**The International Journal of Social Sciences World**
TIJOSSW is Available Online at:
https://www.growingscholar.org/journal/index.php/TIJOSSW
Vol. 6 No. 2, July-December 2024, pages: 66~76
DOI: https://doi.org/10.5281/zenodo.13867212
ISSN **2690-5167**
Growingscholar Publisher

# Children's Privacy Rights and Data Mining in Educational Technology Applications Based on The Theory of Dignified Justice

**Qur'ani Dewi Kusumawardani[1], Teguh Prasetyo [2], Tommy Hendra Purwaka[3]**

Article history:
Received: September 11 2024; Accepted: October, 01 2024; Displayed Online: October, 01 2024; Published: December, 30 2024

***Keywords***

*Agreement;*

*Consent;*

*Data Protection;*

*Dignified Justice;*

**Abstract**

Children's personal data, as part of their right to privacy, must be guaranteed and protected under human rights laws, including the UN Convention on the Rights of the Child, which Indonesia has ratified. Given the significant number of children using the internet in Indonesia and their limited ability to protect themselves, safeguarding their privacy is crucial. This study aims to examine the legal framework governing the protection of children's personal data in Indonesian law and to develop a framework for protecting children's privacy rights in educational technology applications, grounded in principles of dignified justice. This research will employ a normative legal methodology. The study expects to identify significant threats posed by edutech companies, including unauthorized tracking of contact lists, monitoring of children's activities, and secret data processing without consent, often leading to the sale of data to third parties. Additionally, the study proposes a multi-stakeholder framework for safeguarding children's privacy, involving parents, companies, government, educational institutions, and the press.

## 1. Introduction

The internet is increasingly integral to the lives of individuals across all age groups, from children to the elderly. According to the APJII internet profile survey, the highest penetration rates are among adolescents aged 13-18 years, reaching 99.16%, and children aged 5-12 years, at 62.43%. (A. P. J. I. Indonesia, n.d.) However, this surge in internet usage among children correlates with a concerning rise in cases of cyber exploitation, unauthorized disclosure of personal data, theft, and other forms of

[1] *Ministry of Communication and Informatics, Republic of Indonesia, email : quranidewi@gmail.com*
[2] *Universitas Pelita Harapan, Tangerang, Indonesia, email : teguh.prasetyo@uph.edu*
[3] *Universitas Pelita Harapan, Tangerang, Indonesia, tommypurwaka@gmail.com*

digital crime targeting minors (Alfaro, Baar, & Bergman, 2016). Among the methods employed by perpetrators, doxing and grooming stand out. Predators exploit vulnerable children by collecting digital footprints, enabling them to manipulate and coerce victims into sharing personal information or images (E. Indonesia, 2018). This practice, known as sextortion, poses significant threats to children's safety and privacy rights.

The COVID-19 pandemic accelerated the adoption of educational technology (*edutech*), with online platforms like Ruang Guru, Kelas Pintar, and Zenius Education becoming essential tools. However, a collaborative investigation involving Narasi, Human Rights Watch, and international media revealed alarming data mining practices across 165 platforms in 49 countries, including Indonesia (Rahman, 2022) Shockingly, 89% of these platforms engaged in data practices that either implicitly or explicitly violated children's rights by covertly monitoring and selling their data without parental or child consent. Children, as vulnerable members of society, are entitled to protection from all forms of exploitation and inhumane treatment, including the misuse of their personal data. This obligation is enshrined in Indonesia's Child Protection Law No. 35 of 2014, affirming that children's rights are integral human rights that must be safeguarded by parents, families, communities, and the state (*Problems for Children and Their Rights: How Computers Used Private Information about Children While They Learned on The Internet during Covid-19*, 2022).

Despite legal protections, there remains a significant gap in public awareness and behavior regarding personal data security. The widespread practice of uploading sensitive information, including children's data, onto digital platforms reflects a general disregard for privacy safeguards (Karo & Prasetyo, 2020). A national survey on "Public Perception of Personal Data Protection" conducted across 34 provinces highlighted widespread negligence in managing privacy settings on gadgets and social media applications (D. J. A. I. K. K. dan I. R. Indonesia, 2022; Kristianti, 2022).

