Eduvest – Journal of Universal Studies
Volume 4 Number 2, February, 2025
p- ISSN 2775-3735- e-ISSN 2775-3727

CHILDREN'S DIGITAL RIGHTS: AN IN-DEPTH ANALYSIS OF INDONESIA, EUROPE, AND THE US

Ridwan Tahir [1], Titie Yustisia Lestari[2]
Law Faculty, Tadulako University, Palu, Indonesia [1,2]
Email**:** titieyustisia@yahoo.com

ABSTRACT

The protection of children's digital privacy has become an increasingly critical issue in the modern digital age, as children are more connected to the internet than ever before. This study conducts a comparative analysis of child privacy protection frameworks in Indonesia, Europe, and the United States, focusing on legislative approaches, enforcement mechanisms, and parental in-volvement. While the General Data Protection Regulation (GDPR) in Europe provides a com-prehensive and flexible framework, the Children's Online Privacy Protection Act (COPPA) in the United States takes a more targeted approach, focusing on children under 13. Indonesia's Per-sonal Data Protection Law (PDP Law), still in development, offers potential but lacks specific child-focused provisions. Key findings highlight the strengths and weaknesses of these frame-works, particularly in age thresholds for consent, parental involvement mechanisms, and penal-ties for violations. This study underscores the need for Indonesia to harmonize its legal frame-work with international best practices by incorporating child-specific protections, fostering digital literacy, and strengthening enforcement mechanisms. By leveraging lessons from global stand-ards, Indonesia can ensure a safer and more empowering digital environment for its younger generation. The research provides actionable insights for policymakers, educators, and technol-ogy providers to collaboratively address the complexities of safeguarding children's digital privacy.

KEYWORDS *Child privacy, digital rights, personal data protection, online safety*

INTRODUCTION

In today's digital age, the protection of children's privacy online has become a paramount concern for governments, policymakers, and parents alike (Milkaite & Lievens, 2019). The rapid expansion of the internet and the proliferation of social media platforms have raised serious questions about how to safeguard the personal data of minors. This comparative analysis will examine the approaches taken by Indonesia, Europe, and the US in protecting child privacy online, shedding light on the different legal frameworks, regulations, and best practices in place to address

How to cite: Ridwan Tahir, et al. (2025). Children's Digital Rights: An In-depth Analysis of Indonesia, Europe, and the US. Journal Eduvest. 5(2): 1942-1964
E-ISSN: 2775-3727

this critical issue. By understanding the unique approaches and challenges faced by each region, we can gain valuable insights into the global landscape of child privacy protection and work towards creating a safer online environment for children worldwide (Adams et al., 2023)

The increasing number of young internet users worldwide, with one-third under the age of 18, highlights the growing importance of child privacy protection in the dig-ital age. As children spend more time online and start their digital lives at a younger age, it is crucial to address the potential risks and dangers they may face. These risks include invasions of privacy, data breaches, online harassment, and exposure to inappropriate content (Siyam & Hussain, 2021). Legislative Frameworks and Regulations Across In-donesia, Europe, and the US, child privacy protection is regulated by various legislative frameworks. For example, in Europe, both the European Union and the Council of Eu-rope guarantee the rights to privacy and data protection for children. The European Union has implemented the General Data Protection Regulation, which includes spe-cific provisions for the protection of children's personal data (Children and the Digital Environment, 2024).

Similarly, in the United States, child privacy protection is governed by the Chil-dren's Online Privacy Protection Act. This act sets requirements for websites and online services to obtain parental consent before collecting personal information from children under the age of 13.(Apthorpe et al., 2019) In Indonesia, child privacy protection is primarily addressed through the Constitution and various laws that protect against the misuse of personal data. For children raised in a digital world, their privacy is at risk due to the constant generation and collection of their personal data without their awareness or understanding. (Sofian et al., 2021)

Furthermore, the emergence of internet-connected toys and other smart gadgets not specifically designed for children's usage adds to the concerns surrounding child pri-vacy and data protection. Children's privacy on the internet can be improved through a combination of parental guidance and government regulations. In each region, there are different approaches to child privacy protection, but all efforts aim to create a safer online environment for children.(Apthorpe et al., 2019)

Child online privacy refers to the protection of a child's personal information and privacy rights while using the internet. This includes safeguarding their sensitive data such as their name, address, phone number, and any other personally identifiable in-formation from being collected, used, or shared without explicit consent. Furthermore, child online privacy also involves ensuring that children are not exposed to harmful content, online harassment, or any other risks that may compromise their safety and well-being while engaging in online activities. It is essential to establish robust mecha-nisms to obtain parental consent for the collection and processing of a child's personal data, as well as to provide parents

with the tools and resources to monitor and control their child's online interactions and activities. Additionally, educating children about the importance of safeguarding their personal information and promoting digital liter-acy skills to help them navigate the digital landscape safely are integral components of ensuring child online privacy.

Moreover, the development and enforcement of age-appropriate privacy settings and regulations for online platforms and services also play a critical role in protecting the privacy of children while they are online. Overall, the definition of child online privacy encompasses a comprehensive set of measures aimed at preserving the confi-dentiality, security, and integrity of a child's personal information and online experi-ence. In today's interconnected world, the protection of children's privacy online goes beyond geographical borders. It is crucial to recognize that the digital landscape is constantly evolving, and new technologies bring forth additional challenges in safe-guarding children's online privacy(Santer et al., 2023). As we delve deeper into this multifaceted issue, it becomes evident that while legislative frameworks and regula-tions provide a foundational structure for child privacy protection, there are intricacies and nuances that necessitate continual assessment and adaptation.

When examining the global landscape of child privacy protection, it is important to acknowledge that the online environment transcends national boundaries. As such, collaboration and information-sharing among countries are essential to address the complexities of safeguarding children's privacy effectively. Understanding the unique cultural, social, and technological contexts in different regions can inform the devel-opment of comprehensive strategies that resonate with the specific needs of diverse communities.

Moreover, beyond governmental regulations, fostering a culture of digital respon-sibility and empowerment among parents, educators, and technology providers is paramount. Empowering children to make informed decisions about their online in-teractions, while also equipping them with the skills to identify and respond to potential risks, is integral to promoting a safe and secure digital experience for the younger gen-eration.(Torres-Hernández & Arrufat, 2022)

Comparative analysis of child privacy protection in Indonesia, Europe, and the United States reveals the importance of addressing privacy risks and dangers faced by young internet users and implementing effective safeguards to protect their privacy and personal data. In today's digital age, where children spend more time online and start their digital lives at a younger age, it is crucial to address the potential risks and threats to their privacy. In conclusion, child privacy protection is a pressing issue that requires attention from legislators worldwide. Comparative analysis of child privacy protection in Indonesia, Europe, and the United States highlights the different legislative frame-works and measures implemented to

safeguard children's privacy on the internet. The findings emphasize the need for ongoing communication between parents and children regarding internet use, educating children about online threats and cybersecurity, and utilizing parental control software and antivirus programs to enhance child privacy and data protection.

