JURNAL PENGABDIAN MASYARAKAT HABLUM MINANNAS
Vol. 5, No. 1, March 2026 Edition, Page: 30-41

EDUKASI PERLINDUNGAN HUKUM ANAK DI ERA DIGITAL UNTUK MENCEGAH CYBERBULLYING DAN KEJAHATAN SIBER DI FAKULTAS HUKUM UNIVERSITAS ISLAM SUMATERA UTARA

Muhammad Ansori Lubis[1], Elizabeth Ghozali[2], Yusuf Hanafi Pasaribu[3], Indra Gunawan Purba[4], Syawal Amry Siregar
[1,4] Universitas Islam Sumatera Utara, Medan, Indonesia
[2] Universitas Katolik Santo Thomas, Medan, Indonesia
[3,5] Universitas Pembinaan Masyarakat Indonesia, Medan, Indonesia
***Corresponding Author:** ansoriboy67@gmail.com

Abstrak

Perkembangan teknologi informasi dan komunikasi yang pesat menyebabkan meningkatnya kasus cyberbullying dan berbagai bentuk kejahatan siber yang menargetkan anak-anak dan remaja di Indonesia. Data Komisi Perlindungan Anak Indonesia (KPAI) mencatat ribuan kasus kekerasan berbasis digital terhadap anak setiap tahunnya, namun tingkat literasi hukum digital masyarakat dalam menghadapi persoalan ini masih sangat rendah. Kegiatan pengabdian kepada masyarakat ini dilaksanakan oleh Fakultas Hukum Universitas Islam Sumatera Utara (FH UISU) dengan tujuan meningkatkan literasi hukum digital peserta, memberikan pemahaman mendalam tentang hak-hak anak di ruang digital, bentuk-bentuk cyberbullying dan kejahatan siber, serta mekanisme pelaporan dan penegakan hukumnya. Metode pelaksanaan menggunakan pendekatan partisipatif melalui tiga tahapan: persiapan (survei kebutuhan, koordinasi, dan penyusunan materi), pelaksanaan (ceramah hukum, Focus Group Discussion, simulasi kasus, konsultasi hukum, dan edukasi digital), serta evaluasi. Kegiatan diikuti oleh 50 peserta yang terdiri atas siswa SMA/SMK, mahasiswa, orang tua, guru, dan masyarakat umum. Hasil pre-test dan post-test menunjukkan peningkatan rata-rata pemahaman peserta sebesar 49,6 poin persentase (dari 34,7% menjadi 84,3%), dengan tingkat kepuasan peserta mencapai 94%. Kegiatan ini secara efektif meningkatkan literasi hukum digital peserta, kemampuan identifikasi cyberbullying, dan pemahaman tentang mekanisme pelaporan kejahatan siber sebagai upaya membangun budaya digital yang aman dan bertanggung jawab bagi perlindungan anak.

Kata Kunci: *Perlindungan Anak, Cyberbullying, Kejahatan Siber, Literasi Hukum Digital, Pengabdian kepada Masyarakat*

CHILDREN'S LEGAL PROTECTION EDUCATION IN THE DIGITAL ERA TO PREVENT CYBERBULLYING AND CYBERCRIME AT THE FACULTY OF LAW, ISLAMIC UNIVERSITY OF NORTH SUMATRA

Abstract

The rapid development of information and communication technology has led to an increase in cyberbullying cases and various forms of cybercrime targeting children and adolescents in Indonesia. Data from the Indonesian Child Protection Commission (KPAI) records thousands of digital-based violence cases against children annually, yet the digital legal literacy of the community in addressing these issues remains very low. This community service activity was carried out by the Faculty of Law, Universitas Islam Sumatra Utara (FH UISU) with the aim of improving participants' digital legal literacy, providing in-depth understanding of children's rights in digital spaces, forms of cyberbullying and cybercrime, as well as reporting mechanisms and law enforcement. The implementation method used a participatory approach through three stages: preparation (needs survey, coordination, and material development), implementation (legal lectures, Focus Group Discussion, case simulation, legal consultation, and digital education), and evaluation. The activity was attended by 50 participants consisting of high school students, university students, parents, teachers, and the general public. Pre-test and post-test results showed an average improvement in participants' understanding of 49.6 percentage points (from 34.7% to 84.3%), with a participant satisfaction rate of 94%. This activity effectively improved participants' digital legal literacy, ability to identify cyberbullying, and understanding of cybercrime reporting mechanisms as an effort to build a safe and responsible digital culture for child protection.