In this study, we aim to delve deeper into the concept of dignified justice and its potential to effectively safeguard children's privacy rights in the face of the widespread data mining practices prevalent in educational technology applications. Dignified justice, rooted in the principles of human rights and ethical governance, emphasizes the inherent worth of every individual and the obligation to protect their dignity, particularly in vulnerable populations such as children. As educational technology becomes increasingly embedded in learning environments, particularly during and after the COVID-19 pandemic, the potential for misuse of children's data has grown exponentially. The intersection of technology and education offers significant benefits for learning and development, but it also presents substantial risks when children's data is harvested, analyzed, and potentially misused without adequate safeguards. This raises critical ethical and legal questions about the responsibilities of edutech companies, governments, educators, and society at large.

By examining the perspective of dignified justice, this study seeks to provide a framework for understanding and addressing these issues. We explore how dignified justice can be operationalized to create more robust protective measures that respect children's rights and prevent exploitation. This involves scrutinizing current practices in data collection, consent mechanisms, and privacy policies within educational technology platforms, and assessing their alignment with the principles of dignified justice.

## 2. Materials and Methods

This study employs a normative juridical research approach, which focuses on analyzing legal norms, principles, and regulations within a structured legal framework (Hadikusuma, 1995; Nazir, 2005). Normative juridical research is particularly suitable for this study as it allows for a comprehensive examination of the legal protections and ethical considerations surrounding

children's privacy rights in the context of data mining practices by educational technology platforms. The data collection method primarily involves extensive literature studies, drawing on a wide range of legal and academic sources to build a robust understanding of the subject matter. The library materials utilized in this study consist of secondary data, which is supplemented by primary, secondary, and tertiary legal materials.

Primary legal materials form the foundation of the research. These include essential legal documents such as constitutions, statutes, regulations, and other binding legal provisions that establish the basic norms and rules governing the protection of personal data, especially in relation to children's rights. Examples of these materials include Indonesia's Child Protection Law No. 35 of 2014, the General Data Protection Regulation (GDPR), and other relevant international and national legal instruments.

Secondary legal materials serve to interpret, analyze, and provide context to the primary legal materials. These include authoritative texts such as legal commentaries, academic books, peer-reviewed journal articles, and research reports. These materials are crucial for understanding the application of legal principles in real-world scenarios, as well as for exploring scholarly debates and interpretations related to personal data protection. They also provide insights into how different jurisdictions address similar issues, offering a comparative perspective that enriches the analysis.

Tertiary legal materials are used to support the understanding and interpretation of both primary and secondary legal materials. These include legal dictionaries, encyclopedias, and lexicons, such as the Black's Law Dictionary and the Great Dictionary of the Indonesian Language. These resources are invaluable for clarifying legal terminology, concepts, and definitions that are essential for accurate and precise legal analysis.

## 3. Results and Discussions

### *A. Children Privacy Right and Children Data Mining Condition*

Narasi and Human Rights Watch, along with 14 international media outlets, investigated 165 educational technology companies in 49 countries. From Indonesia, the edu-tech platforms observed are Ruang Guru, Kelas Pintar, Zenius Education, Quipper School, Sekolahmu and Rumah Belajar. These six edutech companies also collaborate with the Ministry of Education and Culture as stated in the Circular Letter of the Minister of Education and Culture of the Republic of Indonesia. There are 2 methods used to analyze data mining carried out by edutech companies(*Problems for Children and Their Rights: How Computers Used Private Information about Children While They Learned on The Internet during Covid-19*, 2022), as follows:

*Static Analysis*

It is done by analyzing the application code and the instructions that are executed when the application is opened. The tools used for static analysis are Exodus and Pitheus. All results are verified by scanning each app with Pithus (a mobile app threat intelligence platform), and ÿxodus by ÿxodus Privacy (an open-source privacy auditing platform embedded in Android apps).

*Dynamic Analysis and Child Participation*

It is done by observing the work of edutech company applications in real time using android developer studio. Then it is compiled and analyzed running code to know what data is being sent,

where the data is being sent, and to whom. This analysis process is assisted by the defensive lab agency (Mobile Digital Security Agency in France). In the analysis of children's participation, children are required to download virtual personal networks (VPNs) and EdTech applications on their mobile devices, then children are asked to open, run, and close VPNs and EdTech applications several times a day. Then children have to interact with the app as if they were using it for school or study. After 24 hours, the children deleted both from their phones. Esther Onfroy of the Defensive Lab Agency receives data files and analyzes them to identify data streams and transmissions.