The comparative analysis of child privacy protection in Indonesia, Europe, and the United States reveals the need for strong legislative frameworks and measures to safeguard children's privacy on the internet. The comparative analysis of child privacy protection in Indonesia, Europe, and the United States demonstrates that while there are varying approaches and legislative frameworks in each region, the goal remains the same: to protect children's privacy and personal data online. The comparative analysis also highlights the need for collaboration between regulatory bodies, researchers, and technology developers to ensure informed consent and privacy expectations of young internet users are considered. In this comparative analysis of child privacy protection on the internet in Indonesia, Europe, and the United States, it is evident that addressing privacy risks and implementing effective safeguards is crucial for creating a safer online environment for children.

RESEARCH METHOD

Our research focuses on analyzing child privacy protection in the digital age by comparing the approaches used in Indonesia, Europe, and the United States. Compar-ative analysis on legal research involves a thorough examination and comparison of the legislative frameworks, laws, and regulations related to a specific legal issue across different jurisdictions. (Banakar, 2009)In this case, the comparative analysis on child privacy protection in Indonesia, Europe, and the United States entails critically as-sessing the various laws and regulations enacted in each region to safeguard children's online privacy.

The expected outcome of the comparative analysis is to identify the similarities and differences in the legal frameworks governing child privacy protection in the three re-gions. It aims to highlight the strengths and weaknesses of each legislative approach, examine the effectiveness of existing safeguards, and explore any gaps or areas for im-provement. Ultimately, the comparative analysis seeks to provide valuable insights that can guide policymakers, legislators, and stakeholders in enhancing child privacy pro-tection on the internet.

We then employ a juridical-normative-comparative methodology to examine the legal frameworks and regulations pertaining to child privacy protection in Indonesia, Europe, and the United States. The focal point of our analysis resides in the legislative frameworks that regulate the privacy of children. We diligently collect and examine papers such as the General Data Protection Regulation (GDPR) in Europe and the Children's Online Privacy Protection Act (COPPA) in the United

States, in addition to Indonesian regulations. We analyze these legal regulations, enabling a detailed com-parison of age limitations for online consent, processes for parental consent, and the consequences for failing to comply. By conducting case studies, we construct a coherent account that not only emphasizes the differences but also uncovers the common objec-tive among these areas—to establish a more secure digital space for children. The re-search intends to not only analyze legislative frameworks but also provide practical in-sights and policy recommendations to strengthen worldwide child privacy protection.

RESULT AND DISCUSSION

Indonesia's Approach to Protecting Children's Online Privacy

Mobile phones and other smart phones are becoming increasingly popular among the general population, which is evidence that the growth of information technology has led to an increase in the number of items that are necessary for humans to have in their lives. Everything becomes more efficient because of technology. Through the availability of online learning, children can develop a stronger connection and engagement with digital technology, particularly regarding the utilization of telecommunications services, which are utilized as one of their learning tools. Nevertheless, children and teenagers are inadvertently ensnared in a perilous online environment. Simply because not all children are able to comprehend the digital world.

The children who are included in this article are under the age of 18 and are not married. This restriction applies to all children. There are several children and adolescents who have or have not been able to evaluate the utilization of telecommunications services that have the potential to have a beneficial impact on themselves. The digital world is a double-edged sword that has both beneficial and negative aspects, and this fact cannot be denied. One of the potentially negative things that takes place is the number of breaches that occur with personal data, which includes the personal data of minors who are under the age of 18.

As a result of a lack of public awareness of the subject of protecting personal data, topics pertaining to privacy have not been extensively investigated in Indonesia. This lack of knowledge is shared by both academic institutions and government bodies. Considering the large number of children, it is essential to investigate these concerns about parental privacy. (Suari & Sarjana, 2023)The use of communication services and social media platforms is an essential component of our everyday lives. Children are required to make use of communication services to obtain what they require, such as distant learning. Social media is necessary for satisfying entertainment demands when at home, as it allows users to view life outside their home through a variety of social media applications, which might result in the exposure of personal information without the user's awareness. It is for

this reason that it is essential to place an emphasis on the protection of personal data and the rights of individuals to privacy.

This right to privacy is also included in the Universal Declaration of Human Rights (UDHR), specifically in article 12, which states that "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation." This right to privacy comes from the Universal Declaration of Human Rights. (Prabhakaran et al., 2022)The protection of the law from such interference or attacks is a right that belongs to every single person. The Personal Data Protection Law (PDP Law), which is an important issue for assuring the protection of the privacy and personal data of the Indonesian people, also contains this statement. This law is a significant issue. According to Article 3 of the Personal Data Protection Law, there are two categories: general and specialized. Both categories are compared below. Considering this, those who possess personal data are obligated to protect its secrecy and make use of it in accordance with their requirements. Children may be unaware of certain sorts of personal data that are protected, such as particular categories of data comprising of children's data and general data such as children's names. This type of data is protected.(Sofian et al., 2021)

According to the Minister of Communication and Information, the Personal Data Protection Law (which will be referred to as the PDP Law from this point forward) includes several significant provisions concerning the authority for data rights and obligations. By doing so, if personal data is used in an inappropriate manner or arbitrarily, a variety of fraudulent activities can be identified and readily punished. It is the responsibility of the Personal Data Protection Bill to regulate the various categories of personal data, as well as the role of the government and the penal prohibitions that constrain it. Because of the function that the government plays and the rules of criminal law that bind it, the Personal Data Protection Law is responsible for regulating the many types of personal data already in existence. The protection of society in the face of challenges such as these, as outlined in our constitution in article 28 G paragraph (1) of the 1945 Constitution, ought to be the responsibility of the state according to the constitution.(Anand et al., 2020) This article addresses the human right to be protected against a variety of dangers, which is discussed in this article. The same thing may also be found in paragraph four of Article 28 H, which stipulates that the significance of personal rights must not be interfered with by any individual.