Keywords: *Child Protection, Cyberbullying, Cybercrime, Digital Legal Literacy, Community Service.*

1. INTRODUCTION

Indonesia is one of the countries with the highest growth rate of internet users in Southeast Asia. Based on the We Are Social and Hootsuite (2024) report, the number of internet users in Indonesia has reached more than 215 million people or around 78% of the total population, with an average internet usage time per day reaching 7 hours and 42 minutes. More worryingly, most of the active users of the internet are children and adolescents aged 10-24 years who access various social media platforms, online games, and other digital communication services without adequate supervision from parents and educators. The high penetration of the internet among children and adolescents has serious consequences in the form of an increased risk of exposure to various forms of digital-based crime and violence. Data from the Indonesian Child Protection Commission (KPAI) for the 2022-2024 period recorded more than 4,500 complaints of information technology-based violence cases involving children as victims and perpetrators. These cases include cyberbullying, online sexual abuse, grooming, dissemination of immoral content involving children, online fraud targeting children, and sexual exploitation of children through digital platforms. The Indonesia Judicial Research Society (IJRS) in its 2023 report noted that only about 15% of total cybercrime cases against children were reported to law enforcement officials, indicating an iceberg phenomenon in actual case data.

The legal protection of children in the digital space in Indonesia is supported by a number of comprehensive regulatory frameworks, including Law Number 35 of 2014 concerning Amendments to Law Number 23 of 2002 concerning Child Protection, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), Law Number 44 of 2008 concerning Pornography, and Law Number 27 of 2022 concerning Personal Data Protection. However, the existence of these strong regulations has not been balanced with an adequate level of digital legal literacy in the community, so many victims and their families are unaware of their rights, available reporting mechanisms, and the legal protections they have access to. Universities, especially law faculties, have a strategic role and responsibility in increasing public legal awareness as part of the implementation of the Tri Dharma of Higher Education. Through the community service program, the academic community of the Faculty of Law can translate their legal knowledge into education that is applicable and easy to understand by various segments of society. This role has become increasingly crucial in the digital age when evolving legal issues are increasingly complex and beyond the boundaries of conventional regulations. The Faculty of Law, the Islamic University of North Sumatra (FH UISU) is one of the oldest and leading law faculties in North Sumatra that has a strong commitment to the development of laws based on Islamic values and social justice. FH UISU has competent teaching resources in various fields of law, including cyber law, child protection law, and information technology law, which makes it the right institution to implement digital legal education programs for the community. Based on observations and needs surveys conducted by the service team in September 2025, an urgent need for child legal protection education in the digital space was identified for various segments of society in Medan City, especially among children and adolescents, parents, and educators. Based on the results of needs surveys, field observations, and discussions with various stakeholders, several main problems that are the focus of service activities are identified:

1) Low digital legal literacy in children, adolescents, and the elderly. Most of the survey respondents do not understand the rights of children guaranteed by law in the digital space, do not know the limits of the acts that can be punished in the digital context, and are not familiar with the legal instruments available to protect them from cyber threats.
2) Lack of in-depth understanding of children's rights in the digital space. Many children and adolescents are unaware that they have the right to digital privacy, the right to safety from online exploitation, and the right to be protected from harmful content on the internet as guaranteed by applicable laws and regulations.

3) Lack of knowledge about the various forms of cyberbullying and its manifestations in daily digital life. Many victims don't realize that what they experience in the digital space is a form of violence that can be reported and processed legally, so they tend to keep their traumatic experiences to themselves.
4) Lack of knowledge about the available cybercrime reporting mechanisms, both through the National Police Cyber unit, the State Cyber and Cryptography Agency (BSSN), the Ministry of Communication and Information Technology (Kominfo), KPAI, and through the internal reporting mechanism of the social media platforms concerned.
5) Low public awareness, including potential perpetrators such as children and adolescents, regarding the serious legal consequences that can be imposed on perpetrators of cyberbullying and cybercrime based on the ITE Law, the Criminal Code, and the Child Protection Law, including prison penalties and fairly heavy fines.
6) The limitations of structured and sustainable digital legal education programs in schools and communities in Medan City result in children and adolescents growing up in a digital environment without adequate legal understanding.

