevent child exploitation materials from appearing on their platforms and are required to report any instance of such material to the appropriate authorities. Accordingly, An internet content host must adhere to the following requirements:

> "Section 11. Duties of an Internet Content Host. - An internet content host shall:
>
> (a) Not host any form of child pornography on its internet address;

[74] Ibid., Sec. 9

(b) Within seven (7) days, report the presence of any form of child pornography, as well as the particulars of the person maintaining, hosting, distributing or in any manner contributing to such internet address, to the proper authorities; and

(c) Preserve such evidence for purposes of investigation and prosecution by relevant authorities.

An internet content host shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address that contains any form of child pornography.

An internet content host who shall knowingly, willfully and intentionally violate this provision shall be subject to the penalty provided under Section 15(j) of this Act: Provided, That the failure of the internet content host to remove any form of child pornography within forty-eight (48) hours from receiving the notice that any form of child pornography is hitting its server shall be conclusive evidence of willful and intentional violation thereof.

This legal framework establishes a comprehensive system for protecting children online. By mandating internet content hosts to adhere to the Luxembourg Guidelines, it ensures standardized reporting and facilitates international collaboration in combating child pornography or a transnational crime.

"Section 22. Child Pornography as a Transnational Crime. - Pursuant to the Convention on transnational Organized Crime, the DOJ may execute the request of a foreign state for assistance in the investigation or prosecution of any form of child pornography by:

(1) conducting a preliminary investigation against the offender and, if appropriate, to file the necessary charges in court;

(2) giving information needed by the foreign state; and

(3) to apply for an order of forfeiture of any proceeds or monetary instrument or properly located in the Philippines used in connection with child pornography in the court; Provided, That if the DOJ refuses to act on the request of for delaying the execution thereof: Provided, further, That the principles of mutuality and reciprocity shall, for this purpose, be at all times recognized."

Simultaneously, it prioritizes the child victim's right to privacy throughout investigation and prosecution, and mandates the Department of Social Welfare and Development (DSWD) to provide necessary care and support for their recovery and reintegration.[75]

[75] Ibid., Sec. 14

Furthermore, the clear definition of child pornography and the inclusion of penalties for grooming[76], luring[77] and pandering[78] emphasize the law's commitment to addressing these crimes at multiple levels. This holistic approach not only seeks to deter potential offenders but also enhances the overall safety and well-being of children.

R.A. 10364 – Expanded Anti-Trafficking in Persons Act of 2012

Congress enacted R.A. 9208[79], known as the Anti-Trafficking in Persons Act of 2003, which was later expanded by R.A. 10364. This law penalizes a range of activities, including the recruiting, transporting, or harboring of children for the purpose of engaging in pornography.[80]

A significant aspect of the law is its establishment of the principle that a victim's consent is irrelevant and cannot be used as a defense in prosecuting the unlawful acts prohibited by this Act. Relevant jurisprudence appears to affirm that claims of victim consent neither exempt nor mitigate the offenders' criminal liability and an accused person cannot capitalize on the fact that the victims were recruited freely and voluntarily. This reasoning appears to explain the successful prosecution of a number of trafficking cases that may formerly have been prosecuted as pimping.

It broadly defines pornography as any depiction of a child, whether through publication, exhibition, film, indecent shows, information technology, or other mediums, that involves a person engaging in real or simulated explicit sexual activities. This definition also includes any representation of a person's sexual parts intended primarily for sexual purposes.[81]

The law also introduced additional grounds for Qualified Trafficking[82] which are subject to severe penalties, including life imprisonment. In a recent case of People v. Gumba and Rellama[83], the Supreme Court has upheld the life imprisonment and 2 Million pesos fine imposed on Rizalina Janario Gumba and Gloria Bueno Rellama for qualified human trafficking.

In a decision written by Senior Associate Justice Marvic M.V.F. Leonen, the Court's Second Division affirmed the convictions by the Court of Appeals and the Pasay City Regional Trial Court. Gumba and Rellama were found guilty

---

[76] h. *"Grooming"* refers to the act of preparing a child or someone who the offender believes to be a child for a sexual activity or sexual relationship by communicating any form of child pornography. It includes online enticement, or enticement through any other means.
[77] i. *"Luring"* refers to the act of communicating, by means of a computer system, with a child or someone who the offender believes to be a child for the purpose of facilitating the commission of a sexual activity or production of any form of child pornography.
[78] j. "*Pandering"* refers to the act of offering, advertising, promoting, representing or distributing through any means any material or purported material that is intended to cause another to believe that the material or purported material contains any form of child pornography, regardless of the actual content of the material or purported material.
[79] Republic Act No. 9208 or commonly known as *Anti-Trafficking in Persons Act of 2003*
[80] Republic Act No. 10364, *Expanded Anti-Trafficking in Persons Act of 2012*, Sec. 3(a).
[81] Ibid., Sec. 3(j)
[82] Ibid., Sec. 9
[83] G.R. No. 260823, 26 June 2023

under Section 4(a), in relation to Section 6(a), of Republic Act 9208 (Anti-Trafficking in Persons Act of 2003), as amended by Republic Act 10364.[84]

Recognizing that human trafficking is often a transnational issue, the Anti-Trafficking in Persons Act also encourages international cooperation to effectively combat trafficking networks. This collaborative approach is crucial for sharing intelligence and resources with other countries, thereby strengthening global efforts against the online exploitation of children.[85]

The Anti-Child Pornography Act complements the Anti-Trafficking in Persons Act by addressing the specific manifestations of exploitation that can occur through digital channels. Both laws underscore the State's responsibility to safeguard children from all forms of sexual exploitation. This includes online sexual exploitation, where children are vulnerable to being recruited or coerced through social media and other digital platforms.

The Anti-Trafficking in Persons Act provides a clear legal basis for intervention upon identifying signs of trafficking or exploitation, while R.A. 9775 outlines the mechanisms for investigating and prosecuting individuals involved in child pornography. Both laws include penalties for traffickers, serving as a deterrent to potential offenders.

This emphasis on accountability is essential for protecting children, sending a strong message that trafficking and exploitation will not be tolerated.[86] Ultimately, R.A. 9208 and R.A. 9775 work in tandem to create a comprehensive legal framework that addresses the complexities of child exploitation and trafficking in the Philippines.

RA No. 11930 - Anti-Online Sexual Abuse of Exploitation of Children and Anti-Child Sexual Abuse or Exploitation Materials Act

Republic Act 11930, also known as the Anti-Online Sexual Abuse and Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act, represents a pivotal step in the Philippines's effort to address the alarming rise of online exploitation. Enacted on July 30, 2022, this legislation comes in response to stark findings, including statistics from the International Justice Mission, which reveal that 83% of child sex traffickers in the Philippines are family members of the abused children.[87] With a median age of 11 years, victims endure an average of two years of abuse, with the youngest victims being as young as three years old. In 2022 alone, it was estimated that

[84] The case stemmed from the accused's operation as floor managers of a Cavite bar where they recruited and exploited minors and young women for prostitution. Undercover police officers, acting on a tip, confirmed the illegal activity on October 10, 2014, when Gumba and Rellama offered sexual services with girls, including 15-year-olds AAA and BBB, and 18-year-olds PPP and GGG, for PhP1,500 per person. A subsequent entrapment and rescue operation on October 22, 2014, led to their arrest. The Supreme Court ruled that the prosecution successfully established the accused's guilt in trafficking children for prostitution, as defined under the relevant provisions of RA 9208, as amended.

[85] McQuiggan, S., Kosturko, L., McQuiggan, J., & Sabourin, J. (2015). *A handbook for developers, educators, and learners.* Page 321.

[86] *Ibid*. Page 305

[87] IJM (2020) Online Sexual Exploitation of Children, Available at: https://www.ijm.org/our-work/trafficking-slavery/online-sexual-exploitation-children (Accessed on 25 February 2025)

one out of every 100 Filipino children was a victim of Online Sexual Exploitation of Children (OSEC).[88] To confront these realities, Republic Act 11930 mandates that local governments implement community-based initiatives and pass ordinances[89] that reflect their unique cultural and social contexts. This localized approach is designed to prevent and respond to OSAEC and CSAEM at the barangay level, ensuring community engagement and support.

Educational programs focused on family awareness and preventive strategies form a critical part of these efforts, equipping communities to recognize, respond to, and mitigate the risks associated with child exploitation. Furthermore, the law emphasizes a holistic approach to rehabilitation and reintegration, managed by local social welfare offices, to aid victims' recovery and safeguard their well-being. Through supportive measures like counseling, legal aid, and safe housing, this framework helps build a resilient pathway for survivors while reducing the risk of re-trafficking.

In addition, the law introduces crucial provisions to protect individuals and entities who take action against OSAEC and CSAEM. The "Good Samaritan" provision ensures that those who report cases, block internet addresses, remove websites, or take down harmful content are not held liable, provided their actions are done in good faith, necessary to prevent harm, and reported within 24 hours. This provision encourages proactive involvement in combating online child exploitation.

> "Section 7. Protection of a Good Samaritan. — Any person who has the responsibility of reporting cases under this Act, blocking an internet address, removing a website or domain, taking down of shared videos, pictures, or messages for the services provided by an internet intermediary, and providing information for the purpose of an investigation or prosecution of a case involving acts of OSAEC shall not be held civilly, criminally or administratively liable: Provided, That the action was:
>
> (1) done in good faith;
>
> (2) necessary to prevent access or dissemination of CSAEMs; and
>
> (3) reported within twenty-four (24) hours from the act of blocking an internet address, removing a website or domain, or taking down of shared video, picture or messages.

Moreover, the law introduced an age verification protocols[90], requiring all online providers of adult content shall be required to adopt an anonymous age verification process before granting access to adult content. This requirement aims to ensure that only individuals of legal age can view explicit content,

---

[88] *Ibid.*
[89] Republic Act No. 11930, *Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act*, Sec. 33.
[90] Ibid., Sec. 35

thereby reducing the risk of minors being exposed to harmful or inappropriate material.

> "Sec. 35 Age Verification Protocols. — All online providers of adult content shall be required to adopt an anonymous age verification process before granting access to adult content. Not later than one (1) year after the passage of this Act, the NTC shall complete a policy study into age-verification controls and protocols by internet intermediaries that may be put in place in order to restrict the access of children to materials within the purview of Section 3 (c) (iv) of Presidential Decree No. 1986, with the end in view of promulgating rules and regulations to this effect.
>
> Said rules and regulations governing the adoption of an anonymous age verification process shall be promulgated not later than eighteen (18) months after the passage of this Act. Nothing in this provision shall be construed as an exemption to the provisions of the "Data Privacy Act of 2012."[91]

The provision mandating age verification for online adult content providers in the Philippines marks a crucial advancement in strengthening child protection in the digital landscape. This requirement is designed to restrict access to explicit material solely to individuals of legal age, thereby diminishing the risk of minors encountering inappropriate or harmful content.

At the same time, the implementation of this measure must align with the principles of the Data Privacy Act of 2012, ensuring that while online safety is reinforced, users' rights to privacy and data security are also upheld. A key aspect of this provision is the emphasis on a secure yet anonymous verification process. While the goal is to effectively confirm a user's age, it is equally important to safeguard personal information, preventing potential data breaches or misuse of sensitive data.

Striking a balance between child protection and privacy rights is essential, as overly intrusive verification mechanisms can lead to concerns about data security and user trust. By implementing responsible and ethical data-handling practices, this provision aims to ensure that digital safety measures do not come at the expense of individual privacy.

By mandating age verification, the law shifts the burden of responsibility from individuals and families to the adult content providers themselves. Rather than expecting parents or guardians to monitor and restrict access to explicit material, platforms that host and distribute such content are now held accountable for ensuring that their services comply with child protection standards. This proactive approach strengthens regulatory oversight and places clear legal obligations on digital service providers, reinforcing their role in maintaining a safer online environment for minors.

---

[91] The National Telecommunications Commission is mandated to complete a policy study into age-verification controls. This is in order to come up with rules and regulations to restrict access of children to content within the purview of the Movie and Television Review and Classification Board.

Moreover, this initiative aligns the Philippines with international best practices in digital child protection. Many countries have implemented similar regulations to address the growing concern of children's exposure to inappropriate online content. By adopting these global standards, the Philippines demonstrates its commitment to safeguarding minors from digital exploitation while also fostering a more responsible and ethical online ecosystem.

While this provision is a critical step forward, its effectiveness will largely depend on proper enforcement, technological adaptability, and continuous evaluation. Policymakers, regulatory agencies, and digital platforms must collaborate to refine verification systems, address potential loopholes, and enhance public awareness.

Additionally, integrating digital literacy programs can further empower parents and children to navigate online spaces safely. In an era where digital access is increasingly widespread, such measures are indispensable in ensuring a secure, ethical, and child-friendly online environment.

R.A. 7610 – Special Protection of Children Against Abuse, Exploitation, and Discrimination Act

Enacted to provide special protections against abuse, neglect, cruelty, exploitation, and discrimination, this law acknowledges the heightened vulnerability of children to numerous threats, particularly in the context of digital platforms. Though the Act was promulgated before the widespread use of social media, its comprehensive provisions can be effectively adapted to address contemporary challenges posed by online interactions. As children increasingly engage on platforms like Facebook, Instagram, and gaming networks, the risk of online predators who may groom or exploit minors has significantly intensified.

R.A. 7610's broad definition of abuse and exploitation[92] encompasses a wide range of harmful actions, importantly including any behaviors that endanger children, whether in physical or digital spaces. This expansive interpretation ensures that attempts to lure or groom children online, such as inappropriate messages, solicitations, or the sharing of exploitative content, fall within the jurisdiction of this Act.

By classifying these behaviors as forms of exploitation, R.A. 7610 creates a robust legal framework that empowers authorities to act against offenders targeting children in the digital realm. Furthermore, the Act emphasizes the need for preventive measures, encouraging the development of programs aimed at raising awareness about the risks children face online and the importance of

[92] Section 3. Definition of Terms (b)"Child abuse" refers to the maltreatment, whether habitual or not, of the child which includes any of the following:
(1) Psychological and physical abuse, neglect, cruelty, sexual abuse and emotional maltreatment;
(2) Any act by deeds or words which debases, degrades or demeans the intrinsic worth and dignity of a child as a human being;
(3) Unreasonable deprivation of his basic needs for survival, such as food and shelter; or
(4) Failure to immediately give medical treatment to an injured child resulting in serious impairment of his growth and development or in his permanent incapacity or death.

reporting suspicious activities. Community initiatives can foster safe online experiences while equipping children with the knowledge to navigate social media responsibly. In terms of enforcement, the provisions of R.A. 7610 provide a solid legal foundation for law enforcement agencies to take action against individuals or entities that exploit children online. This includes pursuing legal action against online predators and holding accountable those who create, distribute, or facilitate access to harmful content involving minors. The law's dual focus on protection and accountability enhances child protection efforts in the Philippines, creating a multifaceted strategy against exploitation. Moreover, R.A. 7610 aligns with the provisions of R.A. 9775, the Anti-Child Pornography Act of 2009, and R.A. 9208, the Anti-Trafficking in Persons Act of 2003.

RA No. 10173 - Data Privacy Act of 2012

Echoing the mandate in Article 12 of the Universal Declaration of Human Rights (UDHR), the UN Convention on the Rights of the Child recognizes the right of the child to privacy. Children, in their quest for social acceptance, may be persuaded to share personal information or engage in inappropriate interactions, unaware of the consequences. This is especially concerning in environments where privacy settings are not well understood or used effectively.

The Data Privacy Act ("DPA") or Republic Act 10173 is the primary privacy law in the Philippines. It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring the free flow of information to promote innovation and growth.[93] Under this law, the processing of personal information shall be generally allowed, subject to compliance with requirements of the DPA and other laws allowing disclosure of information to the public.[94] It also protects the privacy of individuals, especially minors, by regulating the collection, processing, and storage of personal data. For children, this is particularly significant given their growing presence on social media platforms where vast amounts of personal data are collected, including information related to their identities, activities, and interactions. The Act mandates that the collection of personal information must be lawful and fair. Specifically, the law provides:

> "SEC. 11. General Data Privacy Principles. – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of **transparency, legitimate purpose and proportionality**.
>
> Personal information must, be:

[93] Republic Act No. 10173, Sec. 2.
[94] *The Sufficiency of our Data Privacy Laws to Protect Children's Personal Data in the Midst of Online Learning*. Dalaguete (2021) page 123

(a) Collected for **specified and legitimate purposes** determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

(b) Processed **fairly and lawfully**;

(c) Accurate, **relevant and, where necessary for purposes** for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;

(d) **Adequate and not excessive** in relation to the purposes for which they are collected and processed;

(e) **Retained only for as long as necessary** for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and

(f) **Kept in a form which permits identification** of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, That adequate safeguards are guaranteed by said laws authorizing their processing.

The personal information controller must ensure implementation of personal information processing principles set out herein."[95] (Emphasis Supplied)

Organizations, including social media platforms, must have legitimate reasons for collecting data and must be transparent about their data practices. This means that when children interact with online platforms, the entities collecting their data must clearly explain how this information will be used, ensuring that families are aware of any potential risks involved.

In the Philippines, the Data Privacy Council Education Sector of the National Privacy Commission issued Advisory No. 2020-01[96] to guide schools and other educational institutions, as well as other stakeholders in the education sector, in their efforts to ensure adequate data protection in the conduct of online learning and other related activities. However, the advisory is only meant to be a set of recommendations and shall not be treated as a policy.[97] Still, a critical aspect of the Data Privacy Act is the requirement for consent when processing personal data, to wit:

---

[95] Ibid., Chapter III, Sec. 11
[96] NPC Advisory No. 2020-01, issued by the Data Privacy Council Education Sector
[97] *The Sufficiency of our Data Privacy Laws to Protect Children's Personal Data in the Midst of Online Learning*. Dalaguete (2021) page 126

"SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

(a) **The data subject has given his or her consent**;

x x x ." (Emphasis Supplied)

For minors, it is acknowledged that consent must typically be obtained from a parent or guardian before any of their personal data can be collected or processed or to create an age-appropriate privacy notice.[98] This requirement adds a vital layer of protection for children, as it ensures that their guardians are involved in decisions regarding their personal information, thus helping prevent unauthorized data usage or potential exploitation.[99] This involvement is crucial in an era where children may not fully understand the implications of sharing personal information online.

The Data Privacy Act holds organizations accountable for the data they collect and process. Under this law, personal information controller is responsible for personal information under its control or custody, including information.

"SEC. 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.

(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.[100]

Entities that fail to comply with the law's provisions may face legal consequences, including fines and penalties.[101] The law requires data handlers to implement appropriate security measures[102] to protect personal information from

[98] NPC Advisory No. 2024 – 03, Child-Oriented Transparency. December 17, 2024
[99] Ibid.
[100] Ibid., Chapter VI, Sec. 21
[101] Ibid., Chapter VIII, Sec. 25
[102] SEC. 20. *Security of Personal Information.* – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

unauthorized access, disclosure, alteration, or destruction. This includes using encryption, access controls, and incorporate Child Privacy Impact Assessment (CPIA). This assessment part of the NPC Advisory No. 2024 – 03, Child-Oriented Transparency. December 17, 2024, to wit:

> "SECTION 2. Risk-Based Assessment.- The processing of children's personal data must adhere to the general privacy principles. PICs shall ensure that, in accordance with the Principle of Transparency, children are aware of the nature, purpose, and extent of the processing of personal data. Consistent with the purpose of a Privacy Impact Assessment (PIA), PICs shall adopt a risk-based and child-oriented approach when informing children whose data they are processing, taking into account their age and the risks involved in the specific processing activity."
>
> A. Privacy Impact Assessment (PIA). PICs must incorporate Child Privacy Impact Assessments (CPIA) as part of their PIAs before launching products or services intended or likely to be accessed by children and thereafter as may be necessary. The PIA is a continuing requirement, regularly reviewed and updated to account for changes in products, services, processes, or regulations. The factors that must be considered include, but are not limited to:
>
> 1. Purpose of processing;
> 2. Types of data to be processed (e.g., collected, used, or disclosed);
> 3. Sources of data;
> 4. Systems to be used (e.g., open or closed systems);

The emphasis on CPIAs and data security measures reflects a growing recognition of the importance of protecting children's privacy online. As children increasingly engage with digital technologies, it is crucial to ensure that their personal information is handled responsibly and ethically. By incorporating CPIAs into their PIAs, organizations can proactively identify and mitigate potential privacy risks, safeguarding children's well-being in the digital age.