As a result of the fact that the government is also receiving assistance from the Ministry of Communication and Information (Kemenkominfo) in its efforts to fulfill the mandate of the constitution, it has been decided that the date of December 1, 2016, will be designated for the implementation of the Minister of Communication and Information Regulation Number 20 of 2016 concerning the

Protection of Personal Data in Electronic Systems (which will be referred to as the PDP Ministerial Regulation from this point forward). The need to protect individuals' privacy from the inappropriate use of their personal data is the driving force behind the implementation of government rules. What is meant by the term "privacy" in this context is the right of the individual who owns personal data to provide other users with access to such data. The reason for this is that if the data is published, whatever is revealed could put the owner of the personal data in danger of having their trust and security compromised.(Syailendra, 2021)

It has been widely acknowledged for a long time that the protection of personal data serves as the foundation for the preservation of individual privacy rights. The provision of protection for the right to privacy can be found in article 28G(1) of the Constitution issued in 1945.(Bentotahewa et al., 2022) In a nutshell, the right to privacy is a fundamental human right that must be safeguarded. Article 26 of the Electronic Information and Transactions Law is actually based on the declaration that is found in Article 28G(1) of the Constitution that was ratified in 1945. It is needed by law that the agreement of the data owner be obtained before any use of personal data in electronic media can take place. Therefore, under this scenario, operators of electronic systems that utilize or make use of personal information obtained from individuals are required to comply with the consent of the data owner.(Syailendra, 2021)

As a result of the fact that the PDP Law is regarded as being extremely vital for the purpose of safeguarding the rights of citizens, it was proposed in the year 2014. (5) [5] It is a statement of protection of privacy, human rights as outlined in Article 28G of the Constitution of 1945, and the entire community that the protection of personal data itself is a statement of protection. has voiced their support for the PDP Law and demanded that it be passed without unnecessary delay. To fulfill the requirements of society and to establish a transparent legal framework for the resolution of disagreements over personal data, the objective is to make certain that the PDP Law is enacted into law.(Sitompul, 2019)

Nevertheless, the Constitution and the rules of the Information and Electronic Transactions Law acknowledge that the scope of personal data that is to be safeguarded in practice must encompass and describe all that is controlled in connection to children's personal data that must be guaranteed. This is a requirement that must be met. The procedure of demonstrating legal claims for identity theft or releasing someone's personal information, particularly regarding children, is the most critical issue. In addition to that, the responsibilities that parents have in this area are important. Particularly if the child is still unable to comprehend the risks associated with the digital environment.(Sofian et al., 2021)

Until 2024, the existing legislation in Indonesia did not explicitly cover data protection, especially the protection of child data. Data protection is addressed

independently through different regulations appropriate to each industry, and there is currently no dedicated regulation for the protection of children's data. The absence of specific regulations has resulted in the inclusion of kid data protection within the purview of the Information and Electronic Transaction Law and the Child Protection Law. The necessity of implementing regulations for the protection of child data becomes apparent considering the ongoing government debates over a data protection law. Explicitly integrating kid data protection into this regulation is imperative, considering the legal ramifications of obtaining authorization for data usage. To ensure that children are recognized as independent legal entities in the digital domain and to protect their well-being, it is imperative to incorporate certain prerequisites such as obtaining parental approval, providing notice, granting permission, and verifying identity. The dangers of child exploitation in the digital era are multifaceted and can have substantial adverse effects on the physical and psychological well-being of children.(Sofian et al., 2021)

Given the ongoing government discussion on the Draft Law on the Protection of Personal Data, it is crucial to address and establish regulations specifically for safeguarding children's personal data within the broader framework of personal data protection. Ensuring the proper growth and development of children requires taking this crucial step to protect them from virtual risks like violence, abuse, and extortion in cyberspace. Indonesia currently does not have explicit legislative regulations to protect children's personal data, unlike many nations such as the European Union and the United States, which have dedicated legislation for this purpose.

Therefore, it is advisable for the Indonesian parliament and the President to promptly amend the Child Protection Act and/or the Electronic Transaction and Information Act to incorporate a specific section on safeguarding children's personal data. This should entail the imposition of criminal penalties, fines, and compensation for any unauthorized utilization of children's personal data. To promptly address the issue, it is advisable for the Ministry of Information and Communication and the Ministry of Women's Empowerment and Child Protection to work together in creating a Joint Ministerial Regulation. This regulation would serve the purpose of safeguarding children's personal information on the internet and enforcing legal penalties against those who violate these protections. Moreover, it is essential to provide education to both children and parents regarding the protection of their personal data to prevent any potential misuse. Child internet privacy protection in Indonesian legislation necessitates prompt attention and amendment, as stated by Agung (2020). It is imperative to acknowledge and confront the distinct challenges and hazards that youngsters encounter in the digital realm.

Child Privacy Protection in the European Framework

It is stated in Recital 38 of the Regulation that children require additional protection when it comes to the processing of their personal data. This is due to the fact that children may have a lower level of awareness about the risks, consequences, and safeguards that are involved, as well as their rights connected to the processing of personal data. This particular protection ought to be applicable, in particular, to the use of personal data of children for the purposes of marketing or establishing personality or user profiles, as well as the collecting of personal data pertaining to children while utilizing services that are supplied directly to a child. In Article 8 of the General Data Protection Regulation (GDPR), the lawmaker from the European Union addresses the aforementioned issue directly. In accordance with this regulation, the processing of personal data belonging to a child who has reached the age of 16 is permitted in the context of information society services that are provided directly to a kid. Only if and to the extent that the permission is granted or authorized by a person who exercises the parental authority over a child or acts as a child's custodian is such processing permissible if the child is under the age of sixteen. This is the only condition under which such processing is considered lawful.(Lievens & Verdoodt, 2017) Additionally, Article 40 instructs the drafters of codes of conduct to provide particular safeguards for the processing of personal data of children, with a focus on obtaining parental permission and verifying the legitimacy of such permission.