Purpose of the Activity:

1) Providing comprehensive education on children's legal protection in the digital era, covering children's rights in a positive Indonesian legal perspective, forms of cyberbullying and cybercrime, and the regulations that govern them.
2) Improve participants' understanding of the different forms of cyberbullying and cybercrime that target children, including how to identify, prevent, and respond to each incident experienced.
3) Improve participants' ability to proactively prevent cyber threats and understand proper reporting procedures to law enforcement officials and authorized child protection agencies.
4) Fostering a culture of healthy, safe, and responsible digital media use among children, adolescents, families, and communities.
5) Building a digital child protection network and ecosystem in the City of Medan through the formation of a digitally literate community and active in cyberbullying prevention efforts.

Benefits of the Activity:

1) For Children and Adolescents: Increased awareness of digital laws that enable them to understand their rights, recognize threats in the digital space, and have the courage and knowledge to report every incident experienced. Children and adolescents are also expected to be agents of change who actively promote a positive digital culture in their environment.
2) For Parents: Improved parents' ability to monitor, guide, and accompany their child's use of the internet wisely, including the ability to recognize the signs of a child who is a victim of cyberbullying and knowledge of what steps can be taken when it occurs.
3) For Schools and Communities: Building the institutional capacity of schools and communities to create a safe and child-friendly digital ecosystem, including the availability of operational guidance in responding to cases of cyberbullying involving students.
4) For Higher Education (FH UISU): The implementation of the Tri Dharma of Higher Education, especially the dimension of community service, strengthening the institution's reputation as an institution that cares about contemporary legal issues relevant to society, and developing lecturer competencies in the field of cyber law and digital child protection.

2. IMPLEMENTATION METHOD

This community service activity was held in the Hall of the Faculty of Law Building, Islamic University of North Sumatra, Jalan S.M. Raja, Sandpaper, Medan City, North Sumatra. The selection of the location on the FH UISU campus aims to utilize adequate academic facilities as well as introduce the campus environment to participants from high school/vocational school

students who are one of the targets of the activity. The activity was held on Saturday, November 1, 2025, from 08.00 to 17.00 WIB, attended by 50 participants from various segments of the target community. The participants of the activity amounted to 50 people with a composition representing various segments of the target community:

1) High school/vocational school students from schools in the Medan City area (20 people), who are prioritized because they are the most vulnerable age group as well as the most active in the digital space.
2) Students of the Faculty of Law UISU and other universities in Medan City (10 people), who are expected to become agents of knowledge dissemination in their respective academic environments.
3) Parents of partner school students (10 people), who have a crucial role in supervising and guiding the use of the internet by children at home.
4) Counseling guidance teachers and educators from partner schools (5 people), who have a strategic function in handling cases of cyberbullying in the school environment.
5) The general public is interested, including child protection activists and members of religious communities (5 people).

This service program uses a Participatory Action Research (PAR) approach that integrates several complementary learning methods:

1) Legal Lecture and Socialization: Delivery of child protection legal material in a systematic and structured manner by resource persons who are experts in the fields of cyber law, juvenile criminal law, and information technology law, using language that is easy to understand by all segments of participants.
2) Focus Group Discussion (FGD): A targeted group discussion based on participant segments (children/adolescent groups, parent groups, and educator groups) to explore real problems faced, share experiences, and formulate contextual prevention strategies.
3) Cyberbullying Case Simulation: The practice of handling cyberbullying cases through realistic case scenarios, where participants practice correct identification, documentation, and reporting steps according to applicable legal procedures.
4) Personal Legal Consultation: A face-to-face consultation session between participants and a team of resource persons consisting of law lecturers and legal practitioners to answer questions and concrete cases experienced by participants.
5) Interactive Digital Education: Practical training using digital media, including demonstrations on how to use the reporting feature on various popular social media platforms, how to secure accounts and personal data, and how to access the KPAI, Kominfo, and Cyber Police online complaint portals.