The result is that edutech companies can track phone contact lists, and monitor children's activities. The edutech companies that were researched, both implicitly and explicitly, stated that they had monitored and processed children's data secretly without the consent of the child or parents and sold the data to third parties, namely advertising companies. Furthermore, the advertising company will sell to clients who target children. In addition, there are several strange things that are found as follows:

1. *Permission Aps or Application Access Permissions (Precise Location Data)*

The App Access permissions ideally adapt to the needs of the app, for example GPS access for transportation apps, or camera access for photo editing apps. However, the edutech company turned out to be making an access request. Of the 6 applications of edutech companies, there are 3 applications that request GPS data precisely, namely sekolah.mu, teacher's room and learning house. From this type of location access permission, the applicator has access to retrieve location data, and user activity precisely. In the description of the app permission in the android store on each application, only your school and the learning home have publicly announced this. Meanwhile, the teacher's room is not open about the ability to access this GPS data sucking. The question that arises then is what is precisely GPS data needed for in an Education application? Because in the Education application, there is not a single convincing reason why the Education application requires a GPS precision location.

2. *Ability to access Read Phone State*

Teacher's Room, Smart Class, Your School and Zenius can access the read phone state. When the read phone state is opened, the applicator can find out the child's phone number, mobile network information and the status of the call in progress. In teacher rooms and smart classrooms, read phone state data is made more specific because it can be used to request access to call logs and contact numbers. When using three access combinations, namely read phone state, call log, and read contacts, the edutech company can find out who is the child's connection relationship. For example, when permission data is collected by applications from students which are then sold to advertising companies, is the identity of the individual in it immediately removed?

The privacy policy of the teacher's room in the personal data disclosure section indicates that the teacher's room does not disclose information about identifiable individuals. However, the teacher's room provides aggregate information about the user. Aggregate information simply includes plural things, aka not targeting individual individuals. However, the teacher's room claim is contrary to narasi.com's findings, because the teacher's room is proven to collect android advertising.id (AAID) on every user of the teacher's room. In short, application developers and google ad networks can use advertising IDs to recognize users' phones among hundreds of millions of existing android gadgets, so that they can serve ads according to the interests and behavior of application users, which means

that not only behavior data from application users (students) but also the teacher's room can also send subjects who own user behavior data.

The collection of advertising IDs carried out by the teacher's room was also carried out by 5 other application developers, but of the 6 applications, only sekolahmu, zenius, and quipper have publicly admitted to having taken advertising IDs. The rest of the teacher's room, study house, and smart classroom cover this. When confirmed in writing via email, Quipper and Ruang Guru denied having collected advertising IDs, but on the other hand Quipper and Ruang Guru have admitted that they collected secondary data in the form of their users' mobile device IDs. Zenius and sekolah.mu have also admitted to sucking up advertising ID data in the context of business development.

3. *Collection of User International Mobile Equipment Identity (IMEI)*

The smart class not only collects advertising IDs, but also collects the IMEI of its users. IMEI is an identity that is attached to a mobile phone and cannot be replaced, so IMEI is very personal. IMEI Access is used by law enforcement to track cases. In fact, in Google's child privacy policy, it is clearly stated that AAID and IMEI are illegally collected or deposited on third parties if their users are children. An IMEI cannot be changed, and it is illegal to do so in some countries. The only means of changing one's IMEI is to throw the phone away and purchase a new one.

4. *Related Software Development Kit (SDK)*

Education application companies in various countries are strongly suspected of selling and sending children's personal data to advertising companies. In the context of technical analysis through Software Development Kit (SDK) data embedded in the application. The data contained in the SDK is used to analyze app performance or track bugs. However, not a few children's data is also deposited for profiling analysis and targeted advertising.

Some applications blatantly send data to advertising marketing analytics companies. For example: SDK data sent by the teacher's room, zenius to AppsFlyer (a global company headquartered in Silicon Valley, USA), smart classes on Adjust (a German company), your school on Snowplow (based in London, United Kingdom). After being confirmed in the teacher's room, it is known that the status of the 3rd party or APPS Flyer is solely used to track marketing activities or attribution, and fraud protection. Although the teacher's room admits that there is a data transfer on Apps Flyer, it argues that the data sent is in the form of aggregate data, not in the form of personal data.

5. *Findings on edutech applications owned by the government, such as Rumah Belajar.*

Based on the analysis of the Investigative Defensive Lab, it is known that children's data is collected and sent to advertising companies, namely to DoubleClick.net domain. Even though Rumah Belajar is an Education application managed by the Ministry of Education and Culture, and funded from taxes. If you look at the privacy policy of Rumah Belajar, it is known that Rumah Belajar honestly admits that user data has been deposited and then returned for targeted advertising for its users.