In the framework of preventative or counseling services that are provided directly to a child, it should not be necessary to obtain the consent of the person who holds the parental responsibility. It is permissible for member states to lower the age restriction in their legislation, provided that they adhere to the guideline that stipulates a minimum age of thirteen(Jasmontaite & Hert, 2014). On the other hand, due to the absence of or limitation on legal capacity, there are significant uncertainties over whether or not such consent or the option will be effective. It is possible that a data controller that offers a cross-border service may not always be able to rely on complying with the legislation of the Member State in which it has its main establishment. Instead, it may be necessary for the data controller to comply with the laws of each Member State in which he offers the information society services. In the double opt-in model, which involves obtaining the consent of a custodial parent or guardian by telephone, using traditional correspondence, or other authorization methods (registration, giving date of birth, etc.), the obligation to check whether the child consenting to the processing of data has the authority to do so or not is a logical consequence of the accountability principle. This obligation manifests itself in the double opt-in model. Only information society services, as defined by Article 1.1 (b) of Directive (EU) 2015/1535 of the European Parliament and of the Council on September 9, 2015, are referred to in the regulations that are

contained in Article 8. Art. 8 does not apply to all services provided by the information society; rather, it is only applicable to those services that are provided directly to minors.(Nouwens et al., 2020)

According to the available research, solely those services that are aimed directly or completely at children and are designed to pique their interest are considered to be those that are delivered directly to the child. When it comes to this particular scenario, the attitude of the service provider towards the relationship with children is more important than the theoretical feasibility of establishing a connection between the topic of the service and a child eight.(Abdullah et al., 2018) Because of the nature of the situation, it is not reasonable to anticipate that every service provider will make it clear on their websites that a particular service is intended just for adults. A requirement of this kind is only permissible in situations where it is mandated by law, such as when it comes to the sale of alcoholic beverages and tobacco products, gambling or betting-related services, or content that is inappropriate for children (such as that which contains vulgar language, nudity, or violent content). During the same time period, Art. will be applicable to services that are aimed at both adult users and youth users. The parents need to be made aware of the situation and given the opportunity to take the necessary precautions in order to avoid them from invading their children's privacy while they are online.(Santer et al., 2023)

One can find millions of images displaying children in uncomfortable positions or parents sharing stories about "funny" scenarios involving minors when browsing social networking sites. These photos feature youngsters in embarrassing settings. When editors asked a child, prior to publication, if he or she would like to become a social media hero of the day on the Internet, the child did not appear to have a complete comprehension of the decision that he or she was making. This indicated that the child was not fully aware of the implications of the decision. In spite of the fact that they are not familiar with the processes of social networking, children have a tendency to defend their privacy and interpersonal relationships in a very natural way. It is possible to draw the conclusion that many parents believe that they own their child's private and control it to the same extent that they manage their own privacy, and that the privacy of a child and that of his or her parent are of the same type. This is because the publication of a child's image by the parent on the Internet leads to making this assumption.(Berti & Fachin, 2021)

The legislator of the European Union is also attempting to address this issue by stating in Recital 65 of the Regulation that the right to have one's personal data erased, also known as the "right to be forgotten," is of utmost significance in situations where the data subject has given his or her consent as a child and is not fully aware of the risks involved in the processing of the data, and later wants to remove such personal data, particularly on the Internet. In the event that the

individual, who was a child at the time, did not consent to the processing of his personal data while the entity that indirectly provided the data to the data controller was his or her parent or legal guardian, it is possible to state that recital 65 will also apply in this scenario. This can be stated by using the minori ad maius as the rule of interpretation. With regard to all of the personal data that were given by a child's parents, the right to request the erasure of personal data is directly derived from Article 17.1(d) on account of the right to have data that has been unlawfully processed erased.(Sloot, 2024)

The United States' Policies on Internet Privacy for Minors

The advent of the internet has revolutionized the way we live, work, and interact with others. However, along with its numerous benefits, the internet also poses significant risks, especially for minors. One of the major concerns surrounding the internet is the issue of privacy, particularly when it comes to minors. Children, especially those under the age of 13, are particularly vulnerable to online privacy breaches and inappropriate content. (Hong et al., 2019)To address these concerns, the United States has implemented policies to protect the internet privacy of minors, primarily through the Children's Online Privacy Protection Act. The Children's Online Privacy Protection Act, enacted in 1998 by the Federal Trade Commission, is a federal law that aims to give parents control over the information collected from their children online. It requires website operators to obtain verifiable parental consent before collecting personal information from children under 13. Additionally, the law imposes specific requirements on how this information should be handled and protected.(Zostant & Chataut, 2023)

COPPA has played a crucial role in safeguarding the online privacy of minors by setting strict standards for website operators and online services directed towards children.(Kahimise & Shava, 2019) However, as technology continues to evolve, it is essential for policymakers to keep pace with the changing digital landscape to ensure continued protection for minors. In recent years, there have been debates and discussions about updating COPPA to address the growing concerns related to online privacy, data collection, and targeted advertising aimed at children.(Gilad et al., 2023) These discussions have highlighted the need to adapt regulations to encompass new technologies and online platforms, including social media and mobile applications, where children are increasingly active. Efforts to enhance the protection of minors' online privacy have also extended to educational institutions, which play a significant role in guiding and safeguarding students' internet usage. Many schools and educational organizations have implemented their own privacy policies and guidelines to complement COPPA regulations, emphasizing the importance of educating both students and parents about safe online practices.(Souris, 2018)

While COPPA has undoubtedly served as a strong foundation for protecting the internet privacy of minors, continual evaluation and potential updates to the law will be essential in effectively addressing the evolving challenges posed by the digital landscape. It is imperative to strike a balance between promoting a safe online environment for minors and allowing them to reap the educational and social benefits of the internet.

The impact of COPPA in safeguarding the online privacy of minors cannot be overstated. It has set important standards for website operators and online services to ensure that children's personal information is handled with care and requires verifiable parental consent for data collection. However, as technology continues to advance, there are valid concerns about the need to update and strengthen COPPA to address the evolving digital landscape.(Children's Online Privacy Protection Rule, 2023)

One of the key areas of focus is the increasing presence of children on social media and mobile applications. These platforms present unique challenges in terms of data collection, targeted advertising, and content exposure. As such, there have been proposals for revisions to COPPA that specifically target the regulation of social media platforms and mobile applications that cater to or attract a significant number of minors.(Vallejos et al., 2021)

In addition to addressing the regulation of specific digital platforms, there has been a call for increased enforcement and oversight of COPPA compliance. Strengthening enforcement measures can enhance the effectiveness of the law in holding website operators and online services accountable for violations. Moreover, there is a growing recognition of the need for comprehensive digital literacy and privacy education in schools. Integrating age-appropriate digital citizenship and online privacy education into curricula can empower students to navigate the online world safely and responsibly.

As discussions about potential reforms to COPPA continue, it is important to consider the perspectives of various stakeholders, including educators, technology experts, advocates for children's rights, and industry representatives. Implementing any revisions to COPPA should be a collaborative effort that takes into account the diverse interests and expertise of these stakeholders while prioritizing the protection of minors' online privacy. The ongoing evaluation and potential updates to COPPA reflect the commitment to ensuring that the policies and regulations governing internet privacy for minors remain effective and responsive to the challenges posed by the dynamic digital environment. To sum up, the Children's Online Privacy Protection Act primarily governs American policies regarding internet privacy for children. COPPA aims to protect children's privacy online by placing restrictions on the collection and use of their personal information. However, with the ever-evolving digital landscape and the increasing presence of children on social media

and mobile applications, there have been calls for revisions to COPPA that address specific platforms and enhance enforcement measures.