The activity is carried out through three systematic stages as described in the following flow chart:

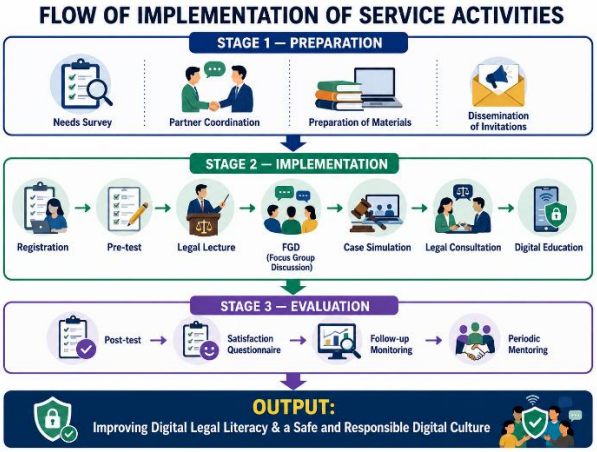

Figure 2. Flow Implementation of Service Activities

a. Preparation Stage

The preparation phase lasted for three weeks before the implementation and included: (1) needs assessment through questionnaires to prospective participants from partner schools and communities to identify the level of digital legal literacy and concrete problems faced; (2) coordination with the Dean of the Faculty of Law of UISU, the principal of partner schools, and other relevant stakeholders to obtain support and implementation permits; (3) the preparation of comprehensive training modules covering child protection laws, cyber regulations, forms of cyberbullying, cybercrime against children, and reporting mechanisms; (4) the development of pre-test and post-test evaluation instruments that have been tested for validity and reliability; and (5) the distribution of invitations through official letters to partner schools, community social media groups, and announcements in the UISU FH campus.

b. Implementation Stage

The implementation stage lasted a full day with a structured program arrangement: (1) participant registration and module distribution; (2) pre-test to measure initial knowledge; (3) the official opening by the Dean of the Faculty of Law UISU accompanied by the broadcast of data and videos of actual cyberbullying cases to build awareness of participants; (4) Session I — Material on Children's Rights in the Digital Space and Child Protection Regulatory Framework; (5) Session II — Anatomy of Cyberbullying: Forms, Impacts, and How to Deal with It; (6) Session III — Cybercrime against Children: Grooming, Online Sexual Exploitation, and Digital Identity Theft; (7) Session IV — Cybercrime Reporting and Law Enforcement Mechanism; (8) FGD per group segment; (9) case simulation; and (10) personal legal consultation sessions.

c. Evaluation Stage

The evaluation stage includes: (1) the implementation of post-tests with equivalent instruments to measure quantitative knowledge improvement; (2) filling out a participant satisfaction questionnaire on the seven aspects of activity evaluation; (3) the establishment of the WhatsApp group 'Medan Anti-Cyberbullying Agent' as a forum for consultation and dissemination of digital legal information on an ongoing basis; and (4) preparation of follow-up monitoring plans including schedules of visits to partner schools to monitor the implementation of the knowledge obtained.

2.5 Success Indicators

The success of the program is determined based on four measurable indicators: (1) an increase in participants' comprehension scores of at least 40 percentage points between pre-test and post-test; (2) the active participation rate of participants is at least 90%; (3) the satisfaction level of participants is at least 85% in the satisfied and very satisfied categories; and (4) the proportion of participants who can demonstrate the procedure for reporting cyberbullying cases correctly is at least 75%.

3. RESULTS AND DISCUSSION

3.1 Implementation of Activities

The educational activity on child legal protection in the digital era was held on Saturday, November 1, 2025, in the Hall of the UISU Faculty of Law Building, Medan. The activity took place from 08.00 to 17.00 WIB and was attended by 50 participants according to the set target. The opening of the activity was officially carried out by the Dean of the Faculty of Law UISU who in his speech emphasized that child protection in the digital space is a shared responsibility between families, schools, communities, and the state, and affirmed the commitment of FH UISU in actively contributing to efforts to prevent cybercrime through community legal education.