This passage highlights the growing importance of protecting children's privacy online. It emphasizes that laws and regulations are evolving to empower parents and legal guardians to safeguard their children from data misuse, such as

---

(b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.
(c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:
(1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
(2) A security policy with respect to the processing of personal information;
(3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and
(4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

identity theft and online exploitation. This reflects a broader societal recognition of the need for proactive measures to ensure that children's personal information is handled responsibly and ethically by organizations and online platforms.

RA No. 10175 – Cybercrime Prevention Act of 2012

The Cybercrime Prevention Act of 2012 serves as a critical legislative framework in the Philippines for addressing the myriad of crimes occurring in cyberspace. Recognizing the rapid advancement of technology and the increasing prevalence of the internet in everyday life, particularly among young users, the law aims to combat various online offenses that pose significant risks to individuals. The Act addresses a wide range of cybercrimes, including offenses against the confidentiality, integrity, and availability of computer data and systems. These offenses include Illegal Access, Illegal Interception, Data Interference, System Interference, Misuse of Devices, and Cyber-squatting. In addition to these offenses, the Act also addresses computer-related offenses such as forgery, fraud, and identity theft, as well as content-related offenses.[103] The Act strengthens the protection of children online by increasing the penalties for offenses under the Anti-Child Pornography Act when committed through a computer system. It also criminalizes acts like cyberbullying and child pornography, which are significant risks for minors using social media.

Cyberbullying has emerged as a critical concern, particularly as more children engage with social media. The law criminalizes acts of cyberbullying, which can include harassment, threats, and the dissemination of harmful content targeted at individuals. By recognizing cyberbullying as a prosecutable offense, the law aims to create a safer online environment for minors, encouraging them to report incidents without fear of retaliation. Schools and parents can also utilize this framework to address bullying issues more robustly.

The Act also emphasizes the importance of educational campaigns aimed at raising awareness among parents, children, and educators about the risks associated with online activities and the importance of reporting suspicious or harmful behaviors. Furthermore, the Cybercrime Prevention Act recognizes the importance of international cooperation in combating cybercrime, particularly concerning offenses related to computer systems and data.

> "Section 22. General Principles Relating to International Cooperation. — All relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or

[103] Content-related Offenses: (1) Cybersex. — The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.
(2) Child Pornography. — The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: Provided, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.
(3) Unsolicited Commercial Communications. — The transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless:
(4) Libel. — The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

> reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal, offense shall be given full force and effect.[104]

Section 22 of the Act states that all relevant international instruments, arrangements, and domestic laws concerning international cooperation in criminal matters shall be given full force and effect for investigations, proceedings, and evidence collection related to cybercrime. This provision facilitates collaboration with other countries in the fight against online offenses, including those that exploit and endanger children.

By strengthening penalties, criminalizing harmful online behaviors, promoting education, and fostering international cooperation, the Cybercrime Prevention Act provides a comprehensive framework for protecting children in the digital age. It recognizes the evolving nature of online threats and seeks to create a safer online environment for all users, especially the most vulnerable.

R.A. 11313 – Safe Spaces Act (Bawal Bastos Law)

Also as the "Bawal Bastos" Law, the Safe Spaces Act is a significant piece of legislation in the Philippines aimed at fostering safe environments for all individuals, particularly women and children, by addressing and prohibiting various forms of gender-based harassment in streets, public spaces, online, workplaces, and educational or training institutions.[105] Enacted in 2019, the law reflects the growing recognition of the importance of ensuring that both physical and online spaces are free from harassment and discrimination such as catcalling, gender-based online sexual harassment[106] and stalking, thus acknowledging the diverse contexts in which individuals may encounter harassment. The Safe Spaces Act provides a broad definition of gender-based harassment, which includes any act or series of acts that degrade or demean an individual's dignity, particularly based on the person's gender. This encompasses a wide range of behaviors, from verbal harassment to physical aggression, specifically:

> "*Section 12. Gender-Based Online Sexual Harassment.* - Gender-based online sexual harassment includes acts that use information and communications technology in terrorizing and intimidating victims through physical, psychological, and emotional threats, unwanted sexual misogynistic, transphobic, homophobic and sexist remarks and comments online whether publicly or through direct and private messages, invasion of victim's privacy through cyberstalking and incessant messaging, uploading and sharing without the consent of the victim, any form of media that contains photos, voice, or video with sexual content, any unauthorized recording and sharing of any of the victim's photos, videos, or any information online,

[104] Ibid., Chapter VI, Sec. 22
[105] Republic Act No. 11313, *Safe Spaces Act*, *April 17, 2019*, Sec. 2.
[106] Ibid

impersonating identities of victims online or posting lies about victims to harm their reputation, or filing, false abuse reports to online platforms to silence victims.[107]

The Act requires government agencies and institutions, including educational and workplace settings, to establish policies and protocols for addressing online sexual harassment.[108] This includes creating reporting mechanisms, conducting training for staff and students, and implementing preventive measures to foster safe environments. Likewise, the law-imposed liability to educational or training institutions, individuals who hold authority, influence, or moral ascendancy—such as principals, school heads, teachers, instructors, professors, coaches, or trainers—can be held accountable not only for directly committing acts of gender-based sexual harassment but also for their failures in other areas.[109]

Specifically, they may face liability for not fulfilling their responsibilities as and/or can be held responsible for failing to take appropriate action when incidents of gender-based sexual harassment are reported within their institution.[110] Ongoing efforts to implement the law effectively, raise public awareness, and cultivate a culture of respect will be essential for realizing its goals and ensuring that all individuals including children can navigate both physical and online spaces free from harassment and abuse.

R.A. 10929 – Free Internet Access in Public Places Act

As digital literacy becomes increasingly vital in today's technology-driven world, educational institutions can leverage this access to implement programs focused on online safety to teach children how to navigate the internet responsibly and identify potential threats. The Free Internet Access in Public Places Act mandates the provision of free internet access in public areas such as schools, libraries, and community spaces, significantly enhancing digital connectivity and accessibility. While its primary aim is to improve access to online resources, it also serves as an essential platform for promoting children's education and protection in digital environments. However, Senator Sherwin Gatchalian's call for a review of the Free Internet Access in Public Places Act highlights a critical issue in the Philippines. He said in an interview, "*Our learners are the ones who will greatly benefit from this because it will improve the flow of information, especially for our poorest constituents.*"[111]

While the Act aims to provide free internet access in public spaces, including schools, the reality is that a very small percentage of public schools actually have this access. This lack of connectivity disproportionately affects students from disadvantaged backgrounds, limiting their ability to fully participate in the digital age, especially in the context of distance learning and online education. The Senator's concerns are further validated by data showing a

[107] Ibid., Sec. 12.
[108] Ibid., Sec. 13.
[109] Ibid., Art. V. Sec. 22
[110] Ibid., Art. V. Sec. 23
[111] *Senator seeks review of slow implementation of free public Wi-Fi*. PNA (2022) https://www.pna.gov.ph/articles/1189028 accessed on 24 February 2025.

declining trend in the number of public schools with free internet access. This suggests that the Act's implementation has been ineffective in addressing the digital divide, and may even be exacerbating it.[112] The COVID-19 pandemic further exposed this issue, as the shift to online learning highlighted the critical importance of reliable internet access for educational continuity and equity.

Despite the challenges that come with increased internet accessibility, the Free Internet Access in Public Places Act significantly enhances opportunities for children to engage in educational and skill-building activities. By providing free internet access in schools, libraries, and other educational institutions, the law fosters an environment where children can explore digital resources that enhance their knowledge and skills. This accessibility lays the foundation for responsible online behavior, encouraging children to use technology for learning and personal development.

Beyond connectivity, the law plays a crucial role in bridging the digital divide, particularly for children from underserved communities. Ensuring equal access to educational materials and information enables children from diverse socioeconomic backgrounds to engage with digital tools that might otherwise be unavailable to them. This provision expands their learning opportunities, allowing them to participate in online education, conduct research, and develop essential digital skills that are increasingly relevant in today's world. Moreover, the law introduces a structured framework for promoting digital literacy and responsible internet use among children.[113] Schools and libraries can leverage this initiative to organize workshops and interactive sessions aimed at educating students about online safety.[114] These sessions can cover critical topics such as recognizing and responding to cyberbullying, understanding privacy settings, identifying misinformation, and safeguarding personal data. By fostering open discussions in safe educational settings, the law encourages children to seek guidance when facing online challenges, ensuring that they are equipped with the knowledge to navigate the digital landscape securely and confidently. This initiative aligns with Article 17 of the United Nations Convention on the Rights of the Child, which underscores a child's right to access information that contributes to their well-being and development. Recognizing the significant role of media in shaping a child's growth, Article 17 places an obligation on states to ensure that children have access to diverse national and international sources of information while being protected from harmful content. The Free Internet Access in Public Places Act reflects this principle by not only promoting accessibility but also incorporating measures that safeguard children's digital experiences.

In summary, the Free Internet Access in Public Places Act serves as more than just a means of providing connectivity—it is a transformative tool that empowers children, particularly those from disadvantaged backgrounds, by enhancing their digital literacy and ensuring safe online engagement. By equipping them with the necessary skills and knowledge to navigate the digital

[112] Ibid.
[113] Republic Act No. 10929, Section 2
[114] Ibid., Section 6.

world responsibly, the law upholds their rights to privacy, information, and expression, fostering an inclusive and informed digital generation.

Senate Bill No. 552

In July 2019, Senator Emmanuel P. Pacquiao filed a Senate Bill No. 552 or the Child Internet Safety and Protection Act of 2019. The Bill seeks to establish a comprehensive framework for ensuring the safety of children online by limiting their exposure to harmful online content.[115] This bill aligns with Article II, Section 13 of the 1987 Philippine Constitution, which recognizes the vital role of the youth in nation-building and mandates the State to promote and protect their physical, moral, spiritual, intellectual, and social well-being. It is designed to protect minors from digital materials that could negatively impact their physical, moral, spiritual, psychological developments, and social well-being.[116]

One of the key provisions of the bill is the requirement for commercial establishments, public internet access points, and educational institutions—both public and private—that provide internet services to implement a filtered "*clean feed internet service.*" This service must utilize end-user or PC-based filtering software, ensuring that online content accessible to users under the age of eighteen (18) is free from harmful or inappropriate material.[117] Such a measure is intended to prevent minors from encountering content that may be unsuitable for their age and developmental stage. Additionally, the bill outlines specific responsibilities for Internet Service Providers (ISPs) under this Act to take reasonable steps to ensure that internet access accounts are not provided to children under 18 years old without parental consent.

Lastly, ISP must provide users with access to one or more approved internet filter software products or services. This can be done by offering an internet link for users to download and install the software, providing a Compact Disc for software installation, or offering a 'server-based' filter software service that filters internet content before it reaches the user's computer. Importantly, any internet filtering software used in commercial establishments or public internet access points must be duly approved and prescribed by the Child Internet Safety Commission (CISC).[118]

The proposed bill will emphasize the role of the State in promoting internet safety, requiring it to actively inform and educate parents or guardians about the availability and benefits of internet filters. By raising awareness and ensuring accessibility of these filtering options, the law aims to empower parents and guardians to take control over the digital environments their children interact with. The introduction of Senate Bill 552, the Child Internet Safety and Protection Act of 2019, represents a proactive effort to fill an important gap. The Philippines has made significant strides in enacting laws and proposing bills aimed at safeguarding minors from the numerous online risks, demonstrating a commitment to uphold the principles outlined in international conventions like

[115] Senate Bill No. 552, *Child Internet Safety and Protection Act of 2019.*
[116] Ibid., Sec. 4.
[117] Ibid., Sec. 5
[118] Ibid., Sec. 6

the UNCRC. However, as technology continues to evolve and social media increasingly influences children's lives, it is essential to conduct ongoing assessments and review of these legal frameworks. Without such tailored protections, Filipinos risk compromising the safety and well-being of future generations as they navigate an ever-evolving digital landscape.

VI. U.S. LAWS

The choice to compare U.S. legislation, specifically the Kids Online Safety Act (KOSA), with Philippine laws on protecting children's online activities is strategic and multifaceted. The U.S. has a relatively mature and detailed approach to digital regulation, with multiple laws specifically designed to protect children in online environments. The Kids Online Safety Act (KOSA) builds on existing regulations, like the Children's Online Privacy Protection Act (COPPA), to address the evolving challenges children face online. This depth of legal precedent provides a well-rounded model to examine how specific, child-focused regulations can be structured and enforced. By choosing the U.S. as a point of comparison, the author is examining a legal system that has continuously evolved to address children's online safety, thus providing a practical framework that the Philippines could look to adapt.

The U.S. has been a pioneer in developing regulations that respond to emerging digital trends, including social media, online gaming, and algorithm-driven content delivery. The U.S. legal system has experience in defining the responsibilities of online platforms in maintaining child safety, and these regulations are increasingly relevant as Philippine children interact more frequently with global social media platforms.

Since the U.S.-based platforms dominate the social media landscape (e.g., Facebook, Instagram, YouTube), their compliance with U.S. laws impacts users worldwide, making the U.S. legal framework particularly pertinent for comparison. The U.S. regulatory framework often influences global standards, and many countries look to the U.S. for guidance on emerging regulatory issues.

Studying U.S. laws and policies gives the Philippines a practical reference for internationally recognized child safety standards. The U.S. approach provides not only a legal precedent but also a model that social media platforms are more likely to comply with internationally, which can aid the Philippines in aligning its laws with global standards. The U.S. and the Philippines have distinct legal, cultural, and social frameworks, and these differences can provide valuable insights into the adaptability of child protection laws. The U.S. legal framework can serve as an aspirational benchmark, highlighting areas where Philippine laws could be strengthened or adapted to fit the unique cultural and digital landscape of the Philippines. The contrast in regulatory approaches may also reveal areas for legal innovation that consider both local and global challenges faced by Filipino children online.

Child Online Protection Act

In the United States, the Child Online Protection Act (COPA) was enacted in 1998 with the primary objective of restricting minors' access to online content deemed harmful to them. COPA specifically targeted commercial websites that provided materials considered "harmful to minor," requiring them to implement age verification systems or other restrictive measures to prevent underage users from viewing such content. The law was designed to address growing concerns about the increasing availability of explicit and inappropriate material on the internet and its potential negative effects on children. COPA mandated that all commercial distributors of material deemed "harmful to minors" implement measures to restrict access by underage users.

Under COPA, "material harmful to minors" was defined based on "contemporary community standards" as content that appeals to the "prurient interest" and includes depictions of sexual acts or nudity, including female breasts. This definition establishes a broader standard than obscenity, as it encompasses content that may not meet the strict legal threshold for obscenity but is still considered inappropriate for minors.

However, COPA faced significant legal challenges on constitutional grounds[119], particularly concerning the First Amendment's protection of free speech.[120] Critics argued that the law's broad definition of "harmful to minors" and its requirement for content-based restrictions placed an undue burden on lawful online speech.

In a series of court rulings, including decisions by the U.S. Supreme Court, COPA was deemed unconstitutional for imposing overly restrictive measures that violated the free expression rights of both website operators and adult users. The law was found to be facially in violation of the First and Fifth Amendments[121] to the U.S. Constitution. Additionally, the courts concluded that less restrictive alternatives, such as parental control tools and internet filtering software, provided more effective and constitutionally sound methods for protecting children online. Due to these constitutional concerns, COPA was never fully enforced and was ultimately struck down. The legal battles surrounding the law underscored the ongoing tension between protecting children from harmful online content and upholding fundamental free speech rights in the digital age.

Despite its invalidation, COPA paved the way for further legislative efforts aimed at enhancing online child protection, including the development of laws such as the Children's Online Privacy Protection Act (COPPA) and more recent proposals like the Kids Online Safety Act (KOSA).

---

[119] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997)

[120] US Constitution. First Amendment., *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of* grievances.

[121] US Constitution. Fifth Amendment, *No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.*

Children's Internet Protection Act (CIPA)

The CIPA was enacted by the U.S. Congress in 2000 as a legislative response to growing concerns about children's exposure to harmful and obscene content online. Recognizing the critical role of educational institutions and public libraries in providing internet access to minors, CIPA established specific regulations to ensure that schools and libraries receiving government-subsidized internet services implement protective measures to safeguard young users.[122]

CIPA applies to schools and libraries that seek discounts on internet access or internal connections through the E-rate program, a federal initiative designed to make communication services and technology more affordable for qualifying institutions. To be eligible for these discounts, institutions must certify compliance with CIPA by adopting and enforcing an internet safety policy that includes technology protection measures. These measures must restrict access to online content that falls under three specific categories: Obscene material,[123] Child pornography[124], and Content harmful to minors[125] when accessed on computers used by children. Before implementing these safety measures, CIPA requires that schools and libraries provide sufficient public notice and hold at least one public meeting to allow community members to discuss the proposed policies.[126] This ensures transparency and gives stakeholders, such as parents and educators, an opportunity to provide input on internet safety strategies.

While CIPA mandates that all internet access, including that of adults, must be filtered, the filtering requirements can be less restrictive for adult users. However, the law includes an exception for bona fide research, allowing institutions to disable filters for adults engaged in legitimate research or other lawful purposes. Notably, CIPA does not define "bona fide research," leaving its interpretation open. In a later ruling, the U.S. Supreme Court clarified this issue, determining that libraries must adopt an internet use policy allowing adult users to request the unblocking of filtered content without being required to justify their reasons. Writing for the Court, Chief Justice William Rehnquist stated:

> *"Assuming that such erroneous blocking presents constitutional difficulties, any such concerns are dispelled by the ease with which patrons may have the filtering software disabled. When a patron encounters a blocked site, he need only ask a librarian to unblock it or (at least in the case of adults) disable the filter."*

---

[122] Federal Communications Commission. (2024). Children's Internet Protection Act (CIPA). Federal Communications Commission. Available at: https://www.fcc.gov/consumers/guides/childrens-internet-protection-act (Accessed on January 12, 2025)

[123] *Miller v. California*, 413 U.S. 15 (1973) clarifying the legal definition of obscenity as material that lacks "serious literary, artistic, political, or scientific value

[124] 18 U.S.C. 2256

[125] Secs. 1703(b)(2), 20 U.S.C. Definition of *"harmful to minors"* – refers to any picture, image, graphic image file, or other visual depiction that – (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

[126] Ibid.

This effectively placed the discretion of what qualifies as bona fide research in the hands of the adult requesting to disable the filter. Following the Court's decision, the Federal Communications Commission (FCC) instructed libraries complying with CIPA to establish a procedure for unblocking filtered content upon an adult's request.

Beyond content filtering, CIPA imposes additional obligations on schools. First, schools must actively monitor minors' online activities to ensure compliance with their internet safety policies. Second, as required by the Protecting Children in the 21st Century Act, schools must integrate digital literacy education into their curriculum.[127] This includes teaching students appropriate online behavior, safe interactions on social networking platforms and chatrooms, and strategies for recognizing and preventing cyberbullying. To enforce CIPA's provisions, the Federal Communications Commission issued regulations in 2001 detailing compliance requirements for schools and libraries. Over time, CIPA has evolved to address emerging online threats. In 2011, regulatory updates were introduced to enhance child safety online, focusing on cybersecurity awareness, safe digital interactions, and the responsible use of internet-connected technologies.[128]

While CIPA remains a critical framework for shielding minors from harmful online content, concerns persist regarding its effectiveness. Critics argue that content filtering measures can be overly restrictive, sometimes blocking access to legitimate educational resources and hindering academic research.[129] Additionally, CIPA primarily focuses on access control rather than fostering comprehensive digital literacy, raising concerns about whether children are adequately equipped to navigate online risks independently. Research suggests that while filtering software can limit exposure to explicit content, it does not replace the need for media literacy education that teaches children how to critically evaluate and engage with digital information.[130]

Overall, CIPA underscores the importance of internet safety in educational settings by mandating technological safeguards and digital awareness programs. However, as technology continues to evolve, ongoing policy adjustments and complementary educational initiatives are necessary to strengthen the protection of children in the ever-changing digital landscape.