The Children's Online Privacy Protection Act has undoubtedly set vital standards for protecting the online privacy of minors, but there are several weaknesses that need to be comprehensively addressed. One of the primary weaknesses of COPPA is its limited scope in the face of rapidly advancing technology. As the digital landscape continues to evolve, the law struggles to keep up with the complex and diverse methods of data collection and targeted advertising aimed at children. Furthermore, while COPPA emphasizes obtaining verifiable parental consent for the collection of personal information from children under 13, there are challenges in effectively enforcing this requirement. Many websites and online services find ways to circumvent this consent process, leading to unauthorized data collection and privacy breaches.(Zhao et al., 2019)

Another weakness of COPPA lies in its definition of "personal information," which does not encompass certain types of data such as location information and behavioral tracking. This creates loopholes that can be exploited by website operators and online services to gather extensive data on minors without parental consent. Moreover, the law places a significant onus on parents to monitor and control their children's online activities, but it does not provide adequate support for parents who may lack the necessary digital literacy skills to navigate the complexities of online privacy protection effectively. (Lievens et al., 2018)Additionally, there are challenges in overseeing and regulating the vast and diverse digital landscape, including social media platforms and mobile applications, where children are increasingly active. The current framework of COPPA may not adequately address the unique privacy risks and data collection practices prevalent in these platforms. Efforts to revise and strengthen COPPA should take into account these weaknesses and work towards addressing the evolving challenges posed by the digital environment, focusing on comprehensive measures to protect the online privacy of minors in a manner that aligns with the current digital landscape. One proposed solution is to broaden the scope of COPPA to include children up to the age of 16, as implemented in the General Data Protection Regulation in the European Union.

Comparisons of Child Privacy Legislation Comparative Analysis of Children's Digital Privacy Rights: COPPA, GDPR, and Indonesia's PDP Law

The rapid growth of digital platforms has necessitated robust legislative measures to protect children's digital privacy. Three prominent legal frameworks addressing this issue are the Children's Online Privacy Protection Act of the United States, the General Data Protection Regulation of the European Union, and Indonesia's Personal Data Protection Law. This essay provides a comprehensive

comparative analysis of these regulations, examining their similarities and differences with respect to the treatment of children's digital privacy rights. The key areas of focus include the scope and age of consent, requirements for parental consent and verification, principles of data minimization and purpose limitation, as well as the enforcement mechanisms and associated penalties.

The General Data Protection Regulation introduced explicit provisions for the protection of children's personal data, recognizing their need for specific safeguards in the digital age (Mačėnaitė, 2017). The regulation sets the age of consent for children at 16 years, with member states having the option to lower this to 13 years. In contrast, COPPA in the United States applies to children under the age of 13, requiring verifiable parental consent for the collection, use, or disclosure of their personal information. (Sofian et al., 2021) Indonesia's PDP Law, while still in draft form, has proposed a similar age threshold of 17 years for children's digital privacy protection. (Sofian et al., 2021)

These frameworks also diverge in their approaches to parental consent and verification. The GDPR requires parental consent for the processing of children's personal data, with member states responsible for establishing appropriate age verification mechanisms. COPPA, on the other hand, mandates that operators of online services directed at children or with actual knowledge of children's use, must obtain verifiable parental consent before collecting, using, or disclosing their personal information. Indonesian law, though not yet finalized, is expected to align with the GDPR's requirements for parental consent and verification.

Another key distinction lies in the principles of data minimization and purpose limitation. The GDPR emphasizes the need for data controllers to collect and process only the personal data that is necessary for the specific purpose, and to use it only for that purpose. (Jasmontaite & Hert, 2014) COPPA, in contrast, focuses more on transparency and disclosure requirements, mandating that operators clearly inform parents about their data collection and use practices.

The enforcement mechanisms and associated penalties also differ across these regulatory frameworks. The GDPR grants data subjects, including children, a range of rights and empowers supervisory authorities to impose fines of up to 4% of an organization's global annual revenue for non-compliance. COPPA, on the other hand, is enforced by the Federal Trade Commission in the United States, which can impose civil penalties of up to $43,792 per violation (Lievens & Verdoodt, 2017). Indonesia's PDP Law, once finalized, is expected to introduce similar enforcement mechanisms and penalties to ensure effective protection of children's digital privacy.

Scope and Age of Consent

COPPA, enacted in 1998, was a groundbreaking and influential piece of legislation that addressed the pressing issue of children's online privacy concerns. It emerged as a direct response to the unregulated collection and exploitation of personal information from children by websites and online services, establishing a global precedent for privacy legislation and setting the stage for future regulatory efforts.(Gilad et al., 2023)

COPPA's primary objective is to regulate the collection, use, and disclosure of personal information from children under the age of 13, requiring operators of websites and online services to obtain verifiable parental consent before gathering any such data. This prescriptive approach aimed to empower parents and provide them with greater control over the digital privacy of their children.

In contrast, the GDPR, implemented in 2018, offers a more comprehensive and flexible framework for the protection of personal data, covering all individuals within the European Union. Regarding children's digital privacy, the GDPR sets a higher default age threshold for consent at 16 years, but allows member states to lower this to no less than 13 years. This flexibility acknowledges the diverse social and cultural norms across the EU, enabling tailored applications that better align with local practices and sensibilities.(Icenogle et al., 2019)

Indonesia's Personal Data Protection Law, currently under consideration, proposes a similar approach to the GDPR, with a suggested age threshold of 17 years for the protection of children's personal data. This alignment with the GDPR's framework reflects Indonesia's efforts to harmonize its digital privacy regulations with international best practices, recognizing the unique vulnerabilities and needs of children in the digital age.(Soemarwi & Susanto, 2021)

Furthermore, the GDPR's scope is extensive, extending to any entity processing the data of EU residents, regardless of the entity's geographical location. This broad reach ensures that the privacy rights of children are safeguarded, even in the face of the ever-evolving digital landscape and the increasingly global nature of data processing operations.