The activity took place very dynamically and interactively. The resource team consisting of four lecturers from the Faculty of Law of UISU with specializations in the fields of criminal law, cyber law, child protection law, and information technology law, as well as one guest speaker from the Cyber Directorate of the North Sumatra Police, delivered material alternately with an adaptive approach according to the participant segment. The FGD session which was divided into three groups based on segments (children/adolescents, parents, and educators) resulted in rich discussions with various real experiences of participants related to cyberbullying incidents in their environment, reflecting how actual this problem is in the daily digital lives of the people of Medan City. The simulation session of cyberbullying cases received a very enthusiastic response, especially from high school/vocational school students. Through realistically designed case scenarios based on actual cases that have been disguised, participants practice the steps: identifying actions that fall into the category of cyberbullying, documenting digital evidence, compiling standards-compliant reports, and accessing appropriate complaint portals. A total of 41 out of 50 participants (82%) successfully completed the simulation reporting procedure, exceeding the target of 75% success indicators.

3.2 Children's Legal Protection Education in the Digital Era

a. Children's Rights in a Legal Perspective

The first material comprehensively discusses children's rights guaranteed by Indonesia's positive law in the digital space. Based on the United Nations Convention on the Rights of the Child (CRC) which has been ratified by Indonesia through Presidential Decree Number 36 of 1990, and translated into Law Number 35 of 2014 concerning Child Protection, every child has the right to protection from all forms of violence including violence mediated by digital technology. The three fundamental rights of children in the digital space that are the focus of discussion are: (1) the right to protection from digital exploitation and violence; (2) the right to privacy and security of personal data as stipulated in Law Number 27 of 2022 concerning Personal Data Protection; and (3) the right to access information that is safe and in accordance with the stages of age development.

b. Forms of Cyberbullying

The second material describes the taxonomy of cyberbullying systematically based on the categorization developed by Willard (2007) and adapted to the Indonesian legal context. The forms of cyberbullying discussed include: (1) flaming, which is the sending of aggressive, abusive, and offensive messages addressed to someone online; (2) harassment, which is the repeated sending of harassing messages; (3) cyberstalking, which is sending messages that threaten and cause fear to the victim; (4) denigration (digital defamation), which is the spread of false information or embarrassing information about a person online; (5) impersonation (identity forgery), which is pretending to be someone else to damage his reputation; (6) outing and trickery, namely the dissemination of embarrassing personal information without permission; and (7) exclusion, which is the exclusion of a person from an online community or group intentionally and repeatedly.

c. Forms of Cybercrime against Children

The third material discusses various forms of cybercrime that specifically target children as victims: (1) phishing that takes advantage of children's innocence to steal personal data or account information; (2) online fraud that lures certain gifts, jobs, or opportunities; (3) grooming, which is the process of conditioning carried out by sexual predators through digital platforms to approach and manipulate children for the purpose of sexual exploitation; (4) Child Sexual Abuse Material (CSAM), which is the production, distribution, or possession of sexual exploitation material involving children; and (5) digital identity theft that utilizes children's data for criminal purposes. Participants gained a deep understanding of the modus operandi of each of these crimes as well as the warning signs that need to be watched out.

3.3 Children's Legal Protection Regulations

The fourth material session provided a comprehensive understanding of the regulatory framework for child protection in the digital space in Indonesia. Participants are introduced to the relevant regulatory hierarchy:

1) Law Number 35 of 2014 concerning Amendments to Law Number 23 of 2002 concerning Child Protection, which is the main legal basis for the protection of children from various forms of violence and exploitation, including digital-based ones.
2) Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), which regulates various criminal acts in cyberspace including digital defamation, dissemination of immoral content, threats through electronic media, and various forms of digital fraud.
3) Law Number 44 of 2008 concerning Pornography which specifically regulates child sexual exploitation material (child pornography) with the threat of severe criminal sanctions for the perpetrators.
4) Law Number 27 of 2022 concerning Personal Data Protection which provides protection for children's personal data and regulates the obligations of digital platform managers in protecting the privacy of their users, including child users.
5) Regulation of the Minister of Communication and Information Technology Number 2 of 2024 concerning the Classification and Security of Internet Content which regulates the mechanism for blocking harmful content including CSAM and content that damages children's development.