Protecting Children in the 21st Century Act

The Protecting Children in the 21st Century Act of 2008 introduced critical amendments to the Communications Act of 1934, focusing on strengthening online safety education for minors. Recognizing the increasing risks associated with children's internet use, the Act mandates that schools and libraries receiving federal funding must incorporate digital safety instruction into their educational programs. This includes teaching minors about responsible online behavior,

---

[127] Ibid.
[128] Federal Communications Commission (FCC). (2011). *CIPA Regulatory Updates for Child Safety Online*.
[129] American Library Association. (2013). *Internet Filtering and Intellectual Freedom: A Critical Analysis of CIPA Implementation in Schools and Libraries*.
[130] Livingstone, S., & Helsper, E. J. (2007). *Gradations in digital inclusion: Children, young people and the digital divide*. New Media & Society, 9(4), 671-696.

cyberbullying prevention, and the safe use of social networking platforms. By requiring these institutions to integrate internet safety education, the Act aims to equip children with the knowledge and skills needed to navigate the digital world securely.

Beyond educational initiatives, the Act also reinforces the need for protective measures to regulate minors' access to harmful online content. Schools and libraries benefiting from federal support must ensure that their internet safety policies include content filtering mechanisms to block access to inappropriate or harmful material. This requirement aligns with broader efforts under the Children's Internet Protection Act (CIPA) to create safer digital environments for young users.

Another significant aspect of the Protecting Children in the 21st Century Act is the pivotal role it assigns to the Federal Trade Commission (FTC) in promoting online safety awareness. Recognizing the complexity of digital risks faced by children, the Act directs the FTC to collaborate with both public and private sector entities to develop and implement comprehensive internet safety campaigns. These efforts involve developing educational materials tailored for parents, educators, and children, launching national awareness programs to inform the public about online risks such as cyberbullying, inappropriate content, and data privacy concerns, and forging partnerships with technology companies, social media platforms, non-governmental organizations, and educational institutions to disseminate best practices and enhance protective measures for children in digital spaces.

By engaging multiple stakeholders, the Act mandates that the FTC submit an annual report to Congress detailing its progress in implementing online safety initiatives. This report provides an assessment of the effectiveness of existing educational programs and public awareness campaigns, an evaluation of emerging digital threats and evolving challenges in protecting minors online, and recommendations for policy adjustments and technological improvements to strengthen child safety protections.

The reporting requirement ensures a continuous cycle of evaluation and improvement, allowing policymakers to refine regulations based on real-time data and evolving digital risks. This iterative approach helps maintain the relevance and effectiveness of child protection strategies amid rapid technological advancements.

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA) is a U.S. federal law enacted in 1998 to safeguard the privacy of children[131] in online environments. Recognizing the increasing presence of young users on the internet, COPPA establishes strict requirements for website operators and online services that cater to children under 13.

[131] The term "child" means an individual under the age of 13. 15 USC 6501 (1)

Specifically, it mandates that these platforms obtain verifiable parental consent before collecting, using, or disclosing personal information from children. The law also imposes obligations on operators regarding data collection practices, transparency, and security, ensuring that children's sensitive information is not exploited or misused. COPPA applies to websites and online services operated for commercial purposes that are either directed toward children under 13 or have actual knowledge that children under 13 are providing personal information online. Most recognized non-profit organizations are exempt from COPPA's requirements. However, the Supreme Court has ruled that non-profits operated for the benefit of their members' commercial activities fall under the Federal Trade Commission's (FTC) jurisdiction and must comply with COPPA.[132]

A key component of COPPA is the requirement for "verifiable parental consent," which follows a "sliding scale" approach established by the FTC. This scale considers the method of data collection and the intended use of the information, requiring stronger verification measures when data is collected for more sensitive or commercial purposes. Despite these safeguards, enforcing meaningful parental involvement remains a challenge. The complexity of privacy policies and data practices often makes it difficult for parents to fully understand how their children's data is being collected and used, creating a communication gap between parents, companies, and developers that can undermine COPPA's effectiveness. Additionally, the rise of mobile apps, social media platforms, and interactive digital experiences has raised concerns about companies' compliance with COPPA, particularly when platforms do not explicitly target children but still collect their data. As a result, lawmakers have pushed for stronger protections, leading to the introduction of COPPA 2.0. COPPA 2.0 was introduced to expand the law's coverage by raising the protected age from under 13 to under 17. Introduced alongside the Kids Online Safety Act, COPPA 2.0 aimed to require minors aged 13 to 16 to provide their own consent for data processing, eliminating the need for parental approval in this age group.

On July 30, 2024, both COPPA 2.0 and KOSA passed the Senate with overwhelming bipartisan support.[133] However, neither bill passed the House before the expiration of the 118th U.S. Congress on January 3, 2025, leaving their future uncertain. With the increasing reliance on online learning platforms, concerns about student data privacy have grown, highlighting the need for stronger regulatory mechanisms to address evolving threats. Moreover, the digital landscape is evolving beyond traditional websites and social media platforms. These innovations create immersive online environments where data collection and behavioral tracking can occur in ways that are harder to regulate. Without proactive legislation like COPPA 2.0, companies may exploit these gaps, further complicating efforts to safeguard minors from intrusive data practices.

Overall, while COPPA remains a cornerstone of child online privacy protection, its effectiveness continues to be tested by rapid technological

[132] California Dental Association v. Federal Trade Commission, 526 U.S 756 (1999)

[133] U.S. Senate Approved Legislation to Protect Youth Online, https://www.mofo.com/resources/insights/240812-u-s-senate-approves-legislation-to-protect-youth-online accessed on 25 February 2025

advancements, enforcement challenges, and the need for greater parental awareness. The push for COPPA 2.0 reflects ongoing efforts to modernize child privacy protections, ensuring that regulatory frameworks keep pace with the evolving digital landscape.

Kids Online Safety Act

The rapid advancement of digital technology and the widespread accessibility of the internet have significantly reshaped childhood, bringing both opportunities and risks. While digital platforms offer invaluable tools for education, creativity, and social connection, they also expose children to potential threats such as cyberbullying, online predators, data privacy violations, and exposure to harmful content. As children increasingly engage with digital environments, existing child protection laws have struggled to keep pace with evolving online dangers, necessitating stronger, more adaptive regulatory frameworks.

Recognizing these challenges, the U.S. Kids Online Safety Act (KOSA)[134], introduced in 2022, represents a modern legislative response to safeguarding minors in the digital space. Unlike earlier regulations that primarily focused on data privacy, KOSA adopts a broader and more proactive approach, addressing risks such as inappropriate content, online grooming, mental health concerns, and social media-related harms. Children today spend unprecedented amounts of time online for both academic and recreational purposes. According to a Pew Research Center study, 95% of teenagers have access to smartphones, with 45% reporting that they are online "almost constantly".[135] This significant rise in screen time has intensified concerns regarding cyber risks, digital addiction, and exposure to harmful content, prompting the need for stronger legislative intervention. Although the Children's Online Privacy Protection Act (COPPA) of 1998 laid the groundwork for safeguarding minors' personal data, KOSA expands its scope beyond privacy protection, acknowledging that modern digital threats extend beyond data collection.

The KOSA seeks to enforce greater accountability for online platforms while promoting transparency, digital literacy, and mental health research to better understand the effects of digital exposure on children. The legislation aims to establish a more comprehensive safety framework, ensuring that platforms prioritize the well-being of young users by enforcing stricter content moderation, age-appropriate design features, and mechanisms to mitigate risks associated with digital exposure.

KOSA's primary objectives include enforcing greater accountability among online platforms, ensuring that they implement effective safety measures to mitigate children's exposure to harmful content, such as self-harm encouragement, sexual exploitation, and addiction-driven algorithms. The Act also enhances parental control mechanisms by requiring platforms to provide

[134] S. 1409, *Kids Online Safety Act*, 118th Cong. (2023-2024).
[135] Anderson, M., & Jiang, J. (2018). *Teens, Social Media & Technology 2018*. Pew Research Center. Available at: https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/ Accessed on March 25, 2025.

tools that enable parents and guardians to monitor and manage children's online activities.

Additionally, KOSA introduces more stringent content moderation and transparency requirements, obligating platforms to disclose their content regulation policies and take active measures to protect minors from algorithm-driven exposure to inappropriate material. Recognizing the significant impact of digital experiences on children's well-being, KOSA promotes research into the mental health effects of social media, allowing policymakers and educators to develop more effective intervention strategies. Furthermore, the legislation emphasizes the importance of digital literacy, urging schools and educators to incorporate online safety education into their curricula to equip children with the necessary skills to navigate digital spaces responsibly. The enactment of KOSA has far-reaching implications for various stakeholders. Parents and guardians benefit from improved oversight tools that enable them to take a more active role in their children's digital lives. Online platforms, conversely, face stricter obligations to prioritize safety features, adjust content algorithms, and enhance transparency regarding data collection and use.

For educators and schools, the Act highlights the importance of integrating digital literacy programs, helping students develop critical thinking skills and an awareness of online risks. Law enforcement agencies and policymakers also stand to gain from KOSA, as its provisions for research and data collection facilitate a more informed and targeted approach to combating online crimes against minors.

Despite its potential, KOSA faces several challenges in implementation. Ensuring compliance across a diverse range of online platforms presents a significant obstacle, as companies may struggle to adopt uniform standards for age verification, content moderation, and parental controls. Additionally, some critics argue that the legislation risks infringing on children’s rights to access information and express themselves online, highlighting the need for a careful balance between protection and digital freedom. Another concern involves the transparency of parental consent mechanisms and how platforms will handle, store, and use such data. The rapid evolution of technology also presents an ongoing challenge, as new threats continuously emerge, requiring KOSA to remain adaptable to address evolving digital risks effectively.

The Kids Online Safety Act represents a substantial legislative milestone in the effort to enhance online child protection. By establishing clear requirements for content moderation, parental involvement, research, and digital literacy, the Act aims to create a safer and more responsible online environment for minors. However, its success will depend on its adaptability, stakeholder collaboration, and the continuous evaluation of its effectiveness in addressing emerging challenges.

As the digital landscape evolves, future amendments and complementary policies will be necessary to strengthen KOSA’s impact and ensure that children can benefit from the internet’s opportunities while being safeguarded from its dangers. The introduction of KOSA underscores the growing global recognition

that child online safety must remain a legislative priority, requiring a collective effort from governments, technology companies, educators, and families to build a safer digital future for children.

Other Foreign Laws

The 21st century is distinctively marked as a period of rapid technological development. An estimated 5.3 billion people around the world use the internet in some form, making up 65% of the world population, and that number is projected only to rise. However, with the proliferation of technology also comes the introduction of new threats that have surfaced within our digital environment. Statistics show that 493.33 million cyber-attacks occurred on the internet last year alone with a hacking incident taking effect once every 39 seconds. These rising new threats combined with their tremendous digital consequences have ignited countries around the world to draft new legislation to protect their citizens from online threats. This article examines a number of countries around the world by continent and highlights laws that they have put in place to address these issues.

VII. INTERNATIONAL STANDARDS

The United Nations (UN) has taken many actions to protect people online. The UN is an international organization that was founded in 1945 for the purpose of maintaining international peace and security. Many of the UN's agencies have been tasked to combat various online threats. These efforts include the United Nations International Children's Emergency Fund's (UNICEF) efforts to fight cyberbullying, the United Nations Educational, Scientific, and Cultural Organization's (UNESCO) efforts to stop human trafficking, and the United Nations Office on Drug and Crime's (UNODC) efforts to increase internet security, among many more agencies' efforts and objectives.

The UN and UNICEF have both also laid out the foundation for children's rights through various policies and legislations, like the Convention on the Rights of the Child. Digital protection is included among these rights. The UN Committee on the Rights of the Child (UNCRC) has recommended that governments take swift action in the form of enacting policies to protect children from harm in the digital environment, stating that children "should also be protected from all forms of violence that happens in the digital environment."[136]

A. AUSTRALIA

Australia has taken a groundbreaking step in online child protection by enacting the world's most stringent social media laws, effectively prohibiting children under 16 from using platforms such as Snapchat, TikTok, Facebook, Instagram, and X.[137] This landmark legislation, or the Australia Online Safety Act, imposes severe penalties of up to 50 Million Australian Dollars (USD 32.5 million) on non-compliant tech companies. Prime Minister Anthony Albanese emphasized the importance of protecting young people from the harmful effects

[136] United Nations: Child and Youth Safety Online, 2023.
[137] BBC News. (2025, March 10). *Australia to ban social media for children under 16 in world-first move.* Available at: https://www.bbc.com/news/articles/c89vjj0lxx9o (Accessed on March 13, 2025)

of social media, a sentiment that resonates strongly with parent groups across the nation. However, the legislation has sparked intense debate, with critics raising concerns about enforcement mechanisms, privacy implications, and the potential impact on minors' social interactions.[138]

Business futurist Morris Misel provided a thought-provoking perspective, highlighting that while imposing such stringent restrictions is possible, the long-term feasibility and societal acceptance of these changes remain uncertain. Misel emphasized that humans are inherently drawn to observing others' lives—a phenomenon social media facilitates—making it unlikely for society to revert to a pre-social media era. He noted that even if society collectively decides to move away from existing platforms, social media would likely be replaced by alternative forms of digital interaction.[139] Misel further pointed out that the issue of social media access is highly specific to Western nations and countries with widespread internet penetration. While approximately 4.6 billion people globally engage with social media daily, a significant portion of the world's population remains disconnected, managing their lives without these digital platforms. This global disparity adds another layer of complexity to the conversation about regulating social media use.[140]

Australia's legislation sets the highest minimum age threshold for social media access globally, with no exceptions granted for existing users or parental consent. The task of determining which platforms fall under these regulations lies with the communications minister, guided by the expertise of the eSafety Commissioner. Notably, while social media platforms are the primary focus, the law exempts gaming and messaging services, as well as websites that can be accessed without an account, such as YouTube.[141]

To enforce these restrictions, the government plans to implement advanced age-verification technologies, placing the onus on platforms to integrate these measures. However, digital researchers have raised concerns about the reliability and security of such technologies, particularly those relying on biometrics or identity verification. Critics argue that these systems may be prone to flaws, raising serious questions about data privacy and efficacy. Furthermore, the ease with which tech-savvy users can circumvent these restrictions using virtual private networks (VPNs) remains a significant challenge.[142] While many Australian parents and caregivers support the legislation, believing it to be a necessary safeguard, experts caution that an outright ban may push children toward unregulated online spaces that pose even greater risks. Major tech companies, including Google, Snap, and Meta, have expressed opposition to the measure, questioning its practicality and effectiveness. TikTok warned of overly

---

[138] Taylor, J. (2024). *Australia's Online Safety Act: A Tough New Stance on Big Tech*. The Guardian. Available at: https://www.theguardian.com/technology/2024/jan/15/australia-online-safety-act-big-tech-penalties (Accessed on March 13, 2025)
[139] Meade, A. (2024). *Could We Ever Quit Social Media? Experts Weigh In on the Future of Digital Life*. The Guardian. Available at: https://www.theguardian.com/technology/2024/mar/10/quit-social-media-future-digital-life (Accessed on March 13, 2025)
[140] *Ibid.*
[141] *Ibid.*
[142] *Ibid.*

broad platform definitions, while X raised concerns about the law's compatibility with international human rights standards.[143]

Youth advocates, including members of the eSafety Youth Council, have criticized the exclusion of young voices from the policymaking process. They argue that effective solutions to online safety should involve the perspectives of those directly affected—young users themselves. Without incorporating these voices, they warn that the legislation risks overlooking critical nuances and unintended consequences[144] Despite the ongoing debate, the Australian government remains steadfast in its position, likening the ban to alcohol restrictions for minors—acknowledging that enforcement may not be flawless but asserting that public safety justifies the intervention. Australia's decisive action has attracted international attention, with Norway expressing interest in similar measures and the UK considering but not yet committing to comparable restrictions.[145]

Ultimately, Australia's bold initiative highlights the growing global consensus that regulatory intervention is necessary to ensure a safer online environment for younger users. Whether the legislation will achieve its intended goals or encounter insurmountable enforcement challenges remains to be seen. Nonetheless, its influence on the evolving international discourse surrounding social media governance is undeniable, serving as a catalyst for further exploration and innovation in the realm of digital child protection.

B. EUROPE

Europe is one of the frontrunners in protecting users online, largely due to the efforts of the European Union (EU). The EU's data protection laws have long been considered the global benchmark for privacy and security. Over the past 25 years, technological advancements have reshaped daily life in unprecedented ways, necessitating a comprehensive review of existing regulations.[146] In response to these evolving challenges, the EU introduced the General Data Protection Regulation (GDPR) in 2016, marking one of its most significant legislative milestones. The GDPR replaced the 1995 Data Protection Directive, which was established when the internet was still in its early stages, ensuring stronger and more adaptive safeguards for user data in the digital age.[147]

Under the GDPR[148], companies are obligated to follow strict regulations when processing user data, such as upholding data minimization, purpose limitation, and obtaining consent from the user. Data users were also given several rights over their own data, such as the right to complain, object, or

---

[143] Hern, A (2024, February 1). *Australia introduces world's toughest social media laws to protect children*. The Guardian. Available at: https://www.theguardian.com (Accessed on March 13, 2025)
[144] *Ibid*
[145] Australia's world-first social media ban for kids under 16 attracts mixed reaction," *The Straits Times*, November 29, 2024.
[146] The History of the General Data Protection Regulation. Available at: *https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en* (Accessed on 13 March 2025)
[147] *Ibid.*
[148] General Data Protection Regulation. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council.* Official Journal of the European Union, L 119/1.

request an erasure. Thus, GDPR is considered one of the most prominent and foundational pieces of legislation in the data protection movement.[149] Many countries have subsequently adopted its policies, regulations, and user rights, rehashing its content into their own legislations.

Following the implementation of GDPR, social media platforms such as TikTok, Facebook, and Snapchat set a minimum age requirement of 13 for users to sign up. However, child protection advocates argue that these self-imposed restrictions are insufficient, as official data from several European countries show that a significant number of children under 13 still have social media accounts. This has raised concerns about the effectiveness of age verification measures and the overall safety of young users online. To address these concerns, the EU enacted the Digital Services Act (DSA), which took effect in 2024. The DSA establishes stricter obligations for online platforms, including enhanced content moderation, greater transparency in algorithms, and stronger safeguards for protecting children from harmful content. The DSA aims to create a safer digital environment by ensuring that online platforms adhere to higher standards of accountability and safety for all users, especially minors.

At the European Union level, regulations require parental consent for the processing of personal data for children under 16. However, individual EU member states have the discretion to lower this threshold to 13, leading to variations in implementation across different countries.[150]

In the United Kingdom, the government has taken further steps to protect children online through the Online Safety Act, passed in 2023. This legislation enforces stricter standards for social media platforms, including implementing more robust age verification systems and imposing significant penalties on non-compliant platforms. Digital Minister Peter Kyle emphasized that ensuring online safety, particularly for children, remains a top priority. Ofcom, the UK's communications regulator, has been tasked with overseeing the enforcement of these safety measures and ensuring that platforms comply with government objectives related to safety by design, transparency, and accountability.[151]

Norway is considering raising the minimum age at which children can independently consent to social media terms from 13 to 15 years old. However, parents will still be allowed to approve their children's social media use if they are below the new age limit. The government has also begun work on legislation to set an absolute minimum age for social media use, though it remains unclear when this law may be passed.[152]

---

[149] Article 8, GDPR. *Where point (a) of Article 6 (1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. (2) Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. (3)Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*

[150] General Data Protection Regulation. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council.* Official Journal of the European Union, L 119/1.

[151] UK Parliament. (2023). *Online Safety Act 2023.* Available at: https://www.legislation.gov.uk/ukpga/2023/22/enacted (Accessed on February 12, 2025)

[152] Norwegian Data Protection Authority. (2018). *Personal Data Act.* Available at: https://www.datatilsynet.no. (Accessed on February 12, 2025)

France has taken a stricter approach, passing a law in 2023[153] that requires social media platforms to obtain parental consent for minors under 15 before they can create accounts. However, enforcement has been delayed due to technical challenges. In April 2024, a government-appointed panel recommended even stricter rules, including banning cellphones for children under 11 and prohibiting internet-enabled phones for those under 13. It remains uncertain when these recommendations might be translated into law.

In Germany, minors aged 13 to 16 are officially allowed to use social media only with parental consent. While there are no current plans to introduce further restrictions, child protection advocates argue that enforcement of existing regulations is weak and should be strengthened.[154]

Belgium enacted a law in 2018 requiring children to be at least 13 years old to create social media accounts without parental permission.[155] Similarly, Italy mandates that children under 14 need parental consent to sign up for social media accounts, while those aged 14 and above can create accounts independently.[156] The Netherlands does not have any laws setting a minimum age for social media use.[157] However, in January 2024, the government banned mobile devices in classrooms to reduce distractions, with exceptions for digital lessons, medical needs, or disabilities.