Indonesia's PDP Law, enacted in 2022, closely aligns with the principles and approaches of the GDPR, but is tailored to the unique social, cultural, and regulatory context of Indonesia. While the PDP Law emphasizes the need for consent from legal guardians when processing children's data, it does not yet specify a clear age threshold for defining a child. This omission can lead to interpretative challenges and result in varied enforcement approaches among operators, potentially creating inconsistencies in implementation. As the PDP Law continues to evolve, it is crucial for policymakers to address this gap and provide clear guidance on the age of consent for children's digital privacy protection, ensuring consistent and effective implementation across Indonesia.(Putri & Martha, 2022)

Data Minimization and Purpose Limitation

COPPA imposes strict limitations on the collection of children's personal data, restricting it to only what is reasonably necessary for the specific activity or service being provided. The regulation prohibits conditioning a child's participation in activities on the provision of more personal information than is needed to facilitate that activity. Furthermore, it mandates that any collected data must be retained only for as long as necessary and deleted thereafter, preventing the accumulation of unnecessary personal information.(Sloot, 2024)

The GDPR's principles of data minimization and purpose limitation closely align with and reinforce COPPA's provisions. The regulation requires that personal data, including that of children, be adequate, relevant, and limited to what is strictly necessary for the intended processing purpose. Additionally, the GDPR mandates the erasure of data once it is no longer required for the specified purpose, promoting accountability among data controllers and ensuring that personal information is not retained indefinitely.(Biega et al., 2020)

Similarly, Indonesia's PDP Law emphasizes the principles of data minimization and purpose limitation. The law mandates that personal data be processed only for the specified, legitimate purposes, and requires the deletion of data once it is no longer needed for those purposes. This ensures that data controllers handle personal information, including that of children, responsibly and transparently, processing it with care and only as needed to provide the intended services.

Parental Involvement and Consent

COPPA's primary mechanism for safeguarding children's digital privacy is its requirement for verifiable parental consent before the collection of personal information from children under 13. This approach empowers parents to make informed decisions about the use of their children's data and grants them a degree of control over the digital footprint of their offspring.(Zhao et al., 2019)

The GDPR's treatment of children's data follows a similar vein, recognizing the need for heightened protection and the importance of parental involvement. The regulation sets a default age of consent at 16 years, but allows member states to lower this to no less than 13 years, acknowledging the diverse cultural and social norms across Europe. This flexibility enables individual countries to strike a balance between empowering children's digital autonomy and safeguarding their privacy through parental guidance.(Milkaite & Lievens, 2019)

The GDPR, while not specific to children, also emphasizes the role of parental consent in the processing of personal data for minors. The regulation requires that for children under 16 (or the age set by member states, which can be as low as 13),

data controllers must obtain consent from the child's parent or legal guardian before collecting or processing their personal information. This alignment with COPPA's focus on parental involvement reflects the shared recognition that children require heightened privacy protection and that parents are best positioned to make decisions on their behalf.

Indonesia's PDP Law, while not yet as detailed as the GDPR or COPPA in its provisions for children's digital privacy, also underscores the importance of parental consent. The law mandates that the processing of personal data belonging to children must be authorized by their legal guardians, acknowledging the vulnerability of young individuals in the digital space and the need for adult supervision and decision-making.(Sofian et al., 2021)

Indonesia's PDP Law aligns with the GDPR's approach, proposing a suggested age threshold of 17 years for the requirement of parental consent. This alignment reflects Indonesia's efforts to harmonize its digital privacy regulations with international best practices, ensuring that the unique vulnerabilities and needs of children in the digital age are addressed.(Suari & Sarjana, 2023)

Despite these similarities, the specific implementation of parental consent mechanisms can vary across the three regulatory frameworks, reflecting the unique cultural and social contexts of each jurisdiction.

Enforcement and Penalties

COPPA is enforced by the Federal Trade Commission, which can impose civil penalties of up to $51,744 per violation per day. While these fines are substantial for smaller entities, they may not provide a sufficient deterrent for larger corporations that can more easily absorb such penalties.(Makridis, 2021)

The GDPR establishes rigorous enforcement mechanisms through national data protection authorities. Non-compliance can result in significant penalties of up to €20 million or 4% of the violating organization's global annual revenue, whichever is higher. These severe sanctions reflect the EU's strong commitment to ensuring strict adherence to data protection standards, as exemplified by a notable GDPR enforcement case involving a €50 million fine imposed on Google for inadequate transparency and improper consent practices.(Goldberg et al., 2024)

Indonesia's PDP Law, enforced by the Ministry of Communication and Information Technology, takes a comprehensive approach to enforcement. It imposes administrative sanctions, including fines, suspension of data processing activities, and even imprisonment for severe infractions. This comprehensive approach underscores the importance of compliance while addressing the unique challenges of data protection in the Indonesian context, which may include a diverse range of data controllers and processors operating within the country.(Putri & Martha, 2022)

The diverse child privacy protection frameworks of COPPA, GDPR, and Indonesia's PDP Law share the common overarching goal of safeguarding the digital privacy and rights of children. However, these legal instruments exhibit significant variations in their scope, age thresholds, consent requirements, and enforcement mechanisms, reflecting the diverse societal, cultural, and regulatory priorities across different jurisdictions. COPPA's protections narrowly focus on children under 13, establishing prescriptive rules for operators of websites and online services to obtain verifiable parental consent before collecting or using personal information from this age group. This approach prioritizes the protection of younger children's privacy, acknowledging their heightened vulnerability in the digital landscape. In contrast, the GDPR adopts a broader, more flexible approach, requiring parental consent for processing the data of children under 16, while allowing member states to adjust the age threshold based on local norms and practices. This flexibility enables individual countries to strike a balance between empowering children's digital autonomy and safeguarding their privacy through parental guidance.

Indonesia's PDP Law, inspired by the GDPR, represents an evolving paradigm tailored to the local context, but still exhibits some ambiguities in its implementation, particularly regarding the specific age threshold for defining a child. This reflects the ongoing challenges of adapting global data protection standards to the unique cultural, social, and economic realities within the Indonesian landscape.

Comprehending these nuanced distinctions across jurisdictions is critical for organizations operating in multiple regions to ensure comprehensive compliance and effectively uphold children's fundamental rights to privacy and data protection. As digital ecosystems continue to evolve, these legal frameworks must adapt and strengthen to address emerging challenges and reinforce the robust protection of children's digital privacy rights, ensuring that the vulnerabilities and diverse needs of young individuals are addressed in a dynamic and responsive manner.

CONCLUSION

The study of child privacy protection frameworks across Indonesia, Europe, and the United States reveals diverse approaches to safeguarding children’s rights in the digital age. Each region has adopted specific legislative measures that reflect their cultural, social, and technological contexts. However, the underlying goal remains universal: ensuring that children are protected from privacy risks and data exploitation in an increasingly interconnected world.