3.4 Results of Activity Evaluation

A comprehensive evaluation of the improvement of participants' competencies is carried out through pre-test and post-test instruments that include six main competency indicators. The results of the evaluation are presented in the following table:

Table 1. Pre-test and Post-test Results of Activity Participants

Competency Indicators	Pre-test	Post-test	Improvement	Categories
Understanding Children's Rights in the Digital Space	36%	84%	+48%	Excellent
Knowledge of Forms of Cyberbullying	40%	89%	+49%	Excellent
Understanding Child Protection Regulations (UU ITE, UUPA)	32%	82%	+50%	Excellent
Cybercrime Identification Capabilities Against Children	38%	86%	+48%	Excellent
Knowledge of Cybercrime Reporting Mechanisms	28%	80%	+52%	Excellent
Understanding the Legal Consequences of Cyberbullying Perpetrators	34%	85%	+51%	Excellent
Overall Average	**34,7%**	**84,3%**	**+49,6%**	**Excellent**

Source: Primary data on the results of service activities (2025)

The data in Table 1 show a very significant increase in all competency indicators. The highest increase occurred in the indicators of knowledge of cybercrime reporting mechanisms (from 28% to 80%, up +52 percentage points) and understanding of the legal consequences of cyberbullying perpetrators (from 34% to 85%, up +51 percentage points). These two indicators previously had the lowest pre-test scores, confirming the preliminary survey findings that procedural aspects and legal consequences constitute the most critical knowledge gaps among

the public. The average overall increase of 49.6 percentage points exceeded the target of the success indicator set by 40 points.

Table 2. Activity Participant Satisfaction Survey Results

Evaluation Aspects	Very satisfied	Satisfied	Enough	Less
Relevance of the Material to the Needs of the Participants	74%	20%	6%	0%
Quality of Delivery of Legal Materials	70%	24%	6%	0%
Resource Person/Facilitator Ability	80%	16%	4%	0%
FGD Session and Case Discussion	68%	26%	6%	0%
Simulation of Handling Cyberbullying Cases	72%	22%	6%	0%
Personal Legal Consultation Session	76%	18%	6%	0%
Facilities and Facilities of Activities	62%	28%	10%	0%

Source: Primary data on the results of service activities (2025)

The results of the satisfaction survey in Table 2 show an overall satisfaction level of 94% in the satisfied and very satisfied categories, exceeding the target of 85%. The aspect of the ability of the resource persons and facilitators received the highest rating (80% very satisfied), followed by the aspect of personal legal consultation sessions (76% very satisfied). The high assessment in these two aspects reflects the competence of the resource team recognized by the participants and the relevance of the consultation session in answering the specific legal needs of the participants.

3.5 Program Impact

In addition to measurable knowledge improvements through pre-tests and post-tests, the program resulted in significant changes in participants' orientation and behavior regarding digital child protection, as presented in the following table:

Table 3. The Impact of the Program on Participants' Digital Awareness and Behavior

Program Impact Indicators	Before	After	Changes
Able to identify cyberbullying in their environment	42%	90%	+48%
Knowing how to report cybercrime to the National Police/BSSN	20%	78%	+58%
Have rules for using the internet in your family/school	35%	72%	+37%
Willing to be an anti-cyberbullying agent in their environment	48%	92%	+44%
Understanding the ITE Law and sanctions for cyberbullying perpetrators	25%	83%	+58%

Source: Primary data on the results of service activities (2025)

The data in Table 3 reveal very significant changes in all aspects of the impact measured. The highest increase occurred in the two aspects that previously had the lowest scores: the ability to know how to report cybercrime (from 20% to 78%, up +58%) and understanding the ITE Law and its sanctions (from 25% to 83%, up +58%). The increasing willingness of participants to

become anti-cyberbullying agents (from 48% to 92%) is the most strategic impact indicator, as it reflects the transformation of participants from mere recipients of information to potential ambassadors of change who are ready to actively contribute to building a safer digital ecosystem in their communities.