Overall, while social media platforms set a general minimum age of 13, European governments have adopted different approaches to regulating children's access to social media. Some, like France and Norway, are pushing for stricter age limits and enforcement, while others, like Germany and Belgium, rely on existing consent-based systems. With the European Union allowing flexibility in age thresholds, regulations across the region remain fragmented, reflecting different national priorities and enforcement challenges.

Rationale for Adopting the U.S. Kids Online Safety Act (KOSA) as a Model for Philippine Digital Child Protection Reform

The increasing vulnerability of Filipino children to online risks underscores the urgent need for comprehensive digital safety reforms in the Philippines. Despite the presence of local laws such as the Data Privacy Act of 2012, existing regulations remain insufficient in addressing the broader issue of digital child protection. The United States Kids Online Safety Act (KOSA) presents the most effective model for tackling these concerns, as it directly regulates algorithmic risks, harmful content exposure, and platform accountability—key areas where Philippine law remains inadequate.

Table 1 presents the comparative matrix among the foreign legislations earlier cited.

---

[153] French Government. (2023). *Loi No. 2023-451 on Parental Consent for Social Media Platforms.*
[154] Federal Republic of Germany. (2018). *Bundesdatenschutzgesetz (BDSG) - Federal Data Protection Act.*
[155] Belgian Data Protection Authority. (2018). *Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.*
[156] Italian Data Protection Authority. (2018). *Legislative Decree No. 101/2018.*
[157] Dutch Ministry of Education, Culture and Science. (2024). *Policy on Mobile Device Use in Schools.*

Feature	KOSA (US)	Online Safety Act (UK)	Digital Services Act (EU)	Australia Online Safety Act
Targeted Platforms	Social media platforms, content providers	Social media, search engines, messaging services	All online platforms, including marketplaces & social media	Social media, gaming, and other online services
Focus on Child Safety	Prioritizes protecting children from harmful content and addictive social media features	Requires platforms to prevent access to harmful content for children	Includes protections for minors but broader in scope	Implements the world's strictest social media ban for minors
Content Regulation	Requires platforms to provide parental tools and algorithms that limit harmful content	Holds platforms accountable for illegal/harmful content, especially for minors	Addresses illegal content, misinformation, and dark patterns	Bans social media for users under 16, enforced through strict verification
Enforcement & Penalties	Enforced by the Federal Trade Commission (FTC), potential fines for noncompliance	Ofcom (UK's communications regulator) enforces, with large fines for violations	Fines up to 6% of global turnover for violations	E-Safety Commissioner enforces, fines for non-compliance
Privacy & Data Protection	Limits data collection from minors, encourages age verification	Requires platforms to reduce risks for children, including stronger data privacy	Strengthens user data protections, transparency on algorithms	Strict identity verification required for age restrictions

Table 2 Comparative Analysis of Global Online Safety Frameworks

While global regulations such as the European Union's General Data Protection Regulation (GDPR) and national laws in the United Kingdom, France, and Norway provide critical privacy protections. they primarily focus on data security rather than the mental health and safety implications of social media

design. These frameworks fail to comprehensively regulate how algorithm-driven recommendations impact children's well-being, particularly their exposure to harmful or addictive content.[158]

In contrast to the UK Online Safety Act and the EU Digital Services Act, KOSA mandates that social media platforms disable algorithmic recommendations by default for minors, thereby reducing their risk of encountering inappropriate material. This preventive approach is particularly relevant to the Philippines, where children constitute a significant portion of social media users and remain highly susceptible to online dangers.[159]

Additionally, KOSA enhances parental controls and platform transparency, offering a realistic and enforceable framework that could be adapted to the Philippine context. Many Filipino parents are unaware of how social media algorithms shape their children's online behavior, and there is currently no Philippine law that imposes a clear duty of care on platforms. By adopting KOSA's principles, Philippine policymakers can establish legal obligations that require tech companies to proactively mitigate mental health harm, online exploitation, and algorithm-driven risks.[160] Unlike age-based restrictions, which are often difficult to enforce due to widespread digital access and limited parental oversight, KOSA's focus on harm prevention and platform responsibility makes it a more practical and effective model for the Philippines. Given the country's high digital penetration rate and challenges in regulatory enforcement, prioritizing proactive measures over reactive enforcement is essential.

The 2021 Australian Online Safety Act provides strong digital safety protections but takes a prohibitionist approach by enforcing a strict social media ban for users under 16.[161] While this model ensures that children are not exposed to harmful content, it also completely restricts access, which may not be culturally or logistically feasible in the Philippines, where internet and social media are integral to education and communication. Instead of a full ban, the Philippines should focus on harm reduction, which KOSA achieves through regulation, transparency, and parental control rather than outright prohibition. The influence of U.S. legislation on global digital policies cannot be overlooked. Major social media platforms—including Facebook (Meta), YouTube (Google), Instagram, TikTok (U.S. operations), Twitter (X), and Snapchat—are all headquartered in the United States. This means that KOSA's regulatory framework is designed to hold these companies accountable in ways that other nations have yet to fully implement. By modeling Philippine law on KOSA, the country could ensure that social media companies operating within its

[158] Livingstone, S., & Stoilova, M. (2021). The 4 Cs: Classifying online risk to children. Communications, Culture and Critique, 14(3), 326-346.

[159] Statista Research Department (2025), Number of social media Users. Available at: *https://www.statista.com/statistics/489180/number-of-social-network-users-in-philippines/* (Accessed on February 12, 2025)

[160] Sundar, S. S. (2023). Media Effects: Advances in Theory and Research. Routledge.

[161] Taylor, J. (2024, January 26). *Australia's bold step on child protection: Social media ban for under-16s sparks global debate*

jurisdiction adhere to the same level of accountability as they would under U.S. regulations.[162]

This approach aligns with the global trend of strengthening digital child protection and ensures that the Philippines remains proactive in adopting modern, effective online safety measures. Given the dominance of U.S.-based platforms in the digital landscape, looking at U.S. legislative efforts provides a strategic and logical foundation for Philippine online safety reforms. Through the adoption of KOSA's key provisions, the Philippines can establish a stronger legal framework that prioritizes child safety, promotes platform accountability, and aligns with international best practices in digital governance

VIII. THEORIES

This article is anchored in Social Responsibility Theory, which serves as the foundational framework for advocating the adoption of the U.S. Kids Online Safety Act (KOSA) in the Philippines to enhance child protection on social media platforms. This theory emphasizes that media entities, particularly social media companies, have an ethical obligation to operate in ways that benefit society beyond their profit-driven motives.[163] The adoption of child protection policies in social media governance aligns with broader societal expectations that corporations must contribute positively to public welfare. Holding digital platforms accountable for safeguarding minors is a critical step in ensuring that children can navigate online spaces safely and responsibly. By enacting comprehensive child protection laws, the Philippines can foster a safer and more ethical digital ecosystem, ensuring that social media platforms fulfill their duty to protect the most vulnerable members of society.[164]

The theoretical foundation of this article is the Social Responsibility Theory, which argues that organizations with significant influence over public welfare—such as social media platforms—must be held accountable for ensuring the safety and well-being of children. This perspective supports the author's advocacy for stricter regulatory measures that mandate online platforms to implement stronger child protection safeguards in their policies, algorithms, and content moderation systems. As applied to this article, the theory highlights the accountability of corporations in regulating content, fostering safe online environments, and ensuring the well-being of users, particularly vulnerable groups such as children. Given the increasing reliance on digital platforms, this theory underscores the necessity for media companies to balance their commercial interests with their duty to uphold ethical standards in protecting public welfare.[165]

The rapid expansion of social media, facilitated by the emergence of second-generation web technologies, has revolutionized digital interactions.

---

[162] Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media.*
[163] Siebert, F. S., Peterson, T., & Schramm, W. (1956). *Four theories of the press: The authoritarian, libertarian, social responsibility, and Soviet communist concepts of what the press should be and do.*
[164] UNICEF. (2021). *Digital connectivity and the protection of children's rights: Challenges and opportunities.*
[165] Christians, C. et al. (2009). *Media ethics: Cases and moral reasoning.*

Platforms such as Facebook have provided a highly interactive virtual space that transcends geographical, ethnic, political, and economic boundaries.[166] These platforms enable users to engage in content creation, dissemination, and social networking, significantly influencing modern communication and societal behavior.[167]

However, while social media offers numerous benefits—such as facilitating education, professional networking, and social activism—it also introduces significant risks, particularly for minors. Studies indicate that children and teenagers face dangers such as cyberbullying, exposure to harmful content, and data privacy breaches due to the lack of stringent safety measures in digital environments.[168]

In the Philippines, the absence of comprehensive online child protection laws exposes minors to these threats, emphasizing the urgency of adopting legislative frameworks like KOSA to address these evolving challenges.[169] Facebook, as the most widely used social media platform, plays a significant role in shaping online behavior and social responsibility. A study[170] examining social responsibility through Facebook usage found that users predominantly engage with the platform for social interaction and professional networking.

Data collected using a structured online survey indicated that, although the average session lasts only 15 minutes, many users log in multiple times a day, demonstrating the platform's pervasive influence. The study further revealed that users actively participate in content sharing and digital networking rather than passively consuming information. Additionally, platforms such as LinkedIn, Instagram, and WhatsApp were also identified as key digital spaces for interaction, with younger individuals tending to register on multiple social networking sites while older demographics exhibit a more selective online presence.[171]

Privacy concerns and security risks remain significant issues among social media users. Research indicates that while 92% of users modify their privacy settings to restrict access to personal information, a considerable portion (87.6%) still supports Facebook's practice of sharing user data with third parties for marketing purposes.[172] This suggests that while users acknowledge privacy risks, many are willing to exchange personal data for the convenience and engagement offered by digital platforms. Facebook's features—including messaging, news updates, events, groups, and multimedia sharing—serve to

---

[166] Kaplan, A. M., & Haenlein, M. (2010). *Users of the world, unite. The challenges and opportunities of social media*

[167] Boyd, D. M., & Ellison, N. B. (2007). *Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication.*

[168] Livingstone, S., Stoilova, M., & Nandagiri, R. (2017). *Children's data and privacy online: Growing up in a digital age*

[169] UNICEF. (2021). Digital connectivity and the protection of children's rights: Challenges and opportunities. United Nations Children's Fund. Available at: https://www.unicef.org/reports/digital-connectivity-children (Accessed on March 13, 2025)

[170] Ferri, F., Grifoni, P., & Guzzo, T. (2012). *New forms of social and professional digital relationships*

[171] *Ibid.*

[172] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). *Privacy and human behavior in the age of information*

strengthen both personal and professional relationships. However, these same features also present vulnerabilities, particularly regarding the spread of misinformation, online harassment, and data exploitation.[173] Despite its advantages, Facebook and other social media platforms pose significant challenges concerning privacy, data security, and content regulation. Studies have shown and emphasized that increased online engagement correlates with heightened exposure to cyber risks, reinforcing the need for stronger protective measures, particularly for minors.[174] Given the increasing amount of time children spend online, social media companies bear a moral and ethical responsibility to implement safety mechanisms that mitigate these risks. Under Social Responsibility Theory, digital platforms should not only provide engaging and accessible environments but also take proactive steps to ensure child safety by enforcing stricter regulations on harmful content, privacy protection, and digital literacy.[175]

KOSA embodies these principles by mandating heightened accountability for social media companies regarding user safety. The Act requires platforms to implement stronger content moderation policies, enhance age verification processes, and provide parental oversight tools.[176] By enforcing these measures, KOSA ensures that online environments prioritize the well-being of young users. Adopting similar legislation in the Philippines will align with global best practices, reinforcing the ethical imperative of corporate social responsibility in the digital age.[177] This theory provides a compelling argument to demand care from platforms to ensure the safety and well-being of children in online spaces. By advocating for this framework, the research seeks to hold social media companies and tech companies accountable for mitigating risks and promoting responsible online behavior. The comparative analysis with the U.S. Kids Online Safety Act serves as a benchmark for identifying specific areas where Philippine laws may fall short. This comparison highlights the need for stronger safeguards against those online harms.

By examining international best practices, particularly those exemplified in the U.S. Kids Online Safety Act, the research identifies concrete strategies that can be adopted and adapted to the Philippine context. This comparative approach allows for the formulation of legislative reforms that are both informed by global standards and tailored to the specific needs and challenges faced by Filipino children online. The study acknowledges its limitations, recognizing that its primary focus on the Philippine legal landscape may limit the generalizability of its findings to other countries. Furthermore, the ever-evolving nature of technology and online platforms necessitates continuous evaluation and adaptation of legal frameworks. The research emphasizes the importance of proactive and adaptive legal mechanisms that can keep pace with these changes and ensure ongoing protection for children in digital spaces. Despite these

[173] Zhang, W., & Livingstone, S. (2019). *Balancing opportunities and risks in children's digital lives*
[174] Holloway, D., Green, L., & Livingstone, S. (2020). EU Kids Online 2020: Survey results from 19 countries
[175] Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media.*
[176] Wright, M. (2022). *Accountability in the digital age: The Kids Online Safety Act. Journal of Cyber Law.*
[177] Livingstone, S., & Stoilova, M. (2021). *The 4 Cs: Classifying online risk to children. Communications, Culture and Critique.*

limitations, the study's ultimate goal is to spark meaningful policy changes that prioritize child welfare in the online sphere.

By advocating for a duty-of-care framework grounded in Social Responsibility Theory, the research aims to foster a safer and more child-friendly digital environment in the Philippines. The use of this framework in this thesis will place a greater responsibility on social media platforms and tech companies to protect children from online harms, promote responsible online behavior, and prioritize child well-being in their design and operation.

In essence, this article serves as a call to action, urging policymakers, tech companies, and other stakeholders to take proactive steps toward creating a digital world where children can thrive without compromising their safety and well-being.

Child Development Theory

Developmental theories underscore the crucial nature of childhood. Piaget's cognitive development theory emphasizes children's evolving understanding of the world through interaction, now increasingly digital. Erikson's psychosocial theory highlights the importance of social relationships in shaping identity. Childhood is a foundational period, and experiences during this time are pivotal.

The concept of childhood has evolved. Early thinkers like Comenius, Rousseau, and Froebel emphasized children's well-being. Societal perceptions have shifted from pre-modern views of children as "adults in training" to modern views of them as "innocent and fragile," and finally to postmodern views of them as active participants in culture.

Today, childhood is threatened by abuse, neglect, consumerism, and excessive technology use, which can replace meaningful interactions. The home environment plays a critical role in shaping a child's character. The "best interests of the child" principle is paramount in all matters concerning children, as affirmed by the Philippine Child and Youth Welfare Code.[178] This principle is echoed in the Child and Youth Welfare Code of the Philippines, which mandates the protection of children against exploitation, improper influences, hazards, and other conditions or circumstances prejudicial to his physical, mental, emotional, social and moral development. A holistic understanding of childhood recognizes the interconnectedness of physical, intellectual, social, and emotional development. Educators recognize that a child's growth is influenced by their cultural and familial contexts, as well as their genetic backgrounds, which contribute to their individuality and learning styles. Despite these insights, there is growing concern among child development advocates about the premature pushing of children toward adulthood. This shift, driven by the pressures of technology, social media, and the rush toward academic achievements, can undermine the essence of childhood.

[178] Coquia, J. R. (2012). *Human rights. Central Book Supply Inc., page 129*

David Elkind's 1982 observations remain relevant today, highlighting the importance of valuing childhood as a period with unique challenges and joys. Elkind argues that children have a fundamental right to experience childhood, with its inherent pleasures and trials, free from the pressures of being hurried into adulthood. The early years of life serve as a critical foundation for all aspects of development, making it essential to respect the differences between childhood and adulthood. Recognizing the distinctive ways in which children learn—through play, discovery, and hands-on experiences—has led to the creation of diverse programs aimed at supporting young learners. These programs reflect a broader societal acknowledgment of the need to nurture and protect the childhood experience, ensuring that children are given the time and space to grow and thrive in their own way.[179]

The exposure to social media at a young age can impact these developmental stages significantly. The premature introduction of inappropriate content or cyberbullying can hinder a child's emotional growth and social skills. Studies show that excessive screen time and exposure to negative online experiences can lead to anxiety, depression, and issues with self-esteem.[180]

Cyberbullying incidents can be found across a wide range of social media platforms, each presenting different forms and levels of severity. From hurtful comments and targeted harassment to more severe cases like threats, these incidents occur on platforms where users, especially minors, interact and communicate. The diversity of social media sites from popular ones like Instagram, TikTok, and Facebook to more niche forums—means that the nature and impact of cyberbullying can vary, but the potential for harm remains a constant concern across the digital landscape. Therefore, understanding child development is essential for assessing how social media use can affect young users and highlights the urgent need for protective legal measures.

Social media platforms often expose children to idealized representations of life, bodies, and success. This constant comparison can foster feelings of inadequacy, anxiety, and depression. Prolonged exposure to harmful content, such as posts glorifying self-harm, eating disorders, or negative body images, can exacerbate these mental health challenges. Children exposed to violent content or inappropriate behaviors online may become desensitized to violence or normalize unhealthy behaviors. Exposure to violent games, graphic videos, or aggressive interactions in online spaces can blur the line between acceptable and unacceptable behavior, potentially leading to aggressive tendencies or apathy toward others' suffering. This exposure may increase the likelihood of children mimicking such behavior, especially if they are exposed to violence within their homes or communities. They may become more prone to bullying others or behaving aggressively, thinking such behaviors are a normal part of social interactions. These effects are more pronounced in younger children, whose ability to differentiate between fantasy and reality is still developing.

[179] Twenge, J. M., Martin, G. N., & Spitzberg, B. H. (2019). *Trends in U.S. adolescents' media use, 1976–2016: The rise of digital media, the decline of TV, and the (near) demise of print.*
[180] Ibid.

Early and excessive use of social media can hinder a child's social development, particularly when online interactions replace face-to-face communication. Social media fosters instant gratification and superficial interactions, which can limit the development of empathy, communication skills, and emotional intelligence. Children may struggle with forming meaningful relationships, as they become more accustomed to interacting through screens rather than real-world experiences.

Social media opens the door for cyberbullying, in which children can become both victims and perpetrators of online harassment. Cyberbullying can cause severe emotional trauma, including social anxiety, depression, and, in extreme cases, suicidal ideation. Unlike traditional bullying, cyberbullying can be relentless, continuing outside school hours and into a child's private life. The anonymity of social media can also embolden bullies to harass or shame others without fear of immediate consequences.

Children's lack of digital literacy makes them particularly vulnerable to online predators who exploit their naivety. Predators can use social media platforms to groom children, gradually gaining their trust with the intent to exploit them sexually or financially. The early exposure of minor children to harmful content on social media presents numerous risks to their mental, emotional, and social well-being. The unchecked consumption of such content can lead to significant long-term effects, including mental health issues, desensitization to violence, and an inability to develop meaningful social relationships. Given these concerns, it is essential that caregivers and policymakers work together to strengthen regulations and educate children about digital safety and responsible internet use.

B. Doctrine of *Parens Patriae*

The United Nations Convention on the Rights of the Child (UNCRC) establishes a comprehensive framework for the protection and promotion of children's rights, including their right to an adequate standard of living. The *parens patriae* doctrine serves as a legal mechanism through which the state fulfills its responsibility to safeguard children, particularly in situations where parents or guardians are unable or unwilling to do so.[181]

The term *parens patriae*, which translates from Latin as "parent of the nation" or "parent of the country," has its roots in English common law, where it originally referred to the king's responsibility to care for those unable to protect themselves, such as minors, individuals with disabilities, and others requiring state intervention. This principle underscores the state's role as the ultimate guardian of minors, ensuring their welfare, security, and access to fundamental needs such as education, healthcare, and protection from abuse and exploitation.

Over time, this principle was adopted by various legal systems, including that of the Philippines, where it forms the legal foundation for government intervention in cases concerning children's welfare. It grants the state the

[181] Coquia, J. R. (2012). *Human rights.* Page 130

authority to step in when a child's best interests are at risk, ensuring that their rights are upheld despite parental incapacity or neglect.[182]

In the Philippine legal system, the doctrine of *parens patriae* has been upheld in multiple Supreme Court rulings, reinforcing the government's role in child protection. A key case demonstrating this principle is Nery v. Lorenzo[183], where the Supreme Court explicitly stated that the state has the duty to act as *parens patriae* when minors are involved.