Human Rights Watch's findings by looking at and analyzing all government-owned education applications in various countries studied, found that only Indonesia has honestly admitted that this child data was sold to advertising companies.

## B. *The perspective of dignified justice in protecting children's privacy related to data mining activities in technology education applications*

The theory of dignified justice is deeply rooted in the philosophy of Pancasila, which serves as a guiding principle, a moral compass, and a foundational norm for Indonesian society (Prasetyo, 2021). Dignified justice emphasizes the importance of upholding the inherent dignity and worth of every individual, particularly within the context of the distinctive values that naturally evolve and flourish within a society (Prasetyo, 2019). These values form the bedrock upon which actions and policies should be based, ensuring that justice is not only fair but also respectful of human dignity. Dignified justice operates on the premise that societal systems should function in a manner that achieves justice in a way that honors the dignity of all individuals. In the context of children's rights and privacy, this theory underscores the need for systems and practices that protect the most vulnerable members of society from exploitation and harm (Prasetyo, 2016).

Recent investigations by Narasi and Human Rights Watch reveal that a staggering 89% of educational technology platforms engage in data practices that are deemed risky or potentially harmful to children. From the perspective of dignified justice, these practices represent a serious violation of children's rights. Such actions are considered inhumane as they exploit children's personal data without their informed consent, thereby disregarding their inherent dignity and right to privacy.

The theory of dignified justice advocates for the protection of children's privacy rights, emphasizing the moral and legal obligation to shield children from any form of exploitation or harm. This protection is not merely a legal duty but a reflection of the societal commitment to uphold the dignity of every child. Ensuring the privacy and security of children's data is a fundamental aspect of safeguarding their dignity and allowing them to develop in an environment free from undue risks and violations.

In the framework of dignified justice, the protection of children's privacy is envisioned as a collaborative effort involving multiple stakeholders, including parents, companies, the government, and the education sector. This collective responsibility is guided by the concept of the "circle of protection," which emphasizes the need for a comprehensive and cohesive approach to safeguarding children's rights in the digital realm.

First, protection begins with parents or guardians, who play a crucial role as the first line of defense in ensuring their children's safety online. According to insights from the Safer Kids Online website, a significant risk to children's privacy stems from parents' lack of understanding of the digital landscape. This gap in knowledge can create vulnerabilities, making it easier for malicious actors to exploit children's personal data. To mitigate these risks, parents must adopt a proactive stance when their children engage with the internet (*Problems for Children and Their Rights: How Computers Used Private Information about Children While They Learned on The Internet during Covid-19*, 2022). This involves two key approaches:

*Benchmarking*

Parents conduct an audit of all services, websites, applications and internet devices that can be accessed by children (including the application of the edutech company). Parents check the edutech application regarding what permission will be given and the data will be given to any party by the application.

*Ongoing safeguards.*

Set a limit such as what information children are allowed to access, what children should do if they see inappropriate content, and how to accept invitations from unknown people on social media platforms. Second, the government plays a pivotal role in guiding educational technology companies through well-defined provisions that focus on three key areas: 1) Company Governance, 2) Product and Service Development, and 3) Product and Service Provision.

*Company Governance*

Educational technology (edutech) companies bear a significant responsibility to create digital environments that are safe and uphold children's rights. The governance of these companies should reflect a deep commitment to the protection of children, integrating the principles established by the Committee on the Rights of the Child into their operations and policies. This responsibility encompasses several critical aspects:

a) Edutech companies must ensure that the rights and best interests of children are central to their policies and management processes. This involves embedding the principles of child protection into the company's culture, management practices, goals, and every stage of product and service development. By making child rights a core consideration, edutech companies can better protect children from potential harm.

b) To truly serve the best interests of children, edutech companies should adopt an interdisciplinary approach. This means involving a range of stakeholders, including children and their families, specialists in child development, and child rights experts, in the governance process. By incorporating diverse perspectives, companies can make more informed decisions that prioritize the safety and well-being of child users.

c): It is imperative that edutech companies adopt the best available technologies to protect children's rights. This includes implementing state-of-the-art privacy protections, robust data security measures, and tools that prevent unauthorized access to children's personal information. The goal is to ensure that all children, regardless of their background, have access to safe digital learning environments.

d) Edutech companies have a duty to regularly test and evaluate their privacy policies, company standards, and age-verification mechanisms. This ongoing assessment ensures that the policies are effective in protecting children and comply with legal and ethical standards. Companies should be transparent about these policies, making it clear how they protect children's privacy and enforce age restrictions.