3.6 Supporting Factors and Constraints

a. Supporting Factors

The success of this activity is supported by several key factors: First, strong institutional support from the Dean and the entire ranks of the UISU Faculty of Law that provides facilities, human resources, and institutional legitimacy for this program. Second, the enthusiasm and openness of the participants was very high, especially from high school/vocational students who welcomed the issue of cyberbullying as a topic that is very relevant to their daily experiences. Third, the high competence of the resource persons and the ability to convey complex legal materials in a language that is easily understood by various segments of participants. Fourth, the involvement of resource persons from the North Sumatra Regional Police Cyber Directorate who provided practical perspectives on cyber law enforcement and actual reporting procedures.

b. Constraints

There are several obstacles faced in the implementation of activities: First, the limited training time results in the depth of discussion of several materials, especially the technical aspects of digital forensics and the procedure of cyber criminal procedural law, must be simplified. Second, the heterogeneity of the level of education and understanding of participants (from high school students to teachers and adult parents) demands adaptation of delivery styles that cannot always be optimal for all segments simultaneously. Third, not all participants had access to digital devices during interactive digital education sessions, so some participants had to observe rather than practice in person.

3.7 Discussion

The results of this service activity provide empirical confirmation of theoretical arguments about the importance of digital legal literacy as a preventive instrument in child protection in cyberspace. The increase in participants' understanding by an average of 49.6 percentage points is consistent with the findings of Hidayat et al. (2023) which show that experiential legal education programs are able to significantly increase participants' legal literacy in the short term. The success of the case simulation session, in which 82% of participants successfully demonstrated the reporting procedure correctly, supported a competency-based pedagogical approach that emphasized the importance of practical skills in addition to theoretical knowledge. These findings are in line with the principles of Clinical Legal Education put forward by Bloch (2011), which emphasizes that true legal understanding can only be achieved through direct experience of applying knowledge in real-world simulations.

From the perspective of child protection theory, the results of this activity strengthen the argument that the preventive approach through education is much more effective and efficient than the reactive approach through law enforcement alone. This is in line with the principle of the best interest of the child which is the basis of the Convention on the Rights of the Child and is adopted in the Indonesian child protection legal system, which places prevention as the top priority over enforcement (Nashriana, 2023). The increase in participants' willingness to become anti-cyberbullying agents (from 48% to 92%) was the most strategically significant finding. This indicates that a well-designed educational program is not only able to transfer knowledge, but also catalyze the moral transformation and social commitment of participants to actively contribute to building a safer digital ecosystem. This change in orientation is in line with the Social Cognitive Theory theory put forward by Bandura (1986), specifically the concepts of

self-efficacy and collective efficacy that encourage individuals to take proactive action when they feel they have adequate social capacity and support.

3.8 Program Sustainability

To ensure that the impact of this activity does not stop at one implementation, the service team has designed several follow-up programs that will be implemented in the next six months:

1) Digital Legal Consultation Clinic: The establishment of a free legal consultation service specifically handling cases of cyberbullying and cybercrime involving children, which will be operated by law students of FH UISU under the supervision of the teaching lecturer.
2) Digital-Friendly Schools: A program of visits to partner schools to carry out mini-workshops on digital child protection for students, teachers, and parents in an integrated manner.
3) Formation of Anti-Cyberbullying Ambassadors: Recruitment and training of outstanding students from partner schools as Anti-Cyberbullying Ambassadors who will actively educate peers in their respective school environments.
4) Periodic Legal Assistance: Legal assistance services for cyberbullying victims and their families in taking the process of reporting and handling cases officially.

4. ACTIVITY DOCUMENTATION

Documentation of activities is carried out systematically at all stages of implementation for the purposes of academic reporting, program evaluation, and dissemination of best practices to a wider range of stakeholders.

Figure 2. Group Photo of Participants and Service Team

5. CONCLUSIONS AND SUGGESTIONS

Community service activities in the form of education on child legal protection in the digital era to prevent cyberbullying and cybercrime carried out by the Faculty of Law UISU have succeeded in achieving all the established success indicators:

1) There has been a very significant increase in digital legal literacy, with an average pre-test score of 34.7% increasing to 84.3% in the post-test, resulting in an average increase of 49.6 percentage points which far exceeds the target of at least 40 points.
2) A total of 82% of participants (41 out of 50 people) successfully demonstrated the procedure for reporting cyberbullying cases correctly in the simulation session, exceeding the target of 75%.