> "Moreover, where minors are involved, the State acts as parens patriae. To it is cast the duty of protecting the rights of persons or individual who because of age or incapacity are in an unfavorable position, vis-a-vis other parties. Unable as they are to take due care of what concerns them, they have the political community to look after their welfare.
>
> This obligation the state must live up to. It cannot be recreant to such a trust. As was set forth in an opinion of the United States Supreme Court: This prerogative of parens patriae is inherent in the supreme power of every State, whether that power is lodged in a royal person or in the legislature, and has no affinity to those arbitrary powers which are sometimes exerted by irresponsible monarchs to the great detriment of the people and the destruction of their liberties. On the contrary, it is a most beneficent function, and often necessary to be exercised in the interest of humanity, and for the prevention of injury to those who cannot protect themselves."

The ruling emphasized that children, due to their age and vulnerability, may find themselves in an unfavorable position compared to other parties. Therefore, it is the collective responsibility of parents, the private sector, and the political community to ensure their protection and welfare. This duty becomes particularly crucial in situations where parents fail to fulfill their obligations or where the best interests of the child are at risk due to neglect, maltreatment, or other harmful conditions.

C. Legal Paternalism

The Legal Transplant Theory explores how legal concepts and frameworks from one jurisdiction can be effectively integrated into another. Table 2 illustrates U.S. legal influences on Philippine laws, demonstrating that the Philippines has a long history of adopting legal principles from the U.S., reinforcing the applicability of this theory.

[182] *Ibid.* Page 131
[183] G.R. No. L-23096, 27 April 1972

U.S. Law/ Principle	Philippines Adaptation	Description
Bill of Rights (U.S. Constitution)	Bill of Rights (1987 Philippine Constitution, Article III)	The Philippine Bill of Rights is heavily influenced by the U.S. Bill of Rights, ensuring fundamental freedoms such as freedom of speech, due process, and equal protection under the law.
Miranda Rights (Miranda v. Arizona, 1966)	Miranda Doctrine (People v. Mahinay, 1994)	The requirement for law enforcement to inform an arrested person of their rights, including the right to remain silent and have legal counsel, is based on the U.S. Supreme Court ruling in Miranda v. Arizona.
Foreign Corrupt Practices Act (1977)	Anti-Graft and Corrupt Practices Act (Republic Act No. 3019)	Similar to the U.S. law, this Philippine law penalizes corrupt practices by public officials, including bribery and misuse of public office.
Administrative Procedure Act (1946)	Administrative Code of 1987 (Executive Order No. 292)	The Philippine Administrative Code establishes procedures for administrative agencies, mirroring U.S. administrative law principles.
Sherman Antitrust Act (1890)	Philippine Competition Act (Republic Act No. 10667)	The Philippine law is modeled after U.S. antitrust laws, promoting fair competition and prohibiting monopolistic practices.
National Labor Relations Act (Wagner Act, 1935)	Labor Code of the Philippines (Presidential Decree No. 442, as amended)	The Philippine labor laws adopt U.S. labor principles, including the right to organize, collective bargaining, and protection against unfair labor practices.
Children's Online Privacy Protection Act (COPPA, 1998)	Data Privacy Act of 2012 (Republic Act No. 10173)	While not identical, the Data Privacy Act adopts privacy principles similar to COPPA, particularly in protecting minors' data online
Freedom of Information Act (FOIA, 1966)	Executive Order No. 2, s. 2016 (Freedom of Information Order)	The Philippine FOI order was influenced by the U.S. FOIA, allowing access to government records to promote transparency and accountability.
Securities Exchange Act (1934)	Securities Regulation Code (Republic Act No. 8799)	The Philippine law follows U.S. securities regulations, ensuring transparency and fair trading in financial markets.

U.S. Law/ Principle	Philippines Adaptation	Description
Cybercrime Prevention Act (U.S. Computer Fraud and Abuse Act, 1986)	Cybercrime Prevention Act of 2012 (Republic Act No. 10175)	Philippine law takes inspiration from U.S. cybercrime laws, addressing hacking, cyber fraud, and online defamation.

Table 2: Legal Transplant Theory & Relevant Laws

From constitutional rights and due process protections to corporate regulations and data privacy laws, the Philippine legal system has successfully incorporated U.S.-inspired legal frameworks while adapting them to local conditions. This historical precedent suggests that the integration of the U.S. Kids Online Safety Act (KOSA) into Philippine law is not only possible but also a logical progression in strengthening child protection online. However, successful legal transplantation requires more than direct adoption—it necessitates alignment with local cultural, social, and institutional contexts. For instance, while the U.S. Miranda Doctrine was integrated into Philippine jurisprudence, it had to be contextualized within the country's existing procedural laws.

Similarly, adapting KOSA's provisions, such as mandatory safety settings, content moderation obligations, and platform accountability, would require careful consideration of the Philippines' digital infrastructure, child protection mechanisms, and existing data privacy laws. Moreover, the Philippine legal landscape often reflects a balance between global best practices and domestic realities, as seen in the adaptation of U.S. competition laws, anti-corruption measures, and securities regulations.

A successful adaptation of KOSA will require multi-stakeholder collaboration, involving government agencies, educational institutions, civil society organizations, and technology companies. Just as Philippine labor laws were shaped by U.S. labor principles but adjusted to the local workforce's needs, KOSA's adoption must be customized to fit the socio-political realities of the Philippines. This includes addressing enforcement challenges, ensuring alignment with existing child protection laws, and fostering digital literacy among parents and educators.

By embracing the principles of Legal Transplant Theory, the Philippines can develop a well-calibrated legal framework for child online safety. Learning from past legal borrowings, the country can ensure that any adaptation of KOSA is not only legally sound but also culturally and socially relevant. This approach will allow for a more informed and sustainable enhancement of child protection laws in the digital age.

IX. METHODOLOGY

This research shall use the doctrinal or blackletter approach. Briefly, it is a type of descriptive research based on thorough analysis and comprehensive interpretation of available and existing documentary materials, data, or facts in law. Furthermore, this approach heavily relies on the doctrinal attitude in the study of law in a substantive manner. As such, it seeks to study and analyze existing laws, jurisprudence, doctrines, and other relevant data, in relation with the subject matter of the research. Notably, the blackletter methodology is not simply a perspective upon, or even a style of articulating, the substantial nature of a research topic. Instead, it is an interpretative scheme whose overall framework of categories, assumptions and concerns operate to both set up and demarcate the very meaning, scope and purpose of one's research optic and project.[184] This research utilizes existing data and sources, such as existing laws, regulations, treaties, international conventions and declarations, and published books or articles in analyzing the legal issues involved, explaining the pertinent legal doctrines and principles, and arriving at the objective of a proposed legislation for the comprehensive protection of children in their online activities, in alignment with the country's international commitments and best practices

The blackletter approach provides an avenue for a straightforward manner of understanding the law through research. It provides a practical basis through which independent legal research can be undertaken and leads to the development of core research skills such as retrieval, assessment, and analysis of legal texts as vital legal practices.[185] This is essential for this particular research, considering that its main objective is to compare and institutionalize protective mechanisms for children in the country, using publicly available sources and relevant data requested from pertinent agencies and organizations. This research approach provides a significant advantage to this article, given its primary objective of enhancing child protection in digital spaces through legislative reform or adoption of best practices of foreign laws.

Furthermore, analyzing these data points enables the author to develop a practical and effective legislative measure tailored to safeguarding children online. Lastly, this approach facilitates an evaluation of the potential impact of the proposed legislation on the Philippine legal system, both at the domestic and international levels, ensuring that it aligns with global standards for child online safety. However, given this approach, the article does not provide an individualized analysis of the suitability or effectiveness of the proposed legislation for each child using social media in the Philippines. Instead, this research conducts a comprehensive legal analysis of available data, aiming to recommend legislative measures that ensure the country's full compliance with its international obligations on child online protection. In line with this, the article does not employ surveys or interviews as an integral part of its methodology, focusing instead on legal and policy analysis.

---

[184] Michael Salter and Julie Mason, *Writing Law Dissertations,* (England: Pearson Education Limited, 2007).
[185] ***Black Letter and Socio Legal Research Methods,*** https://www.studocu.com/row/document/university-of-balochistan/constitutional-law/black-letter-and-socio-legal-research-methods/16555844, accessed on 24 February 2025.

Historical

The historical method involves tracing the development of child protection laws in the Philippines, particularly in relation to digital spaces. This approach examines the evolution of Philippine legislation influenced by both domestic needs and foreign models, notably U.S. legal principles. Understanding the historical context provides insights into why certain gaps exist in the current framework and how previous reforms were shaped. By analyzing historical legislative patterns and legal borrowings, the article aims to reinforce the relevance and feasibility of adopting foreign models like the U.S. Kids Online Safety Act (KOSA) to address modern challenges faced by Filipino children on social media. This historical lens highlights that Philippine legal reforms often emerge in response to societal shifts rather than proactive regulation. It also reveals that while foreign influences have been crucial in legal development, localized adaptation remains a persistent challenge. By studying past efforts to regulate media and technology, the research identifies patterns of delay, partial adoption, and gaps in enforcement. Ultimately, this historical understanding strengthens the case for a more comprehensive and forward-looking approach to online child protection.

Analytical

This involves understanding both the strengths and limitations of Philippine legislation when it comes to addressing the unique challenges posed by social media use among minors. By pinpointing these gaps, the article aims to recommend improvements to better protect children in online environments. By interpreting these legal provisions, the article can determine whether they align with international standards and best practices.

It also evaluates how comprehensively they address new challenges posed by digital platforms, such as protecting children from inappropriate content, ensuring their privacy, and holding social media companies accountable for child safety. This approach is effective in determining whether the existing legal framework is sufficient or if reforms are needed to address emerging online risks to children.

Comparative

Comparative analysis encompasses the examination of various legal systems to gain insights into how different jurisdictions tackle similar legal issues. This approach is particularly relevant in the context of child protection online, as it allows for a thorough analysis of the U.S. Kids Online Safety Act (KOSA) and other foreign laws as a benchmark for enhancing legal protections for children in the Philippines. The rationale for this comparison lies in the fact that different countries have adopted varied legal approaches to online child safety and studying these differences can reveal best practices and effective regulatory measures that could be adopted or adapted by the Philippines.

The U.S. KOSA, for instance, provides comprehensive guidelines on content moderation, data privacy, and ensuring age-appropriate user

experiences, making it a useful benchmark for evaluating Philippine laws. This comparison helps the study to explore how different jurisdictions tackle similar challenges in protecting children online, such as managing the content that minors are exposed to and ensuring their online data privacy. It allows the research to highlight gaps in the Philippine regulations where they may lack the specificity or enforcement mechanisms seen in U.S. laws. This analysis can further uncover opportunities for policy adaptation, such as incorporating specific provisions from KOSA that address issues like digital literacy, transparency in content algorithms, and stronger protections against harmful content. By pinpointing these gaps, the study aims to offer practical recommendations for reforming Philippine laws, aligning them with international best practices in child protection.

Ultimately, leveraging insights from comparison can facilitate a more robust legal framework in the Philippines, ensuring that children's rights and safety are prioritized in the ever-evolving digital landscape. By adopting proven strategies from other jurisdiction, the Philippines can enhance its commitment to protecting minors online and fostering a safer internet environment. The sources of data for this research are the following:

i. The 1987 Philippine Constitution;
ii. Relevant domestic laws related to child online protection;
iii. Supreme court decisions and jurisprudence;
iv. Administrative rules, regulations, memoranda, department orders or circulars, and other issuances;
v. Reports and databases from relevant government agencies, including the UNHCR and DOJ;
vi. National Privacy Commission advisories and issuances;
vii. Reports from other relevant international organizations;
viii. Published articles and research papers, both printed and online;
ix. Congressional hearings and transcripts, if available;
x. Internet sources; and
xi. Books and other printed or recorded materials.

The article relies on secondary sources of data, focusing on legal documents, scholarly literature, historical records, and case law analysis. It draws on a range of existing laws and policies in the Philippines related to child protection on social media, examining government publications, economic reports, and legal documents to assess current regulatory measures and their effectiveness in safeguarding children online. Additionally, it reviews relevant judicial decisions and legal interpretations concerning child protection and digital rights to identify trends and precedents. Scholarly literature, such as academic papers and journals, provides theoretical perspectives and empirical findings that support a comprehensive understanding of child digital safety.

The author utilized online databases and visited libraries, including UST, Makati City Hall Library, and Quezon City Library, which provide convenient access to extensive compilations of secondary data. These resources allow students to draw from a vast collection of studies and references for in-depth analysis. To reiterate, the blackletter approach is best suited for this research due to its primary objective of proposing a legislative framework for the

comprehensive protection of children on social media in the Philippines. This approach ensures alignment with the country's international obligations under relevant conventions on child online safety.

Accordingly, the most effective method to achieve this objective is to examine existing laws, regulations, and policies governing online child protection, evaluate their effectiveness and compliance with international standards, and propose legislative reforms that institutionalize stronger and more comprehensive protective mechanisms for children in the digital space.

X. EXISTING PHILIPPINE LAWS AND JURISPRUDENCE PROTECT CHILDREN FROM ONLINE ACTIVITIES?

Before delving into the specific rights of children in the digital space, it is essential to first examine the legal frameworks currently in place in the Philippines. This assessment includes the scope, limitations, and guiding principles behind the adoption and enforcement of relevant laws. To comprehensively address this research problem, this article first analyzes the existing statutes, policies, and jurisprudence that govern child online protection. It then evaluates whether current legislative measures are sufficient to address emerging threats and propose areas for potential reform.

With the rapid increase in internet and social media usage among Filipino children, digital platforms have become both an indispensable tool and a significant source of risk. While these platforms provide access to educational resources, social interaction, and creative expression, they also expose minors to threats such as cyberbullying, online sexual exploitation, exposure to harmful content, and data privacy breaches. Thus, ensuring a safe digital environment for children requires not only strong legislative safeguards but also effective implementation and enforcement mechanisms. This section presents a detailed examination of the Philippine legal landscape on child online protection, analyzing how existing laws safeguard minors from digital risks. It also explores the penalties imposed on violators and evaluates the adequacy of these legal provisions in addressing the evolving challenges of the digital age. Table 3 summarizes key Philippine laws relevant to child online protection:

Existing Philippine Laws			
Philippine Law	**Year of Enactment**	**Purpose**	**Children's Rights Protected**
RA No. 9775 – Anti-Child Pornography Act	2009	Criminalizes child pornography, prohibits the use of children in any pornographic material, and mandates ISPs to block access to such content.	Protection from sexual exploitation, right to dignity, and privacy.

RA No. 10364 – Expanded Anti-Trafficking in Persons Act	2012	Strengthens measures against human trafficking, including recruitment and exploitation of children for pornography. Recognizes that a victim's consent is irrelevant in trafficking cases.	Protection from trafficking, right to security and protection from abuse.
RA No. 11930 – Anti-Online Sexual Abuse and Exploitation of Children (OSAEC) Act	2022	Addresses online exploitation, mandates community-based interventions, and requires age verification for adult content.	Protection from online abuse, right to safety, and freedom from exploitation.
RA No. 7610 – Special Protection of Children Against Abuse, Exploitation, and Discrimination Act	1992	Provides special protection against abuse, neglect, cruelty, and exploitation, including digital and online threats.	Protection from all forms of abuse and discrimination, right to development in a safe environment.
RA No. 10173 – Data Privacy Act	2012	Regulates the collection, processing, and storage of personal data, particularly for minors, ensuring their privacy and safety online.	Right to privacy, protection from data exploitation and cyber threats.
RA No. 10175 – Cybercrime Prevention Act	2012	Criminalizes cybercrimes such as child pornography, cyberbullying, identity theft, and other digital offenses.	Protection from cyberbullying, digital exploitation, and harmful online content.

RA No. 11313 – Safe Spaces Act (Bawal Bastos Law)	2019	Prohibits gender-based sexual harassment in public, workplaces, schools, and online spaces. Requires institutions to establish policies against harassment.	Right to a safe environment, protection from gender-based harassment and abuse
RA No. 10929 – Free Internet Access in Public Places Act	2017	Provides free internet in public spaces, promoting access to education and digital literacy while addressing online safety concerns.	Right to access information, right to education, and protection from online risks

Table 3: Existing Philippine Laws

Through this analysis, the article evaluates the effectiveness of current Philippine laws in mitigating digital threats against children, identify legislative gaps, and emphasize the need for a more robust and comprehensive legal framework. In doing so, it assesses whether existing protections align with international standards and best practices, ensuring that Filipino children are safeguarded in an increasingly interconnected digital landscape.

R.A. 9775 (Anti-Child Pornography Act of 2009)

The Anti-Child Pornography Act of 2009 criminalizes the creation, possession, and distribution of child pornography. The law mandates internet service providers (ISPs) to block access to websites containing child pornography and requires internet content hosts to report any instances of such material.

Strengths:

1. Provides a clear definition of child pornography
2. Mandates proactive measures from ISPs and internet content hosts
3. Aligns with international standards like the Luxembourg Guidelines

Limitations:

1. May not fully address new and evolving forms of online child sexual exploitation, such as live streaming of abuse and the use of social media for distribution
2. Enforcement can be challenging due to the anonymity and cross-border nature of online offenses.

R.A. 10364 (Expanded Anti-Trafficking in Persons Act)

This Act expands the previous anti-trafficking law (R.A. 9208) to include online offenses. It prohibits the recruitment, transportation, or harboring of children for the purpose of engaging in pornography or sexual exploitation

through online means. The law recognizes that a victim's consent is irrelevant in cases of child trafficking[186] and exploitation.

Strengths:
1. Explicitly addresses online child trafficking and exploitation
2. Emphasizes the State's responsibility to protect children from all forms of sexual exploitation
3. Promotes international cooperation to combat trafficking networks

Limitations:
1. May not specifically address online grooming and the use of social media to facilitate trafficking
2. Enforcement can be complex due to jurisdictional issues and the difficulty in identifying online traffickers.

R.A. 11930 (Anti-OSAEC and Anti-CSAEM Act)

This Act directly addresses online sexual abuse and exploitation of children (OSAEC) and child sexual abuse or exploitation materials (CSAEM). It mandates local governments to implement community-based initiatives for prevention and response. It also requires online providers of adult content to adopt age verification protocols.

Strengths:
1. Specifically targets OSAEC and CSAEM
2. Promotes a localized approach to prevention and response
3. Emphasizes rehabilitation and reintegration of victims
4. Mandates age verification for adult content websites

Limitations:
1. Implementation and effectiveness require further examination.
2. Challenges remain in enforcing age verification and monitoring online content.

R.A. No. 7610 (Special Protection of Children Against Abuse, Exploitation, and Discrimination Act)

While enacted before the widespread use of social media, this Act provides a broad definition of child abuse and exploitation that can be adapted to the digital context. It emphasizes preventive measures and empowers authorities to act against online offenders.

Strengths:

[186] Republic Act No. 10364, An Act Expanding the Definition of Trafficking in Persons and Amending Republic Act No. 9208, Otherwise Known as the "Anti-Trafficking in Persons Act of 2003," and for Other Purposes, June 21, 2012. Child Trafficking - Any person who shall engage in trading and dealing with children including, but not limited to, the act of buying and selling of a child for money, or for any other consideration, or barter, shall suffer the penalty of reclusion temporal to reclusion perpetua. The penalty shall be imposed in its maximum period when the victim is under twelve (12) years of age.

1. Provides a broad legal framework that can encompass online forms of abuse and exploitation
2. Emphasizes preventive measures and community initiatives

Limitations:
1. Requires specific interpretation and application to the digital context
2. May need further amendments to explicitly address online grooming and cyberbullying

R.A. 10173 (Data Privacy Act of 2012)

This Act regulates the collection, processing, and storage of personal data, including children's data. It requires organizations to obtain consent from parents or guardians before processing children's data.

Strengths:
1. Protects children's privacy by regulating data collection and processing
2. Promotes transparency and accountability in data handling practices

Limitations:
1. General application to individuals, but no specific provisions for children
2. Application to children's data on social media lacks clear guidelines and requires further clarification.
3. Enforcement mechanisms need strengthening.

R.A. 10175 (Cybercrime Prevention Act of 2012)

This Act addresses various cybercrimes, including cyberbullying and child pornography. It increases the penalties for offenses under the Anti-Child Pornography Act when committed through a computer system.