*Product and Service Development*

In the design and development of both online and offline educational technology products, companies are obligated to adhere to and prioritize the rights of children as outlined in Article 3.1 of the Committee on the Rights of the Child. This commitment requires edutech companies to consider several critical aspects:

a) All processing of children's data must be relevant to the specific purposes for which the data is collected, ensuring that the least amount of personal data is used. This principle emphasizes the need for data minimization, which helps protect children from unnecessary exposure and reduces the risks associated with data breaches or misuse.

b) Children should be provided with user-friendly online tools that allow them to easily access, correct, delete, restrict, or object to the processing of their personal data. This empowers children to take control of their digital identities and ensures that their data is handled in accordance with their rights and preferences.
c) Products and services designed for children must be free from commercial coercion, particularly covert marketing strategies. This includes protecting children under the age of 16 from being targeted by advertisements in digital environments. The goal is to create a safe space where children can learn and explore without being subjected to manipulative commercial influences.
d) The design of edutech services and application products should focus on providing enriching, educational, and enjoyable experiences for children. These experiences should not be monetized or exploitative, ensuring that children are not treated as mere consumers but as individuals with the right to learn and grow in a supportive environment.
e) Nudge techniques—design elements intended to influence user behavior—must be employed transparently and ethically, always prioritizing the best interests of the child. These techniques should guide children towards positive and safe online behaviors, rather than exploiting their vulnerabilities for commercial gain.
f) Edutech companies must strive to protect children from inappropriate content and harmful contacts. This includes developing systems that prevent unauthorized interactions, shield children from exposure to child sexual abuse material, and ensure that the digital environments they create are secure and age-appropriate.
g) By default, edutech applications should implement high privacy settings. This means that features such as profiling and geolocation should be turned off unless explicitly activated by a parent or guardian. These settings help safeguard children's privacy from the outset, reducing the risk of data exploitation.
h) Online tools should support parental control and mediation, enabling parents to oversee their children's digital activities and ensure that their privacy and safety are maintained. These tools can help parents guide their children's online experiences in a way that aligns with their values and expectations.
i) Children should have the option to engage with digital products and services without being subjected to data collection. This means that edutech companies must offer children opportunities to learn, play, and participate in digital environments without compromising their privacy.

*Product and Service Provision*

Once an educational technology product or service is launched, it is crucial to ensure that the framework for its provision prioritizes the protection of children's rights and safety. The following key measures must be implemented by edutech companies:
a) Children's Data Protection Impact Assessments (CDPIA): Edutech companies are required to conduct Children's Data Protection Impact Assessments (CDPIA) to evaluate and mitigate the potential risks associated with their digital products or services, particularly those accessed by children. The primary goal of CDPIA is to identify any vulnerabilities that could expose children to privacy breaches or other forms of digital harm. By proactively assessing these risks, companies can implement protective measures that safeguard children's data from the outset.
b) It is imperative for edutech companies to prevent any use of children's data that could negatively impact their welfare. This involves strict oversight and monitoring to ensure that data is not exploited for purposes that could harm children, whether physically, emotionally, or psychologically.

Companies must establish clear protocols to prevent the misuse of data, reinforcing their commitment to upholding the best interests of the child in all aspects of their operations.
c) Providing clear age indications for edutech products and services is essential for parents and guardians to make informed decisions about their children's digital engagement. Age-appropriate design ensures that content, features, and functionalities are tailored to the developmental needs and abilities of children within specific age groups. This not only enhances the educational value of the product but also protects children from exposure to content that may be unsuitable for their age.
d) The data processing mechanisms employed by edutech companies must be transparent, accessible, and easily understandable for both children and their families. This means that companies should clearly explain how data is collected, processed, and used in language that is simple and accessible to different age groups and literacy levels. Transparency in data practices builds trust and ensures that families are fully informed about how their children's information is being handled.
e) Children's data is inherently sensitive and must be treated with the utmost care. Edutech companies should adopt a strict policy against disclosing children's data to third parties unless there is an exceptional and compelling reason, such as safeguarding the child's safety or fulfilling a legal obligation in the best interest of the child. Protecting children's data from unauthorized dissemination is crucial in maintaining their privacy and security in the digital space.