3) The satisfaction level of participants reached 94% in the satisfied and very satisfied category, exceeding the minimum target of 85%.
4) There was a significant change in the orientation and commitment of participants, reflected in the increase in willingness to become an anti-cyberbullying agent from 48% to 92%.
5) This activity proves that legal education that is designed in a participatory, contextual, and practical skills-oriented manner is an effective instrument in building a safe and responsible digital culture, especially for child protection.

Suggestions:

1) To Parents: It is recommended to increase active involvement in assisting children's internet use, build open communication about children's digital experiences, and do not hesitate to report cases of cyberbullying that befall children to schools, KPAI, or law enforcement officials.
2) To Schools: It is recommended to integrate digital legal literacy materials into the counseling and extracurricular guidance curriculum, establish an Anti-Cyberbullying Task Force Team in schools, and build formal cooperation with FH UISU for an ongoing student legal assistance program.
3) To Higher Education (FH UISU): It is recommended to institutionalize the Digital Legal Clinic as a permanent service unit, incorporate cyber law and digital child protection materials into the mandatory curriculum of law students, and develop advanced research to measure the long-term impact of this educational program.
4) To Local Governments: It is recommended to allocate a special budget for programs to increase people's digital legal literacy, strengthen the capacity of the Integrated Child Protection Unit (UPAT) at the sub-district level, and facilitate cross-sector collaboration between universities, schools, law enforcement officials, and the community in building a safe digital ecosystem for children.
5) To Law Enforcement Officials: It is recommended to increase the accessibility of cybercrime reporting mechanisms for child victims and their families, strengthen the capacity of the National Police Cyber Unit at the Police and Police levels, and actively participate in community legal education programs.
6) To the Next PkM Researchers and Implementers: It is recommended to develop a longitudinal research design to measure the long-term impact of the program on participants' digital behavior, expand the scope of the target to groups of children under secondary school age, and develop educational modules based on digital technology (animated videos, mobile applications) that can be disseminated more massively.

6. BIBLIOGRAPHY

[1] Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Prentice-Hall.
[2] Bloch, F. S. (Ed.). (2011). The global clinical movement: Educating lawyers for social justice. Oxford University Press.
[3] National Cyber and Cryptography Agency (BSSN). (2024). Indonesia's cybersecurity annual report 2023. BSSN of the Republic of Indonesia.

[4] Hidayat, A., Nugroho, B., & Ramadhani, C. (2023). The effectiveness of experiential legal education programs in improving people's digital legal literacy. Journal of Legal and Human Rights Education, 11(2), 89-107. https://doi.org/10.20885/jpham.vol11.iss2.art5
[5] Indonesian Child Protection Commission (KPAI). (2024). Child protection complaint data in the field of pornography and cybercrime 2022-2023. KPAI of the Republic of Indonesia.
[6] Nashriana. (2023). Criminal law protection for children in Indonesia (4th edition). PT RajaGrafindo Persada.
[7] Regulation of the Minister of Communication and Information Technology Number 2 of 2024 concerning the Classification and Security of Internet Content. (2024). Ministry of Communication and Information of the Republic of Indonesia.
[8] Prasetyo, B., & Andayani, T. R. (2022). Cyberbullying in Indonesian adolescents: Prevalence, characteristics, and psychological impact. Journal of Social Psychology, 20(1), 45-62. https://doi.org/10.7454/jps.2022.5
[9] Raharjo, S. T., & Astuti, S. I. (2023). Legal protection of children victims of cybercrime: A normative and empirical analysis in Indonesia. Journal of Law IUS QUIA IUSTUM, 30(3), 521-545. https://doi.org/10.20885/iustum.vol30.iss3.art4
[10] Sitompul, A. (2022). Internet law and user protection in Indonesia (revised edition). CV Utomo.
[11] Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. (2016). Government of the Republic of Indonesia.
[12] Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection. (2022). Government of the Republic of Indonesia.
[13] Law of the Republic of Indonesia Number 35 of 2014 concerning Amendments to Law Number 23 of 2002 concerning Child Protection. (2014). Government of the Republic of Indonesia.
[14] We Are Social & Hootsuite. (2024). Digital 2024: Indonesia. https://datareportal.com/reports/digital-2024-indonesia
[15] Willard, N. E. (2007). Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress. Research Press.
[16] Justice, T. V. (2022). Compilation of child protection and cybercrime laws in Indonesia. Judiciary Library.