Strengths:
1. Criminalizes cyberbullying and online child pornography
2. Provides a legal framework for addressing various online offenses

Limitations:
1. Lacks specific provisions tailored to child online safety
2. Enforcement can be challenging due to the borderless nature of cybercrime.

R.A. 11313 (Safe Spaces Act)

This Act prohibits gender-based sexual harassment in online spaces, which is relevant to protecting children from online harassment and abuse. It requires institutions to establish policies and protocols for addressing online sexual harassment.

Strengths:

1. Addresses online sexual harassment, which can affect children
2. Requires institutions to take proactive measures to prevent and address online harassment

Limitations:
1. May need further strengthening and specific provisions to address the unique vulnerabilities of children in online spaces
2. Enforcement and monitoring mechanisms may be insufficient to ensure full compliance by online platforms.

R.A. 10929 (Free Internet Access in Public Places Act)

This Act mandates the provision of free internet access in public places, including schools and libraries. While its primary aim is to improve access to information, it can also be leveraged to promote online safety education for children.

Strengths:
1. Provides opportunities for online safety education in schools and libraries
2. Promotes digital literacy and access to information

Limitation:
1. Does not mandate online safety education or provide specific guidelines for its implementation
2. Increased internet access may expose children to online risks without corresponding protective measures in place.

U.S. KIDS ONLINE SAFETY ACT REGULATE CHILDREN'S USE OF ONLINE PLATFORMS

It provides a focused analysis of the U.S. legal framework for child online protection, with a particular emphasis on the Kids Online Safety Act (KOSA) and its interplay with existing legislation. Table 4 provides a clear understanding of how these U.S. laws collectively contribute to safeguarding minors in digital spaces.

US Laws	**Year Enacted**	**Purpose**	**Children's Rights Protected**
Child Online Protection Act (COPA)	1998	Restricted minors' access to online content deemed harmful. Declared unconstitutional due to First Amendment concerns.	Protection from harmful online content (not enforced).

US Laws	Year Enacted	Purpose	Children's Rights Protected
Children's Online Privacy Protection Act (COPPA)	1998	Regulates online data collection from children under 13, requiring parental consent.	Privacy and data protection.
Children's Internet Protection Act (CIPA)	2000	Requires schools/libraries using federal funds to implement content filters and safety policies.	Protection from obscene/harmful online content.
PROTECT Our Children Act	2008	Strengthens law enforcement's ability to combat child exploitation online and Mandates internet safety education in schools and libraries receiving federal funds	Protection from online sexual exploitation and abuse.
Kids Online Safety Act (KOSA) (Proposed)	Pending	Expands protections by requiring platforms to implement safety measures, content moderation, and parental controls.	Protection from harmful content, mental health risks, and online exploitation

Table 4 : US LAWS

The Children's Online Privacy Protection Act (COPPA)

Enacted in 1998[187], COPPA is a foundational law for protecting children's online privacy in the U.S. It requires websites and online services directed at children under 13 to obtain verifiable parental consent before collecting, using, or disclosing personal information. COPPA mandates clear privacy policies, gives parents access to their child's information, and allows them to request its deletion.

Strengths:

1. Parental Control: Empowers parents by requiring verifiable consent before children's data is collected
2. Transparency: Mandates clear privacy policies, allowing parents to monitor and manage their child's online data

[187] Signed into law by President Bill Clinton on 21 October 1998.

3. Legal Accountability: Holds online services accountable for improperly handling children's personal information

Limitations:
1. Narrow Age Scope: Applies only to children under 13, leaving older minors without specific protections
2. Evasion by Platforms: Some websites and apps circumvent COPPA by claiming they are not directed at children.
3. Challenges in Enforcement: Keeping up with evolving technologies and ensuring compliance remains difficult.

The Children's Internet Protection Act (CIPA)

CIPA focuses on protecting children in schools and libraries that receive federal funding for internet access. It requires these institutions to implement internet safety policies and technology protection measures to block access to harmful content, including obscenity, child pornography, and material harmful to minors. CIPA also mandates online safety education for minors.

Strengths:
1. Safe Educational Environments: Requires schools and libraries to implement protective measures for internet use
2. Mandatory Online Safety Education: Ensures students receive education on safe internet use
3. Funding Requirement Compliance: Institutions must meet CIPA standards to receive federal internet subsidies.

Limitations:
1. Focus on Filtering: Primarily relies on content filtering rather than addressing root causes of online risks
2. Limited Scope: Applies only to schools and libraries receiving federal funding, leaving other children unprotected
3. Potential Over blocking: May restrict access to beneficial educational content due to broad filtering.

The Kids Online Safety Act (KOSA)

KOSA, introduced in 2022, represents a significant step forward in child online protection in the U.S. It addresses a wider range of online risks, including cyberbullying, promotion of self-harm and eating disorders, and predatory behavior. KOSA requires platforms likely to be accessed by minors to:

1. Implement age-appropriate design features, parental controls, and tools to mitigate risks of harm;
2. Regularly assess the risks their products and services pose to minors;
3. Provide easy-to-use mechanisms for minors and parents to report concerns and control settings; and
4. Clearly explain data collection practices and provide access to privacy policies.

Strengths:

1. Broad Protection: Addresses various online risks beyond data privacy, including mental health and safety concerns
2. Platform Accountability: Places legal obligations on online platforms to assess risks and implement protections
3. Adaptability: Encourages ongoing research and updates to ensure effectiveness against emerging threats

Limitations:

1. Enforcement Complexities: Ensuring compliance from global platforms presents jurisdictional challenges
2. Parental Control vs. Autonomy: Potential concerns over how much control parents should have over teenagers' online activities
3. Industry Pushback: Tech companies may resist stricter regulations due to compliance costs and business interests.

The Kids Online Safety Act (KOSA) in the United States introduces a comprehensive framework to regulate children's use of online platforms by imposing obligations on digital service providers. Unlike KOSA, Philippine laws lack specific and enforceable provisions that directly address child online safety in the same manner. While existing laws such as the Anti-Child Pornography Act (R.A. 9775) and the Anti-Online Sexual Abuse and Exploitation of Children (OSAEC) Act (R.A. 11930) aim to protect children from digital exploitation, they do not establish a broad, platform-wide responsibility for social media companies similar to KOSA. Table 5 presents the analysis of KOSA vis-à-vis Philippine laws.

Table 5: Comparative Analysis of U.S. KOSA and Philippine Existing Laws

KOSA COMPARATIVE ANALYSIS		
Key Provision	**U.S KOSA**	**PH LAWS**
Mandatory Safety Settings	✔ (for minors)	✘
Risk Assessments	✔ (for platforms)	✘
Content Moderation Obligations	✔ (for harmful content)	✘
Platform Accountability	✔ (for child safety practices)	✘
Age-appropriate design	✔ (considerations for children)	✘
Parental control requirements	✔ (tools and information provided)	✘
Data Privacy Protections	✔ (specific provisions for children)	✔ (but enforcement and clarity need improvement)

One key aspect of KOSA is its requirement for mandatory safety settings for minors, ensuring that platforms mitigate exposure to harmful content and online risks. However, in the Philippines, there is no corresponding law that

requires online platforms to implement automatic safety measures, leaving child protection largely at the discretion of service providers and parents. Without mandated default protections, Filipino children remain vulnerable to harmful content, targeted advertising, and potential online predators.

Another crucial distinction is KOSA's requirement for digital platforms to conduct regular risk assessments to identify and mitigate potential harms to children, such as exposure to cyberbullying, self-harm content, and online exploitation. This proactive approach compels companies to anticipate and address risks before they become widespread. In contrast, Philippine laws do not impose similar requirements, making it difficult to systematically assess and mitigate online dangers affecting children. The Cybercrime Prevention Act (RA No. 10175) criminalizes online offenses, but it primarily addresses individual cybercrimes rather than placing proactive obligations on online platforms to prevent harm. Without mandated risk assessments, Filipino children continue to be exposed to digital threats without structured preventive mechanisms. In terms of content moderation, KOSA enforces strict policies requiring platforms to prevent the spread of harmful content targeting minors, including material related to self-harm, child exploitation, and other online dangers. The law ensures that platforms actively filter and remove harmful materials before they reach children.

The Philippines, however, lacks a parallel legal mandate compelling platforms to take similar measures. While existing laws such as the Special Protection of Children Against Abuse, Exploitation, and Discrimination Act (RA No. 7610) and the OSAEC Act address child exploitation, they do not establish comprehensive content moderation requirements for social media companies. Instead, enforcement primarily relies on voluntary compliance by platforms, which may result in inconsistent or inadequate protection. Moreover, KOSA introduces a strong platform accountability framework by holding digital service providers responsible for implementing child safety measures, ensuring transparency in their policies, and demonstrating compliance with safety standards. This places a legal obligation on companies to prioritize child protection rather than merely offering optional safety features. In contrast, Philippine laws do not impose similar accountability measures on online platforms, leaving child safety largely unregulated in the digital space. The absence of clear liability for tech companies means that violations often go unchecked, and there are limited legal consequences for platforms that fail to protect children online. This regulatory gap underscores the urgent need for policies that mandate corporate responsibility in ensuring a safer online environment for minors.

Another significant provision of KOSA is the requirement for age-appropriate design, ensuring that platforms consider the developmental needs and vulnerabilities of children when designing their services. This includes features such as restricted notifications, reduced addictive design elements, and stronger privacy settings by default.

Philippine laws currently lack equivalent regulations, thus, children in the country may access platforms that are not designed with their safety in mind.

Without an age-appropriate design framework, young users may be exposed to content, interactions, and addictive digital features that may negatively impact their well-being. Implementing similar guidelines in the Philippines can help mitigate these risks and promote healthier online experiences for children.

Additionally, KOSA mandates that platforms provide parental control tools and clear information on how to protect children online. This ensures that parents and guardians have access to user-friendly safety settings that allow them to monitor and manage their children's digital activities. While some platforms operating in the Philippines offer similar parental control tools, there is no legal requirement for them to do so. This lack of regulation makes parental supervision more challenging, particularly for families who may not be familiar with digital safety measures. Establishing a legal mandate for parental control mechanisms can help bridge this gap and empower guardians to actively safeguard their children's online experiences. Both KOSA and Philippine laws contain provisions related to child data privacy, but enforcement in the Philippines remains inconsistent and unclear. The Data Privacy Act of 2012 (RA No. 10173) provides general protections for personal data, but it lacks explicit child-specific provisions aside from the National Privacy Commission's (NPC) Advisory on Child Transparency.

This advisory, however, does not carry the same legal weight as KOSA's robust data protection framework, which strictly limits the collection, processing, and retention of minors' personal information. Without stronger child-specific data privacy laws, Filipino children remain vulnerable to data exploitation, targeted advertising, and unauthorized profiling by online platforms.

Overall, while the United States has implemented a robust regulatory framework for child online protection through KOSA, the Philippines lacks specific, enforceable laws addressing these concerns. The absence of mandatory safety settings, risk assessments, content moderation requirements, and platform accountability leaves significant gaps in child online protection. As social media continues to play an increasingly influential role in children's lives, it is essential for the Philippine government to consider adopting similar legal safeguards. Implementing legislation modeled after KOSA will establish clear responsibilities for online platforms, enhance regulatory oversight, and create a safer digital environment for Filipino children. By prioritizing child welfare in the digital space, the Philippines can ensure that minors are protected from the evolving risks of social media while fostering responsible online engagement.

INCORPORATING BEST PRACTICES, SUCH AS THE "DUTY OF CARE" PRINCIPLE,

The duty of care principle is a fundamental legal concept that requires entities, including online platforms, to take reasonable and proactive measures to prevent foreseeable harm. In the context of child online safety, this principle imposes a legal obligation on digital service providers to protect minors from harmful content, cyberbullying, online grooming, and privacy violations.

As former US President Biden emphasized, tech companies that have profited immensely from children's engagement must take collective responsibility in ensuring that minors are not exposed to harmful content that could impact their well-being. This underscores the need to shift the onus of responsibility from individual users and parents to the platforms that design and manage digital spaces, compelling them to implement robust safeguards to mitigate online risks.[188]

Based on the study, the Philippine laws failed to impose an obligation or the duty of care on social media platforms in protecting children in their online engagement. While existing laws, such as the Anti-Child Pornography Act (RA No. 9775) and the Anti-Online Sexual Abuse and Exploitation of Children (OSAEC) Act (RA No. 11930), provide general protections for minors online, they do not explicitly hold online platforms such as Facebook, Tiktok, or Instagram accountable for proactively mitigating online harms. To effectively incorporate best practices, such as the "duty of care" principle, into Philippine legislation and ensure that social media platforms protect children from harmful content, several steps can be undertaken. This regulatory gap leaves social media companies and digital service providers with minimal legal liability in preventing harm to minors, effectively allowing them to regulate themselves.

To bridge this gap, the Philippine legal framework must institutionalize the duty of care principle, compelling online platforms to assess, mitigate, and prevent digital risks through clear, enforceable standards. A legally mandated duty of care framework will require online platforms to:

1. Strengthen content moderation policies to proactively detect and remove harmful material, particularly those that exploit or endanger children.
2. Enhance age-verification systems to ensure that minors are not exposed to inappropriate content.
3. Implement parental control tools that allow guardians to monitor and regulate their children's online activities.
4. Ensure transparency in data collection and algorithmic decision-making to prevent the exploitation of children's personal information for targeted advertising or harmful content recommendations.

To institutionalize the duty of care principle, the Philippine government can pursue multiple legislative and regulatory strategies. One approach is to enact new legislation specifically designed to address child online safety as herein further discussed in this article or improve existing bill, such as Senate Bill 552 to explicitly impose liability on platforms that fail to implement adequate child protection measures. Additionally, government agencies such as the National Privacy Commission (NPC), Department of Information and Communications Technology (DICT), and Department of Justice (DOJ) can issue policy directives and guidelines that define the responsibilities of online platforms in safeguarding minors. A statutory or oversight body who has a

[188] Transcript: President Biden's 2023 State of the Union Address, https://www.voanews.com/a/transcript-president-biden-s-2023-state-of-the-union-address/6953032.html accessed on 26 February 2025.

primary responsibility to monitor compliance and to penalize the violators can be a stepping stone for the Philippines in ensuring online protection for the Filipino children.

Beyond legislation, courts can play a crucial role by interpreting existing laws to establish legal precedents that promote greater accountability among digital service providers. Through judicial rulings, the Philippine legal system can create binding interpretations of child protection laws that emphasize platform social responsibility, thereby strengthening enforcement and legal deterrence against non-compliant digital service providers.

A comprehensive regulatory framework for the duty of care principle must clearly define the following:

1. Scope of Application – Identifying which online platforms are covered under the law, ensuring that both local and international digital service providers comply
2. Compliance Measures – Mandating risk assessments, transparency in algorithmic content curation, and age-appropriate design standards that prioritize children's safety
3. Accountability and Oversight – Requiring regular reporting, third-party audits, and independent regulatory assessments to monitor compliance
4. User Empowerment – Ensuring platforms provide accessible safety tools, clear reporting mechanisms, and educational resources to help parents and children navigate online risks
5. Stakeholder Collaboration – Encouraging coordinated efforts between government agencies, tech companies, educators, child protection organizations, and civil society groups to develop adaptive and sustainable safety measures for children

While integrating a duty of care framework into Philippine law offers significant benefits for online child protection, its implementation presents several challenges. One major concern is balancing child safety with digital rights and freedom of expression—overly restrictive content moderation policies can raise censorship concerns and limit access to educational or socially beneficial content. Additionally, effective enforcement mechanisms must be established to ensure compliance, particularly in cases involving global digital platforms that operate beyond Philippine jurisdiction. International cooperation and cross-border enforcement mechanisms may be necessary to hold multinational tech companies accountable. Furthermore, continuous adaptation of regulations is essential, as emerging technologies—such as artificial intelligence, virtual reality, and evolving social media algorithms—introduce new risks that current policies may not fully address. Regular updates to legislation, continuous research, and engagement with child safety experts will be necessary to ensure that policies remain relevant and effective in an evolving digital landscape.

By adopting the duty of care principle, the Philippines can create a legal and regulatory environment that compels online platforms to take proactive steps in protecting children. This shift will not only enhance child safety and prevent online harm but also foster greater accountability among digital service

providers, ensuring that online spaces become safer, more transparent, and more suitable for young users.

The findings underscore the urgent and undeniable need to strengthen the Philippine legal framework for child online protection, as the current system remains inadequate in addressing the complex and evolving risks that children face in digital spaces.

There is a growing demand for use of big data and the rapid development of technologies for its collection and analysis. This accumulation implies that more data will be collected on children over their lifetime than ever before. In short, without broader and coherent ethical and legal frameworks for the governance of children's data, children are likely to suffer the consequences hardest and longest.[189] However, it should be noted that children are also likely to reap the greatest potential benefits that data analysis would give over their lifetime. This uncertainty between the potential harm and benefit that data collection and accumulation over the lifetime of a child should be assessed against Article 3 of the UNCRC, which provides that in all actions concerning children the best interest of the child shall be a primary consideration.

Primary amongst the various issues on the protection of children's privacy right is the issue on informed consent. Under various national and international legislative and regulatory frameworks, guardians or parents are responsible for providing parental consent for the collection of data from children under eighteen or the relevant age of majority. Various international regulatory frameworks have tried to address issues on informed consent. An example of such a framework is the Children's Online Privacy Protection Act (COPPA) and the European Union (EU) General Data Protection Regulation (GDPR).

Under COPPA, it is a requirement that commercial websites aimed at children under age 13, give parents notice about their data collection activities, obtain verifiable consent from parents prior to collection of data from children, provide parents with access to any information collected from children, and finally give parents the opportunity to discontinue further uses of data collected.[190] The GDPR, for its part, explicitly recognizes that children deserve specific protection of their personal data and introduces added rights and safeguards for children. It says that children merit specific protection regarding their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.[191]

In the Philippines, consent is one of the primary requirements for the lawful collection of data.[192] The DPA requires that the data subject has given his or her consent to the processing of personal information. Further, it ensures the right of the data subject to be informed whether personal information about him

[189] Berman, G. and Albright, K. (2017). Children and the Data Cycle: Rights and Ethics in a Big Data World, Innocenti Working Paper 2017-05, UNICEF Office of Research, Florence.
[190] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505.
[191] Recital 88 of Article 8 of the European Union – General Data Protection Regulation.
[192] Supra 15. Section 12(a) and Section 13 (a).

or her shall be, are being, or have been processed.[193] Under the DPA, consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or agent specifically authorized by the data subject to do so.[194] However, unlike its international counterparts, the DPA does not provide any other qualifications, requirements, or safeguards to ensure that informed consent is taken from children or minors. Several Advisory Opinions[195] issued by the National Privacy Council have emphasized on taking the consent of minor children through their parents or legal guardians, but none of them have explicitly stated any other safeguards or added requirements on the taking of consent from children or minors.

On the other side of the spectrum, recommendations have been raised to consider the evolving capacities of children as guaranteed by Article 5 of the UNCRC in obtaining informed consent. Article 5 introduces the idea that children should be able to exercise their rights as they acquire the competence to do so. State parties should take this right into account when establishing minimum ages on particular issues.[196] This is particularly true with regard to data privacy rights. Some adolescents aged 14-17, who are still considered children in many countries, are more capable in navigating and understanding the internet than their parents or legal guardian. The effect is that this class of children will be in a better position to weigh the opportunity and risks in providing consent.

The rapid growth of social media has exacerbated threats such as harmful content, cyberbullying, privacy violations, and online predation, yet existing laws lack a proactive approach to mitigating these dangers. Adopting the U.S. Kids Online Safety Act (KOSA) as a legislative model will fill these glaring legal gaps by establishing a duty-of-care framework, ensuring that social media platforms and online service providers take preventive rather than reactive measures to safeguard children. Unlike the Cybercrime Prevention Act and the Data Privacy Act which focus primarily on penalizing offenses and regulating data processing, KOSA mandates risk assessments, enforces child-centric safety tools, and integrates age-appropriate design features. Moreover, it introduces platform accountability, legally requiring tech companies to implement parental controls, default privacy settings for minors, and accessible reporting mechanisms—a stark contrast to the current lack of corporate responsibility in the Philippines.