Third, Governmental Protection through Comprehensive Policies and Regulations. The government's role in protecting children's personal data is paramount, and this can be achieved through the formulation and implementation of comprehensive policies and regulations. These should focus on several key areas:
a) Creation of security standards for the use of children's data, such as mandatory child data protection impact assessment, minimization of children's data, and limitations on data retention.
b) Transparency and accountability, such as privacy policies in edutech companies that are qualified and accommodate the best interests of children.
c) Periodic audit arrangements by edutech companies.
d) Arrangements for basic adjustment of the processing of children's personal data by edutech companies.
e) Establishment of a supervisory institution for law enforcement, and enforcement of violations against edutech companies that violate children's data.
f) Providing education to increase public awareness about the importance of protecting children's personal data.

Fourth, the education sector, as an extension of the government's efforts, plays a crucial role in safeguarding children's personal data by rigorously evaluating the data processing practices of edutech companies before integrating their products into the learning environment, ensuring adherence to established data protection standards, and prioritizing the best interests of children. Schools must act as gatekeepers, endorsing only platforms committed to protecting children's data. Additionally, digital literacy education should be integrated into curricula to raise awareness about the importance of data protection, using interactive and engaging tools that make learning both informative and enjoyable, ensuring students of all ages can navigate the digital space safely.

## 4. Conclusion

The covert data harvesting practices of online learning platforms during the pandemic have exposed children to significant risks, including the creation of detailed profiles that can predict their behaviors, emotions, and interests. This not only infringes on their privacy but also raises the

potential for abuse, where children may be guided towards outcomes that are not in their best interest.

To address these concerns, a collaborative effort is crucial. Parents, edutech companies, government, and the education sector must work together to implement stringent data protection measures, promote digital literacy, and ensure transparency and accountability in data handling. By doing so, we can create a digital environment that prioritizes children's privacy and well-being, upholding their right to protection from harm and the safeguarding of their human rights. Will we take action to protect our children's digital futures, or will we continue to compromise their rights and well-being?

**Acknowledgments**

This manuscript has no conflict of interest. The authors extend their gratitude to the reviewers and the publisher for the opportunity and help accorded to them, especially during the process of reviewing and publishing.

## References

Alfaro, M., Baar, S., & Bergman, E. (2016). *Children's Rights and the Internet From Guidelines to Practice*. New York.

Hadikusuma, H. (1995). *Metode Pembuatan Kertas Kerja atau Skripsi Ilmu Hukum*. Bandung: Mandar Maju. Retrieved from https://www.hrw.org/sites/default/files/media_2022/10/HRW EdTech ETR v5 HH.pdf

Indonesia, A. P. J. I. (n.d.). Survei Profil Internet Indonesia 2022.

Indonesia, D. J. A. I. K. K. dan I. R. (2022). Survei Nasional Persepsi Masyarakat atas Pelindungan Data Pribadi, tahun 2021.

Indonesia, E. (2018). *Modul Eksploitasi Sosial Anak di Ranah Online untuk Anak*. Jakarta.

Karo, R. P. K., & Prasetyo, T. (2020). *Pengaturan Pelindungan Data Pribadi di Indonesia (Perspektif Keadilan Bermartabat)*. Bandung: Nusa Media.

Kristianti, L. (2022). Kebocoran hingga pencurian data masih jadi tantangan besar di 2022. Retrieved October 25, 2022, from www.antaranews.com website: https://www.antaranews.com/berita/2615261/kebocoran-hingga-pencurian-data-masih-jadi-tantangan-besar-di-2022.

Nazir, M. (2005). *Metode Penelitian*. Jakarta: Ghalia Indonesia.

Prasetyo, T. (2016). *Sistem Hukum Pancasila (Sistem, Sistem Hukum dan Pembentukan Peraturan Perundang-Undangan di Indonesia) Perspektif Teori Keadilan Bermartabat*. Bandung: Nusa Media.

Prasetyo, T. (2019). *Pemilu dan Etika Penyelenggaraan Pemilu Bermartabat*. Bandung: Nusa Media.

Prasetyo, T. (2021). *Keadilan Bermartabat Perspektif Teori Hukum*. Bandung: Nusa Media.

*Problems for Children and Their Rights: How Computers used Private Information about Children while They Learned on The Internet during Covid-19*. (2022). New York.

Rahman, F. (2022). Data Pribadi Anak Rawan Disalahgunakan Platform Teknologi Pendidikan, Apakah UU PDP yang Baru Mampu Melindunginya? Retrieved October 25, 2022, from https://theconversation.com website: https://theconversation.com/data-pribadi-anak-rawan-disalahgunakan-platform-teknologi-pendidikan-apakah-uu-pdp-yang-baru-mampu-melindunginya-187976