In Europe, the General Data Protection Regulation (GDPR) sets a comprehensive standard by emphasizing data minimization, purpose limitation, and stringent parental consent mechanisms for processing children's personal data. It

allows member states to adapt the age of consent between 13 and 16, offering flexibility to align with local norms. In the United States, the Children's Online Privacy Protection Act (COPPA) enforces strict parental consent requirements for children under 13. While this law has been pivotal, its limited scope and challenges in addressing advanced data practices highlight the need for updates. Meanwhile, Indonesia's Personal Data Protection Law (PDP Law), inspired by international standards, is in its nascent stage. Although promising, it lacks specific provisions for children's data protection and a clear age threshold, leaving gaps that need immediate attention.

The comparative analysis highlights the importance of developing tailored yet globally informed legislative frameworks. While the General Data Protection Regulation provides a robust model with flexible adaptations, the Children's Online Privacy Protection Act serves as a cautionary example of the risks associated with overly rigid regulations. Indonesia stands at a critical juncture, where integrating child-specific protections into its Personal Data Protection Law can shape its digital future.

The findings also emphasize the pivotal role of parental involvement in safeguarding children's online privacy. The mechanisms for obtaining parental consent vary significantly, with the GDPR and COPPA establishing structured approaches that Indonesia can emulate. Additionally, the enforcement mechanisms differ, with the GDPR imposing substantial penalties that effectively deter violations. In contrast, COPPA's penalties, though significant, may not adequately deter large corporations. Indonesia's evolving framework should aim for a balanced enforcement strategy that ensures compliance without stifling innovation.

To address these challenges, the study proposes several recommendations. First, Indonesia should harmonize its legal framework with global standards by incorporating clear age thresholds and child-specific protections in its PDP Law. Public awareness campaigns should educate parents and children about digital privacy risks and rights, fostering a culture of digital literacy. Schools can play a pivotal role by integrating privacy education into their curricula.

Moreover, Indonesia must enhance its enforcement mechanisms by imposing administrative penalties, criminal sanctions, and fines proportionate to the severity of violations. Collaborative efforts among government agencies, technology providers, educators, and parents are vital to creating a safer online environment. For instance, a joint regulation between Indonesia's Ministry of Communication and Information Technology and the Ministry of Women's Empowerment and Child Protection could address the immediate need for protecting children's data.

Leveraging technological advancements, Indonesia can develop tools that enhance privacy protections, such as parental control systems, AI-driven monitoring, and privacy-preserving technologies, which can effectively mitigate

risks. The evolving digital landscape necessitates a dynamic and proactive legislative approach, and periodic reviews of the PDP Law will ensure its continued relevance and alignment with emerging global challenges.

In summary, safeguarding children's digital privacy mandates a multifaceted approach that balances legal frameworks, public awareness, and technological innovation. As Indonesia navigates this complex terrain, it can draw valuable insights from the experiences of Europe and the United States. By adopting these comprehensive measures, Indonesia can ensure a safe, empowering, and equitable digital future for its younger generation.

REFERENCES

Abdullah, A., Cudjoe, E., & Frederico, M. (2018). Barriers to Children's Participation in Child Protection Practice: The Views and Experiences of Practitioners in Ghana. In Children Australia (Vol. 43, Issue 4, p. 267). Cambridge University Press. https://doi.org/10.1017/cha.2018.41

Adams, C., Pente, P., Lemermeyer, G., & Rockwell, G. (2023). Ethical principles for artificial intelligence in K-12 education. In Computers and Education Artificial Intelligence (Vol. 4, p. 100131). Elsevier BV. https://doi.org/10.1016/j.caeai.2023.100131

Anand, G., Hernoko, A. Y., & Dharmadji, A. G. (2020). THE URGENCY OF ENACTING PERSONAL DATA PROTECTION LAW AS A PATRONAGE FROM THE DEVELOPMENT OF COMMUNICATION AND INFORMATION TECHNOLOGY IN INDONESIA. In Perspektif (Vol. 25, Issue 1, p. 54). Universitas Wijaya Kusuma Surabaya. https://doi.org/10.30742/perspektif.v25i1.750

Apthorpe, N., Varghese, S., & Feamster, N. (2019). Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arXiv.1903.

Banakar, R. (2009). Power, culture and method in comparative law. In International Journal of Law in Context (Vol. 5, Issue 1, p. 69). Cambridge University Press. https://doi.org/10.1017/s1744552309005047

Bentotahewa, V., Hewage, C., & Williams, J. (2022). The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries. In SN Computer Science (Vol. 3, Issue 3). Springer Nature. https://doi.org/10.1007/s42979-022-01079-z

Berti, L. G., & Fachin, Z. (2021). SHARENTING: VIOLAÇÃO DO DIREITO DE IMAGEM DAS CRIANÇAS E ADOLESCENTES PELOS PRÓPRIOS GENITORES NA ERA DIGITAL. In Revista de Direito de Família e Sucessão (Vol. 7, Issue 1, p. 95). National Council for Research and Postgraduate Studies in Law. https://doi.org/10.26668/indexlawjournals/2526-0227/2021.v7i1.7784

Biega, A. J., Potash, P., Daumé, H., Díaz, F., & Finck, M. (2020). Operationalizing the Legal Principle of Data Minimization for Personalization. In arXiv

(Cornell University). Cornell University. https://doi.org/10.48550/arXiv.2005.

Children and the Digital Environment. (2024). https://www.coe.int/en/web/data-protection/home/-/asset_publisher/RMbj8Pk1ApgJ/content/children-and-the-digital-environment

Children's Online Privacy Protection Rule. (2023). https://www.ftc.gov/system/files/ftc_gov/pdf/p195404_coppa_reg_review.pdf

Gilad, M., Fishbein, D. H., Nave, G., & Packin, N. G. (2023). Science for policy to protect children in cyberspace. In Science (Vol. 379, Issue 6639, p. 1294). American Association for the Advancement of Science. https://doi.org/10.1126/science.ade9447

Goldberg, S. G., Johnson, G., & Shriver, S. K. (2024). Regulating Privacy Online: An Economic Evaluation of the GDPR. In American Economic Journal Economic Policy (Vol. 16, Issue 1, p. 325). American Economic Association. https://doi.org/10.1257/pol.20210309

Hong, S., Lu, N., Wu, D. D., Jimenez, D. E., & Milanaik, R. (2019). Digital sextortion: Internet predators and pediatric interventions [Review of Digital sextortion: Internet predators and pediatric interventions]. Current Opinion in Pediatrics, 32(1), 192. Lippincott Williams & Wilkins. https://doi.org/10.1097/mop.0000000000000854