Beyond enforcing stricter safety measures, KOSA also promotes transparency and oversight, compelling platforms to disclose risk assessments, content moderation policies, and algorithmic influences on minors—ensuring digital environments remain ethical and accountable. Most importantly, KOSA acknowledges the dynamic nature of online risks, providing a flexible framework for continuous adaptation and enforcement.

---

[193] Supra 15, Section 16.
[194] Supra 15, Section 3(a).
[195] National Privacy Commission Advisory Opinion Nos. 2020-046, No. 2019-020.
[196] Supra 10, Article 5.

In an era of rapid digital transformation, the Philippines must act decisively—not just to react to online harm but to prevent its occurence. By integrating US KOSA's principles into Philippine law, the government can bridge critical legal deficiencies, uphold children's rights, and enforce greater accountability on tech companies.

XI. SUMMARY

This article has underscored the urgent need for a stronger and more comprehensive legal framework in the Philippines to effectively protect children from the increasingly complex and evolving risks of the digital world. While existing laws reflect the country's commitment to child online safety, the analysis reveals significant gaps in platform accountability, enforcement mechanisms, and proactive safety measures. These limitations leave children vulnerable to online threats, such as harmful content, cyberbullying, grooming, and privacy breaches, highlighting the inadequacy of current legislation in addressing the full scope of digital risks.

A comparative analysis with the U.S. Kids Online Safety Act (KOSA) has illustrated how a proactive duty-of-care framework can bridge these legal gaps. KOSA's approach, which mandates risk assessments, child-centric platform design, and stronger corporate accountability, provides a compelling model for the Philippines to consider. However, adopting such a framework requires careful adaptation to the country's unique cultural, technological, and regulatory landscape to ensure its effectiveness and feasibility.

The findings emphasize the need for a multi-faceted approach to safeguarding Filipino children online. Strengthening child protection in the digital sphere necessitates increased investment in digital literacy programs, fostering a collaborative effort among the government, tech companies, educators, and civil society organizations, and ensuring that policies remain dynamic and responsive to emerging technologies and online threats.

By integrating stronger legal protections with proactive governance and education, the Philippines can create a safer, more accountable, and child-friendly digital environment that effectively addresses the ever-changing challenges of online safety.

XII. CONCLUSION

This article proposes enhanced protective measures for children online, particularly through legislative reform. To strengthen these recommendations, the author has examined the best practices from the United States and other foreign countries, particularly laws and policies that have successfully institutionalized commitments to child online protection.

The digital era has seamlessly integrated the internet into daily life, reshaping communication, access to information, and social interactions on a global scale. For children, this technological revolution offers vast educational and social opportunities. However, as discussed, it also exposes them to significant online risks, including cyberbullying, exploitation, and harmful content. As digital platforms transcend geographical boundaries, the challenges of child online protection have evolved beyond the capacity of individual states to regulate effectively.

Just as globalization spurred the development of international legal frameworks to address cross-border concerns, the borderless nature of the internet necessitates a collective and harmonized approach to safeguarding minors online. Ensuring a safe digital environment requires the active collaboration of governments, policymakers, technology companies, and international organizations. A crucial step toward this goal is the implementation of comprehensive legal measures, such as incorporating key principles from the U.S. Kids Online Safety Act (KOSA) into Philippine legislation.

The growing global recognition of children's digital rights underscores the urgency of establishing legal safeguards that prioritize their safety and well-being in online spaces. By aligning national regulations with international best practices, the Philippines can strengthen its legal framework, ensuring a proactive and responsive approach to child online protection while reinforcing its commitment to upholding children's rights in the digital age.

Limited similarities between Philippine laws and US KOSA

The comparative analysis between existing Philippine laws and the U.S. Kids Online Safety Act (KOSA) underscores fundamental differences in their approaches to protecting children online. While both frameworks share the objective of safeguarding minors from digital threats, Philippine legislation predominantly adopts a punitive stance, addressing online harms only after they have occurred.

Laws such as the Anti-Child Pornography Act (R.A. 9775), the Expanded Anti-Trafficking in Persons Act (R.A. 10364), and the Anti-Online Sexual Abuse and Exploitation of Children Act (R.A. 11930) focus on penalizing offenders, enhancing law enforcement capabilities, and providing legal remedies for victims. These provisions play a vital role in combatting online exploitation, but they lack preventive mechanisms that will compel digital platforms to actively reduce risks before harm takes place.

In contrast, KOSA takes a preventive, platform-centered approach, shifting responsibility from individual users and law enforcement to the online service providers that shape digital environments. The legislation mandates platforms to conduct regular risk assessments, implement age-appropriate safety settings, enhance content moderation mechanisms, and provide parental control tools. By requiring platforms to integrate child safety into their design and operations, KOSA ensures that online spaces are inherently safer rather than merely reactive to violations. Moreover, the law emphasizes transparency and accountability,

compelling platforms to disclose how their algorithms and recommendation systems may contribute to harmful experiences, thus allowing regulators and the public to scrutinize their practices.

Another critical gap in Philippine law is the absence of explicit obligations for social media companies and digital platforms to assess or mitigate the risks their services pose to children. While existing laws impose severe criminal penalties on perpetrators and offer protective mechanisms for child victims, they do not place a legal duty on tech companies to implement proactive safeguards. This regulatory deficiency shifts the burden of child protection onto law enforcement agencies, child welfare organizations, and parents, rather than the corporations that design, operate, and profit from these platforms. Without legal mandates holding online service providers accountable for child safety, digital risks remain largely unregulated, leaving children exposed to potential harm.

Given these significant disparities, it is evident that the Philippines must pursue substantial legislative reforms to establish a more effective, preventive framework for child online protection. Incorporating elements from KOSA, such as mandatory platform accountability measures, risk assessment requirements, default safety settings, and algorithmic transparency, would bridge the gaps in current Philippine regulations. By enacting laws that prioritize prevention over punishment, the government can ensure that digital platforms actively contribute to the protection of minors, creating a safer and more responsible online environment for Filipino children.

Important concepts and regulations in the US KOSA that cover developments in modern technology were not found in the existing Philippine Laws.

One of the most significant findings of this article is the lack of key provisions in Philippine laws that reflect modern technological advancements and the increasing complexity of digital risks. While existing legislation acknowledges online threats, it remains largely reactive, focusing on penalizing online crimes rather than proactively mitigating risks before harm occurs. This gap is particularly evident in areas such as social media algorithms, targeted advertising, and data profiling, which have become central to children's online experiences yet remain unchecked and unregulated under Philippine law.

To emphasize, the U.S. Kids Online Safety Act (KOSA) and other foreign laws introduced crucial regulations that address these evolving challenges by holding online platforms accountable for actively preventing harm. KOSA mandates that digital platforms:

1. To conduct regular risk assessments to identify potential harms to children, ensuring that companies take a data-driven approach to mitigating risks.
2. To implement age-appropriate design principles, requiring that platforms prioritize child-friendly features, such as limiting addictive engagement mechanisms and restricting inappropriate content.

3. To provide transparent reporting mechanisms, enabling regulators and parents to monitor the effectiveness of child protection policies and hold companies accountable for their digital safety measures.
4. To enforce default safety settings, ensuring that social media platforms automatically implement protective measures for minors, rather than shifting the responsibility onto parents or guardians to configure them manually.

The absence of these provisions in Philippine laws highlights a critical gap in the country's child protection framework. Without comprehensive risk assessment protocols, age-sensitive platform designs, and enforceable safety regulations, children remain vulnerable to digital exploitation, harmful content exposure, and privacy violations. Moreover, the lack of transparency and accountability in how online platforms operate makes it difficult for regulators and stakeholders to address emerging threats effectively.

To bridge this gap, Philippine lawmakers must consider adopting legal measures similar to those in KOSA. Incorporating mandatory platform accountability, algorithmic transparency, and proactive content moderation into Philippine legislation will significantly enhance the country's ability to protect children in the digital age. A legislative shift toward preventive, platform-centric regulations—rather than purely punitive measures—will align the Philippines with international best practices and ensure a safer online environment for Filipino children.

Principle that may be incorporated to the Senate Bill 552 or drafting a similar bill to ensure full protection and accountability from social media platform

To ensure comprehensive protection and platform accountability, the Philippines must integrate the duty-of-care principle into its legislative framework. This principle, as widely recognized in jurisdictions like the U.K. and the U.S., holds digital service providers accountable for preventing harm to users—particularly children—by requiring them to implement proactive safety measures. To underscore its importance, the duty-of-care principle can be incorporated into the proposed Senate bill on child online safety through the following measures:

1. Mandatory Risk Assessments for Platforms – Social media companies should be legally required to identify, assess, and mitigate risks associated with their services, particularly those that expose children to inappropriate content, addictive design patterns, and online predators.
2. Clear Accountability for Platform Design – Digital platforms must be held responsible for the effects of their algorithms, ensuring that harmful content is not deliberately promoted to young users for engagement-driven profit.
3. Parental Control and Age Verification Standards – Philippine law should mandate stronger parental control settings and age verification mechanisms to prevent children from accessing content that is inappropriate for their age group.

4. Regulatory Oversight and Penalties – Establishing a regulatory body tasked with monitoring compliance and enforcing penalties on platforms that fail to meet child protection standards will ensure accountability.

By incorporating these elements, the Philippines can move beyond a reactive approach and adopt a preventive, child-centered legal framework that aligns with international best practices. This will ensure that digital platforms take an active role in addressing online harm and upholding their responsibility to protect young users.

Shared Accountability: Balancing the Responsibilities of Parents, Social Media Platforms, and the Government

While the primary objective of Senate Bill No. 552 is to mandate social media platforms to uphold a duty of care for children online, it is imperative to emphasize that child online safety is a shared responsibility. Parents and guardians remain the first line of defense in protecting children from digital harm. They are entrusted with the crucial role of supervising their children's online behavior, guiding their digital habits, and reinforcing moral and psychological resilience. However, the introduction of stronger legal mandates for platforms should not be interpreted as diminishing parental responsibility. Instead, the law should reinforce the role of parents as active digital stewards, working in tandem with platforms and the government. The provisions of the bill must make it clear that no provision should be used by parents as a shield for negligence, nor should it be abused to evade their duty to monitor and guide their children's online engagement. Legal safeguards must include educational programs for parents, facilitated by government agencies and accredited digital platforms, to empower them with tools and strategies for digital parenting in an evolving tech landscape.

At the same time, the government plays a pivotal role in institutionalizing mechanisms that facilitate collaboration among all stakeholders. It must provide adequate funding, enforce compliance, and establish oversight bodies to ensure long-term policy coherence. By distributing responsibility among parents, platforms, and the state, the legislative framework ensures that no single party bears the burden alone, fostering a holistic, multi-sectoral response to child online protection.

XIII. RECOMMENDATIONS

To strengthen Senate Bill No. 552 in effectively protect Filipino children in the digital landscape, the author proposes several amendments or an improved bill incorporating key principles from the U.S. Kids Online Safety Act (KOSA) and the U.K. Online Safety Act, along with the adoption of international best practices on online safety and data privacy.

Mandating a Duty-of-Care Framework for Social Media Platforms

To ensure greater accountability from online platforms, the Philippines should explicitly require social media companies to take proactive steps in preventing online harm to children. This can be achieved by amending existing laws or integrating duty-of-care provisions into Senate Bill No. 552 or a proposed bill, which should include:

5.1.1.1 Mandatory Risk Assessments – Platforms should be required to conduct regular risk assessments to evaluate how their design, algorithms, and content recommendations impact children.

5.1.1.2 Obligations for Harm Prevention – Online platforms should have a legal obligation to address exposure to harmful content (e.g., violent, sexually explicit, or self-harm-related material).

5.1.1.3 Transparency and Reporting Requirements – Platforms should be required to publicly report their child safety efforts, risk assessments, and mitigation strategies.

Strengthening Parental Control and Age-Appropriate Design Standards

Current Philippine laws do not mandate social media platforms to implement strong parental control features or age-appropriate settings by default. To align with KOSA and international best practices, the proposed bill should introduce:

5.1.2.1 Stronger Age Verification Mechanisms – Require platforms to verify the age of users using secure, privacy-respecting methods to prevent underage access to harmful content.

5.1.2.2 Default Safety Settings for Minors – Platforms must automatically set accounts of minors to the highest privacy and safety levels upon registration.

5.1.2.3 Enhanced Parental Controls – Require platforms to provide easy-to-use parental controls that allow guardians to manage their child's screen time, content exposure, and interactions.

Establishing a Regulatory Oversight Body for Online Child Safety

To ensure the effective enforcement of child online protection laws, the Philippine government should establish a dedicated regulatory body tasked with overseeing the implementation of online safety regulations. As outlined in Senate Bill No. 552, the Child Internet Safety Council (CISC) will serve as the primary statutory body responsible for safeguarding Filipino children in the digital space. CISC, which will operate under the Department of Social Welfare and Development (DSWD), shall be led by an Undersecretary and composed of designated representatives from key government agencies and relevant organizations, including:

1. Department of Education (DepEd) – To ensure that digital literacy and online safety education are integrated into school curricula and that educational institutions play an active role in protecting children online.
2. Department of the Interior and Local Government (DILG) – To facilitate coordination with local government units (LGUs) and ensure that grassroots initiatives support the Council's objectives.

3. Council for the Welfare of Children (CWC) – To provide expertise on child protection policies and ensure that the best interests of children remain at the forefront of legislative efforts.
4. Commission on Information and Communications Technology (CICT) – To provide technical expertise on information and communications technology, ensuring that internet filtering, parental controls, and other technical solutions are effectively implemented.
5. National Youth Commission (NYC) – To advocate for the interests and safety of Filipino youth, ensuring their voices are included in the policy-making process.
6. National Telecommunications Commission (NTC) – To monitor and regulate telecommunications providers and internet service providers (ISPs) to ensure compliance with child protection standards.
7. Philippine Information Agency (PIA) – To develop and implement public awareness campaigns on safe internet practices and online risks.
8. Non-Government Organizations (NGOs) Concerned with the Welfare of Children – To provide insights from civil society and ensure that community-based perspectives are considered in policy development.

To ensure a more comprehensive and multidisciplinary approach to online child safety, the author proposes additional agencies that can contribute specialized expertise and resources in the Child Internet Safety Council to effectively protect Filipino children in the digital environment. Expanding the CISC's membership will strengthen its ability to address the diverse threats that children face online and ensure that all aspects of child protection—legal, technological, educational, and psychological—are adequately addressed.

In addition to the agencies already listed under Senate Bill No. 552, the following agencies should be included:

1. Department of Justice (DOJ) – The DOJ plays a critical role in enforcing laws and prosecuting violations related to online exploitation, cybercrimes, and child abuse. Including the DOJ in the CISC will ensure that the legal framework remains updated and that offenders are swiftly brought to justice. It will be tasked to Lead the investigation and prosecution of online offenses involving children, as well as assist in the formulation of policies and regulations on child internet protection.
2. National Bureau of Investigation (NBI) – Cybercrime Division, which is tasked with investigating cyber-related offenses, including online child exploitation, and cyberbullying. Its expertise in forensic investigation and cybercrime detection makes it a crucial partner in ensuring compliance with online safety laws. It may also conduct digital forensics and investigations to track down perpetrators of online abuse; ollaborate with law enforcement agencies to dismantle child exploitation networks; and provide intelligence reports on emerging online threats affecting children.

The Child Internet Safety Council (CISC) shall play a pivotal role in ensuring the effective implementation of child internet protection laws by performing a wide range of functions aimed at safeguarding Filipino children in the digital space. It shall oversee and ensure the implementation of relevant regulations, advise the President on matters relating to child internet protection, and assist concerned agencies in reviewing and redrafting existing policies or formulating new ones aligned with the objectives of the Act.

CISC shall identify and determine internet materials that are harmful to children, approve appropriate internet filtering software to limit children's access to unauthorized websites, and restrict access to harmful online content. It will also conduct regular inspections of commercial establishments and public internet points offering internet services, either through its deputized representatives or by initiating random inspections, to monitor compliance with established standards and make necessary recommendations to appropriate agencies.

Additionally, CISC shall deputize local government agencies and law enforcement agents to assist in discharging its duties and functions, ensuring that enforcement efforts extend to the community level. Moreover, the Council shall develop and enforce mechanisms to engage parents, parent-school associations, and children in research and policy development, fostering a participatory approach to child online safety.

CISC will coordinate with other government agencies and private sector organizations to ensure effective implementation and will perform any other functions necessary to achieve the objectives of the Act. To strengthen its regulatory capacity, CISC shall also monitor compliance with safety regulations by conducting regular audits of social media platforms, impose penalties for non-compliance by establishing clear consequences such as fines, temporary suspensions, or stricter regulatory interventions, and develop public awareness campaigns to promote digital literacy and educate parents, educators, and children on safe online practices.

Imposing Stricter Regulations on Algorithmic Targeting of Children

Many platforms use algorithms that expose children to harmful content or exploit their attention for engagement-driven profit. To address this, amendments to Senate Bill No. 552 should include:

5.1.4.1 Restrictions on Harmful Algorithmic Amplification – Social media companies must prevent algorithms from actively promoting harmful or addictive content to minors.

5.1.4.2 Limitations on Data Collection from Minors – Prohibit platforms from profiling children for targeted advertising or engagement-based content manipulation.

5.1.4.3 User-Friendly Opt-Out Options – Require platforms to offer simple settings allowing minors or their guardians to disable algorithmic recommendations

Expanding Online Safety Measures in Schools and Public Institutions

To complement legal reforms, the government should invest in digital literacy and online safety education by integrating a comprehensive and multi-stakeholder approach to protect children online. Implementing these measures will ensure that Filipino children, parents, educators, and law enforcement personnel are equipped with the knowledge and skills needed to navigate the digital world safely.

5.1.5.1 Integrating Digital Safety Education into School Curricula –

Schools should incorporate digital safety education into existing curricula to teach children responsible social media use, privacy awareness, and the recognition of online threats. The Philippines

can take inspiration from the U.K.'s Digital Literacy Curriculum, which mandates that schools teach children about internet safety, cyberbullying, and data protection from an early age.

Additionally, the Australian eSafety Commissioner's program provides age-appropriate digital literacy modules that equip students with practical skills to navigate social media responsibly. The Philippines should develop a structured curriculum that includes lessons on identifying inappropriate content, protecting personal information, and understanding the consequences of online behavior. These lessons should be mandatory at all levels of education to ensure a progressive and age-appropriate approach to digital safety.

In line with Senate Bill No. 2934[197] or the proposed Internet Safety Protection Act introduced by Senate President Pro Tempore Jinggoy Ejercito Estrada, the Philippines should institutionalize internet and social media safety education in both elementary and high school levels.

This measure seeks to proactively equip children with essential knowledge and skills to navigate the digital world responsibly. It emphasizes education on safe online behavior, cyberbullying, data privacy, identification of fake news, and protection against online predators. The Department of Education (DepEd), as mandated in the bill, should develop and implement this program using multimedia applications and lesson plans, as well as provide professional training for educators and launch public awareness campaigns. This legislation complements existing protective laws such as the Anti-OSAEC and CSAEM Act by providing a preventive and empowering educational framework for Filipino students.

5.1.5.2 Training Educators and Law Enforcement on Digital Protection – Teachers, parents, and law enforcement officers should receive regular training on the latest developments in digital protection and online risks. Drawing from the U.S. Federal Trade Commission's (FTC) "Net Cetera" campaign, which trains educators to guide students in making smart online choices, the Philippines can create a similar nationwide initiative. Likewise, it empowers educators and parents with resources and strategies to address emerging online threats. Training sessions should focus on recognizing signs of cyberbullying, grooming, and exploitation, as well as implementing interventions to protect children from harm. Law enforcement officers should be trained in handling cases of online child exploitation and digital forensics to effectively investigate and prosecute offenders.

[197] An Act Establishing a Safety Internet Education Program in the Curriculum of All Elementary and Secondary Schools, 22 January 2025 by Estrada, Jinggoy E.

5.1.5.3 Public-Private Partnerships for Child Online Protection –The Philippines should encourage collaboration between government agencies, social media platforms, and civil society organizations to implement child safety initiatives. Australia's eSafety Office has demonstrated the effectiveness of public-private partnerships in identifying and removing harmful content online. Similarly, it leverages artificial intelligence to identify and remove child sexual abuse materials from the internet. The Philippines can establish partnerships with tech companies, NGOs, and digital platforms to promote the responsible use of technology and enhance reporting mechanisms for harmful content. These partnerships can also support the development of online safety tools, such as content moderation technologies, age-verification systems, and reporting hotlines that empower children and their guardians to report abusive content.

Implementing Online Safety Certification Programs for Schools

To reinforce accountability, the Philippines can introduce Online Safety Certification Programs similar to the "Safer Internet Day Charter" implemented in the European Union. This certification program will require schools to meet certain online safety standards, such as establishing reporting mechanisms, integrating digital literacy education, and training educators. Certified schools will be recognized for their commitment to providing a safe online environment for students. By adopting these international best practices, the Philippines can create a holistic and sustainable framework for protecting children online, ensuring that every stakeholder—schools, educators, parents, law enforcement, and the private sector—actively contributes to a safer digital environment for Filipino children.

Implementing Stricter Penalties for Non-Compliance

To enhance the protection of children in the digital space, it is recommended that the Philippines adopt a legal framework that clearly imposes liability on social media platforms, modeled after international best practices such as the U.S. Kids Online Safety Act (KOSA) and other related laws. Platforms must be held directly responsible for the safety of their young users, particularly when they fail to implement preventive measures against online harms:

5.1.5.4 Substantial Fines and/or Penalties – Platforms found non-compliant with duty-of-care obligations should face significant financial penalties. For instance, under the United Kingdom's Online Safety Act, non-compliance can result in fines of up to 10% of the platform's global annual revenue.[198] A similar approach should be adopted in the Philippines to ensure platforms prioritize child protection. Drawing from U.S. practices under the Federal Trade Commission (FTC) Act, civil penalties

[198] Social Media Platform faces huge fines under UK's New Digital Safety Laws (2023). Available at: https://www.theguardian.com/media/2025/mar/17/social-media-companies-fines-uk-illegal-content-online-safety-act#:~:text=Companies%20that%20breach%20the%20act,can%20also%20be%20taken%20down. (Accessed on March 15, 2025)

can be imposed for non-compliance. In the U.S., the FTC may impose monetary fines of up to $50,120 per violation per day. A Philippine version can impose administrative fines ranging from ₱500,000 to ₱5,000,000 per violation, depending on the severity and extent of non-compliance. These penalties should be regularly updated to reflect inflation and the growth of digital markets.

5.1.5.5 Temporary or Permanent Platform Suspension – Platforms that consistently fail to address violations may face temporary suspension of their services within the Philippines, similar to penalties under Australia's Online Safety Act 2021, which grants the eSafety Commissioner the authority to block non-compliant platforms.

5.1.5.6 Individual Liability for Senior Executives – Inspired by the UK's Online Safety Act, senior executives of non-compliant platforms should be held personally accountable, with potential penalties such as imprisonment or substantial fines for failure to protect children from online harm.

5.1.5.7 Compensation for Victims – Victims of online exploitation or harm should be entitled to compensation from non-compliant platforms, ensuring that children and their families receive appropriate redress.

5.1.5.8 Criminal Penalties for Gross Negligence – In extreme cases where gross negligence results in significant harm to minors, criminal liability should be considered. Executives or responsible individuals may face imprisonment if it can be proven that their willful or reckless disregard of child safety obligations caused substantial harm. However, criminal penalties should be reserved for the most serious and egregious violations to maintain fairness and proportionality.

As the digital landscape continues to evolve, so too must the legal framework governing online child protection in the Philippines. The rapid advancement of technology and the widespread use of social media have created an urgent need for stronger, more comprehensive legislation that ensures the safety and well-being of children in the digital space. While existing Philippine laws such as the Anti-Child Pornography Act (R.A. 9775), the Cybercrime Prevention Act (R.A. 10175), and the Anti-Online Sexual Abuse and Exploitation of Children Act (R.A. 11930) provide a foundation for safeguarding children online, they remain fragmented, reactive, and insufficient in addressing the emerging risks posed by modern social media platforms. These laws focus largely on penalizing offenses rather than preventing harm before it occurs, leaving significant gaps in the protection of children online.

One of the major weaknesses of the current legal framework is the lack of a cohesive and proactive approach to online child safety. Unlike the United States's Kids Online Safety Act (KOSA), which imposes clear obligations on social media

platforms to conduct risk assessments, implement safety features, and provide parental control mechanisms, Philippine laws do not place explicit responsibility on online platforms to mitigate risks associated with their services. This gap in regulation means that children remain vulnerable to harmful content, online exploitation, and privacy violations, as social media companies are not legally required to implement child-specific safety measures. To bridge these gaps, it is crucial for lawmakers to consolidate existing child online protection laws under a comprehensive and cohesive legal framework. One potential avenue for achieving this is through the passage of Senate Bill No. 552, which seeks to strengthen online child protection by establishing clearer regulations for social media platforms, promoting digital literacy, and enhancing parental and governmental oversight. However, to maximize its effectiveness, the bill must be strengthened with international best practices such as those found in KOSA.

Ensuring legislative adaptability by periodically reviewing and updating child online safety laws will allow the Philippines to keep pace with evolving digital threats and technological advancements. The fast-changing nature of the internet requires a legal framework that is flexible and responsive to emerging risks, ensuring that protections remain relevant and effective over time.

To achieve this, the government must establish a dedicated regulatory body responsible for overseeing online child protection, conducting research on emerging digital threats, and recommending legislative updates based on new developments in technology and online behavior. Another key aspect of strengthening the country's child online protection laws is fostering collaboration among various stakeholders. Government agencies, educational institutions, civil society organizations, and technology companies must work together to implement effective safety measures and promote digital literacy among children, parents, and educators.

Public awareness campaigns and educational programs can empower families to take an active role in protecting children online, while industry partnerships can encourage social media companies to adopt best practices voluntarily, even before legal mandates are in place.

Passing Senate Bill No. 552 or similar bill with the recommended enhancements—including a duty-of-care framework, stronger platform accountability measures, and proactive risk prevention strategies—will serve as a significant step toward creating a safer digital environment for Filipino children. However, enforcement will be key to ensuring the effectiveness of these legal reforms. The government must allocate sufficient resources to regulatory agencies tasked with monitoring compliance, investigating violations, and imposing penalties on platforms that fail to meet their obligations. Furthermore, mechanisms for reporting and addressing online harms must be streamlined to ensure that children and their guardians can seek assistance quickly and effectively.

By integrating these reforms, the Philippines can shift from a reactive to a preventive approach, ensuring that children are protected from online exploitation, harmful content, and data privacy risks. This shift is essential in

building a digital ecosystem that prioritizes child safety without stifling technological innovation or digital freedoms. A balanced approach that upholds both protection and accessibility will enable children to navigate the online world safely while enjoying the benefits of digital connectivity and education.

Ultimately, modernizing the legal framework through these reforms will not only strengthen child protection but also foster a culture of accountability among social media platforms. By holding companies responsible for the safety of their youngest users, the Philippines can ensure that the digital space remains a safe and empowering environment for future generations.

The passage of stronger online child protection laws will signal the country's commitment to safeguarding its youth in the digital age, setting a precedent for responsible internet governance and reinforcing the Philippines' role in the global effort to create a safer online environment for children.

REFERENCES

Books and Published Journals

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Aguiling-Pangalangan, E., & Cordon, F. J. J. (2017). Comparative children's rights in the ASEAN. UP Law Center.

Alder, S. (2024, August 1). Children's online privacy legislation overwhelmingly passed by Senate. The HIPAA Journal. Retrieved October 15, 2024, from https://www.hipaajournal.com/coppa-2-0-kosa-passed-senate/

Anderson, M., & Jiang, J. (2018). *Teens, Social Media & Technology 2018*. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/

Anti-Money Laundering Council. (2020). Child pornography in the Philippines: Post-2019 study using STR data. Retrieved October 16, 2024, from http://www.amlc.gov.ph/images/PDFs/2020%20DEC%20CHILD%20PORNOGRAPHY%20IN%20THE%20PHILIPPINES%20POST-2019%20STUDY%20USING%20STR%20DATA.pdf

Archard, D. (2020). *Children: Rights and childhood* (3rd ed.). Routledge.

Jain, S. (2025, January 9). 160 cybersecurity statistics 2025. Astra Security. https://www.getastra.com/blog/security-audit/cyber-security-statistics/ Accessed on 17 March 2025.

Berlin, I. (1958). *Two concepts of liberty*. Clarendon Press.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Brighouse, H. (2002). School choice and social justice. Oxford University Press.

Cantwell, S. (n.d.). S.1409 - 118th Congress (2023-2024): Kids Online Safety Act | Congress.gov | Library of Congress. Retrieved October 15, 2024, from https://www.congress.gov/bill/118th-congress/senate-bill/1409

Christians, C. G., Fackler, M., Richardson, K. B., Kreshel, P. J., & Woods, R. H. (2009). Media ethics: Cases and moral reasoning. Pearson Education.

Coquia, J. R. (2012). Human rights. Central Book Supply Inc.

Crowe-Clay, R. (2022). Transformative teaching around the world: Stories of cultural impact, technology integration, and innovative pedagogy (C. J. Bonk & M. Zhu, Eds.). Routledge.

Elkind, D. (1982). *The hurried child: Growing up too fast too soon*. Addison-Wesley.

European Parliament. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj Access on 17 March 2025

Falch-Eriksen, A. (2018). Human rights in child protection: Implications for professional practice and policy. Springer. https://doi.org/10.1007/978-3-319-94800-3

Falch-Eriksen, A., & Toros, K. (Eds.). (2021). *Professional practice in child protection and the child's right to participate.* Routledge.

Feinberg, J. (1980). The child's right to an open future. In W. Aiken & H. LaFollette (Eds.), Whose child? Children's rights, parental authority, and state power (pp. 124–153). Rowman & Littlefield.

Ferri, F., Grifoni, P., & Guzzo, T. (2012). New forms of social and professional digital relationships: The case of Facebook. Future Internet, 4(1), 1-14. https://doi.org/10.3390/fi4010001

Gillespie, T. (2018). Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.

Gillespie, T. (2023). Regulating Social Media: The Role of U.S. Law in Global Internet Governance. Oxford University Press.

Gordon, A. M., & Browne, K. W. (2017). Beginnings & beyond: Foundations in early childhood education (10th ed.). Cengage Learning.

Holloway, D., Green, L., & Livingstone, S. (2020). EU Kids Online 2020: Survey results from 19 countries. LSE, London: EU Kids Online. https://doi.org/10.21953/lse.47fdeqj01ofo

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. Business Horizons, 53(1), 59-68. https://doi.org/10.1016/j.bushor.2009.09.003

Kant, I. (1997). Groundwork of the metaphysics of morals (M. Gregor, Ed. & Trans.). Cambridge University Press. (Original work published 1785)

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harassment and bullying online. Journal of Child Psychology and Psychiatry, 55, 611-627. https://doi.org/10.1111/jcpp.12054

Livingstone, S., Stoilova, M., & Nandagiri, R. (2017). Children's data and privacy online: Growing up in a digital age. London School of Economics and Political Science. https://doi.org/10.2139/ssrn.2927660

Livingstone, S., & Stoilova, M. (2021). The 4 Cs: Classifying online risk to children. Communications, Culture and Critique, 14(3), 326-346. https://doi.org/10.1093/ccc/tcab019

MacMullen, I. (2015). Faith in schools? Autonomy, citizenship, and religious education in the liberal state. Princeton University Press.

McQuiggan, S., Kosturko, L., McQuiggan, J., & Sabourin, J. (2015). A handbook for developers, educators, and learners. John Wiley & Sons, Inc.

Meade, A. (2024, May 7). *What if Australia were to ban social media altogether?* ABC News. https://www.abc.net.au/news/2024-05-07/what-if-australia-were-to-ban-social-media-altogether/103809062

Mintz, S. (2004). Huck's raft: A history of American childhood. Belknap Press.

Saini, N., & Mir, S. (2023, August). Social media: Usage and the impact on education. Journal of Namibian Studies. https://doi.org/10.59670/jns.v33i.4041

Senate Economic Planning Office. (2022, December). COVID-19 school closures: Lessons from disrupted learning. https://legacy.senate.gov.ph/publications/SEPO/SEPO%20Policy%20Brief_School%20Closure_final.pdf

Siebert, F. S., Peterson, T., & Schramm, W. (1956). Four theories of the press: The authoritarian, libertarian, social responsibility, and Soviet communist concepts of what the press should be and do. University of Illinois Press.

Sundar, S. S. (2023). Media Effects: Advances in Theory and Research. Routledge.

Plunkett, L. A. (2019). Sharenthood: Why we should think before we talk about our kids online. The MIT Press. https://doi.org/10.7551/mitpress/11756.001.0001

Twenge, J. M., Martin, G. N., & Spitzberg, B. H. (2019). Trends in U.S. adolescents' media use, 1976–2016: The rise of digital media, the decline of TV, and the (near) demise of print. Psychology of Popular Media Culture. American Psychological Association.

Wright, A. (2022). Understanding the U.S. Kids Online Safety Act (KOSA) and its implications. Journal of Online Safety & Child Protection, 10(2), 45-67.

Wright, M. (2022). Accountability in the digital age: The Kids Online Safety Act. Journal of Cyber Law, 20(1), 23-37.

Zhang, W., & Livingstone, S. (2019). Balancing opportunities and risks in children's digital lives. International Journal of Communication, 13, 2308-2332.

International Documents

United Nations. (1989). Convention on the Rights of the Child. United Nations Treaty Series, 1577, 3-178. https://treaties.un.org/doc/Treaties/1990/09/19900902%2003-14%20AM/Ch_IV_11p.pdf

UNICEF. (2021). Digital connectivity and the protection of children's rights: Challenges and opportunities. United Nations Children's Fund. https://www.unicef.org/reports/digital-connectivity-children

News & Reports

BBC. (2025). *Australia to Ban Social Media for Children Under 16 in World-First Move.* Retrieved from https://www.bbc.com Accessed on 13 March 2025

GMA Public Affairs. (2023, October 20). Bata, aksidenteng naka-order ng 60 packages sa isang e-commerce shop! | Dapat Alam Mo! [Video]. YouTube. https://www.youtube.com/watch?v=ozBQj6I9XmM

History Tools. (n.d.). The complete guide to ARPANET: The groundbreaking computer network that led to the internet. Retrieved October 19, 2024, from https://www.historytools.org/concepts/arpanet-complete-guide#google_vignette

Hern, A. (2024, February 1). *Australia introduces world's toughest social media laws to protect children*. The Guardian. https://www.theguardian.com

Internet History of 1970s. (n.d.). Internet history | Computer History Museum. Retrieved October 19, 2024, from https://www.computerhistory.org/internethistory/1970s/

Taylor, J. (2024, January 26). *Australia's bold step on child protection: Social media ban for under-16s sparks global debate*. BBC News. https://www.bbc.com

ANNEX A

PROPOSED BILL:

The Filipino Child Online Safety and Empowerment Act

Section 1. *Title* - This Act shall be known as the "Filipino Child Online Safety and Empowerment Act."

Section 2. *Declaration of Policy* - It is the policy of the State to recognize the vital role of children in nation-building and to promote and protect their physical, moral, spiritual, intellectual, and social well-being. Pursuant to Article II, Section 13 and Article XV, Section 3(2) of the 1987 Constitution, the State shall ensure that Filipino children are equipped with the knowledge, skills, and tools to navigate the digital world safely and responsibly.

The State further acknowledges the growing influence of digital platforms in shaping the experiences and identities of children. In light of the risks posed by unregulated online environments—including exposure to harmful content, exploitation, algorithmic manipulation, and cyberbullying—this Act adopts a preventive, education-centered, and regulatory framework that promotes digital safety, platform accountability, and child empowerment.

Section 3. *Definition of Terms*:

1. Children - Any person below eighteen (18) years of age.
2. Digital Platform – Any website, application, or online service that collects, processes, or displays content and is accessible to minors.
3. Age-Appropriate Design – Design features, default settings, and functions tailored to the developmental needs and privacy rights of children.
4. Harmful Content – Content that includes, but is not limited to, sexual exploitation, self-harm, cyberbullying, misinformation, and age-inappropriate material.
5. Algorithmic Targeting – The automated delivery or recommendation of content to users based on behavioral data or inferred preferences.
6. Additional terms may be defined in the IRR.

Section 4. *Education and Curriculum Integration* - The Department of Education (DepEd), in coordination with the Department of Information and Communications Technology (DICT), shall develop and implement a mandatory Internet Safety Education Program at all levels of basic education, both in public and private schools. The curriculum shall include:

a. Responsible social media and internet use;
b. Online privacy, data protection, and personal information management;
c. Identification of online threats, including grooming, cyberbullying, and misinformation;
d. Strategies for safe digital engagement and well-being.

Teachers and school personnel shall be trained to deliver digital safety education effectively.

Section 5. *Shared Duties*

A. Online Platforms Accessible to Minors

All digital platforms with operations in or access to users in the Philippines shall:

a. Exercise a duty of care to minimize the risk of exposure to harmful content;
b. Implement age-appropriate design standards;
c. Provide tools for parental supervision and time management;
d. Ensure transparency in algorithmic content targeting for minors;
e. Allow minors and guardians to opt out of personalized content or tracking;
f. Enable accessible reporting mechanisms for abusive content.

B. Role and Responsibilities of Parents and Guardians - While online platforms are mandated to exercise a duty of care in protecting children, parents and legal guardians shall likewise share in the responsibility of ensuring the safe, informed, and balanced digital participation of their children.

Parents and guardians shall have the following responsibilities:

a. Actively engage in their children's digital lives by supervising online activity and guiding appropriate internet usage;
b. Utilize parental control tools and safety settings provided by digital platforms to monitor and limit exposure to harmful content;
c. Participate in digital safety education sessions organized by schools, LGUs, or the Child Internet Safety Council (CISC)
d. Encourage open communication and educate children on the risks of cyberbullying, grooming, oversharing of personal information, and engaging with strangers online;
e. Promote responsible digital citizenship by modeling appropriate online behavior and fostering a healthy balance between screen time and real-life activities.

The State, through the CISC and DepEd, shall support parents and guardians by providing educational materials, digital literacy campaigns, and access to digital safety tools and counseling resources.

Section 6. Creation of the Child Internet Safety Council (CISC)

A Child Internet Safety Council (CISC) is hereby created under the DICT. It shall consist of representatives from:

a. DICT
b. DepEd
c. Department of Justice (DOJ)
d. Council for the Welfare of Children (CWC)
e. Recognized child advocacy NGOs
f. Experts in digital rights and child psychology

Mandate of CISC:

a. Monitor compliance of platforms with safety standards;
b. Issue safety certifications and public advisories;
c. Recommend legislative and policy improvements;
d. Coordinate research and impact assessments on digital harms to children.

Section 7. *Public Education and Awareness* - The CISC and DepEd, in collaboration with local government units, shall conduct:

a. Parent and teacher training on child online safety;
b. Community-based digital literacy programs;
c. Annual observance of National Digital Safety Week for Children.

Section 8. *Platform Accountability and Sanctions*

a. Platforms that violate the mandatory safety provisions of this Act shall be subject to:
    - First offense: Fine of ₱500,000 to ₱1,000,000 per day of violation;
    - Second offense: ₱1,000,000 to ₱5,000,000, and temporary suspension of services;
    - Third offense: Blocking of the platform within Philippine jurisdiction, revocation of business permits, and penalties up to ₱10,000,000.

b. If violations result in actual harm to minors, civil damages and reputational sanctions may apply.
c. Willful or grossly negligent violations may incur criminal liability under existing child protection laws.

Section 9. *Transnational Limitations* - This Act shall primarily apply to activities within the Philippine jurisdiction. While it does not address transnational online crimes, such acts shall continue to be prosecuted under Republic Act No. 11930 and other applicable international cooperation treaties. This Act is preventive and educational in nature, and shall not be interpreted as superseding criminal frameworks for transnational offenses.

Section 10. *Funding* - The initial implementation shall be funded under the DICT and DepEd's current appropriations. Thereafter, such amounts as may be necessary shall be included in the annual General Appropriations Act (GAA).

Section 11. *Implementing Rules and Regulations* - The DICT, in coordination with DepEd, DOJ, and other stakeholders, shall promulgate the Implementing Rules and Regulations (IRR) within ninety (90) days from the effectivity of this Act.

Section 12. *Separability Clause* - If any provision of this Act is declared unconstitutional or invalid, the remainder shall remain in full force and effect.

Section 13. *Repealing Clause* - All laws, executive orders, rules, and regulations inconsistent with this Act are hereby repealed or amended accordingly.

Section 14. *Effectivity* - This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.