Icenogle, G., Steinberg, L., Duell, N., Chein, J., Chang, L., Chaudhary, N., Giunta, L. D., Dodge, K. A., Fanti, K. A., Lansford, J. E., Oburu, P., Pastorelli, C., Skinner, A. T., Sorbring, E., Tapanya, S., Tirado, L. M. U., Alampay, L. P., Al‐Hassan, S. M., Takash, H. M. S., & Bacchini, D. (2019). Adolescents' cognitive capacity reaches adult levels prior to their psychosocial maturity: Evidence for a "maturity gap" in a multinational, cross-sectional sample. In Law and Human Behavior (Vol. 43, Issue 1, p. 69). American Psychological Association. https://doi.org/10.1037/lhb0000315

Jasmontaite, L., & Hert, P. D. (2014). The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet. In International Data Privacy Law (Vol. 5, Issue 1, p. 20). Oxford University Press. https://doi.org/10.1093/idpl/ipu029

Kahimise, J., & Shava, F. B. (2019). An analysis of children's online activities and behaviours that expose them to cybercrimes. In 2022 30th Telecommunications Forum (TELFOR) (p. 1). https://doi.org/10.1109/telfor48224.2019.8971089

Lievens, E., & Verdoodt, V. (2017). Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation. In Computer Law & Security Review (Vol. 34, Issue 2, p. 269). Elsevier BV. https://doi.org/10.1016/j.clsr.2017.09.007

Lievens, E., Livingstone, S., McLaughlin, S., O'Neill, B., & Verdoodt, V. (2018). Children's Rights and Digital Technologies. In International human rights (p. 487). Springer Nature. https://doi.org/10.1007/978-981-10-4184-6_16

Mačėnaitė, M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. In New Media & Society (Vol. 19, Issue 5, p. 765). SAGE Publishing. https://doi.org/10.1177/1461444816686327

Makridis, C. (2021). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. In Journal of Cybersecurity (Vol. 7, Issue 1). Oxford University Press. https://doi.org/10.1093/cybsec/tyab021

Milkaite, I., & Lievens, E. (2019). Child-friendly transparency of data processing in the EU: from legal requirements to platform policies. In Journal of Children and Media (Vol. 14, Issue 1, p. 5). Taylor & Francis. https://doi.org/10.1080/17482798.2019.1701055

Nouwens, M., Liccardi, I., Veale, M., Karger, D. R., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence (p. 1). https://doi.org/10.1145/3313831.3376321

Prabhakaran, V., Mitchell, M., Gebru, T., & Gabriel, I. (2022). A Human Rights-Based Approach to Responsible AI. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arXiv.2210.

Putri, E. P., & Martha, A. E. (2022). The Importance of Enacting Indonesian Data Protection Law as a Legal Responsibility for Data Leakage. In Varia Justicia (Vol. 17, Issue 3, p. 287). Muhammadiyah University of Magelang. https://doi.org/10.31603/variajusticia.v17i3.6231

Santer, N. D., Manago, A. M., Starks, A., & Reich, S. M. (2023). Early Adolescents' Perspectives on Digital Privacy. In The MIT Press eBooks (p. 123). The MIT Press. https://doi.org/10.7551/mitpress/13654.003.0012

Sitompul, J. (2019). DEVELOPING A LEGAL FRAMEWORK OF PERSONAL DATA PROTECTION IN THE INDONESIAN CRIMINAL PROCEDURE LAW. In Indonesia Law Review (Vol. 9, Issue 3). University of Indonesia. https://doi.org/10.15742/ilrev.v9n3.582

Siyam, N., & Hussain, M. (2021). Cyber-Safety Policy Elements in the Era of Online Learning: A Content Analysis of Policies in the UAE. In TechTrends. Springer Science+Business Media. https://doi.org/10.1007/s11528-021-00595-8

Sloot, B. van der. (2024). Principles relating to processing of personal data. In Oxford University Press eBooks (p. 135). Oxford University Press. https://doi.org/10.1093/law/9780192855220.003.0004

Soemarwi, V. W. S., & Susanto, W. (2021). Digital Technology Information in Indonesia: Data Privacy Protection is a Fundamental Right. In Advances in Social Science, Education and Humanities Research/Advances in social science, education and humanities research. https://doi.org/10.2991/assehr.k.210805.088

Sofian, A., Pratama, B., Besar, Pratomo, F. C. P., & Capaldi, M. P. (2021). A Brief Review: Children Online Privacy Protection in Indonesia. In Advances in Social Science and Culture (Vol. 3, Issue 3). https://doi.org/10.22158/assc.v3n3p12

Souris, R. N. (2018). Parents, Privacy, and Facebook: Legal and Social Responses to the Problem of "Over-Sharing." In AMINTAPHIL (p. 175). Springer International Publishing. https://doi.org/10.1007/978-3-319-74639-5_12

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. In Jurnal Analisis Hukum (Vol. 6, Issue 1, p. 132). https://doi.org/10.38043/jah.v6i1.4484

Syailendra, M. R. (2021). PERLINDUNGAN DATA PRIBADI TERHADAP TINDAKAN PENYEBARAN SEX TAPE MENURUT HUKUM POSITIF DI INDONESIA. In Jurnal Muara Ilmu Sosial Humaniora dan Seni (Vol. 5, Issue 2, p. 440). https://doi.org/10.24912/jmishumsen.v5i2.12506.2021

Torres-Hernández, N., & Arrufat, M. J. G. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review [Review of Indicators to assess preservice teachers' digital competence in security: A systematic review]. Education and Information Technologies, 27(6), 8583. Springer Science+Business Media. https://doi.org/10.1007/s10639-022-10978-w

Vallejos, E. P., Dowthwaite, L., Creswich, H., Portillo, V., Koene, A., Jirotka, M., McCarthy, A., & McAuley, D. (2021). The impact of algorithmic decision-making processes on young people's well-being. In Health Informatics Journal (Vol. 27, Issue 1). SAGE Publishing. https://doi.org/10.1177/1460458220972750

Zhao, J., Wang, G., Dally, C., Slovák, P., Edbrooke‐Childs, J., Kleek, M. V., & Shadbolt, N. (2019). `I make up a silly name': Understanding Children's Perception of Privacy Risks Online. In arXiv (Cornell University) (p. 106). Cornell University. http://arxiv.org/abs/1901.10245

Zostant, M., & Chataut, R. (2023). Privacy in computer ethics: Navigating the digital age. In Computer Science and Information Technologies (Vol. 4, Issue 2, p. 183). Institute of Advanced Engineering and Science (IAES). https://doi.org/10.11591/csit.v4i2.p183-190