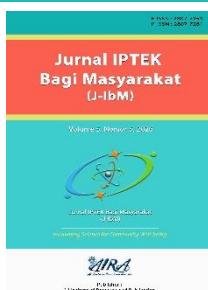


Data Security and Privacy Education in the Artificial Intelligence Era through Digital Literacy

(*Edukasi Keamanan Data dan Privasi di Era Kecerdasan Buatan melalui Literasi Digital Sekolah Dasar*)



Yuniar Andi Astuti ^{a,1*}, Ester Hervina Sihombing ^{a,2}, Sujarwo ^{a,3}, Sondang ^{a,4}, Berupilih Br Ginting ^{a,5}, Mega Puspita Sari ^{b,6}

^a Politeknik Unggul LP3M, Medan, 20156, Indonesia

^b Universitas Medan Area, Medan, 20141, Indonesia

E-mail: ¹zulia020174@gmail.com; ²sieran271328@gmail.com; ³sujarwo2268@gmail.com;
⁴sondang@politeknikunggul.ac.id; ⁵berupilihenginting69@gmail.com; ⁶mega@staff.uma.ac.id;

*Corresponding Author.

E-mail address: andiyuniar45@gmail.com (Y.A. Astuti).

Received: January 9, 2026 | Revised: January 30, 2026 | Accepted: February 2, 2026

Abstract: The development of artificial intelligence (AI) technology has brought significant changes to various aspects of life. However, it has also given rise to serious challenges related to data security and user privacy protection. The low level of digital literacy among the public, particularly in understanding the risks of data breaches and the misuse of personal information, has increased vulnerability to cybercrime in the digital era. This community service activity aims to enhance public knowledge, awareness, and skills in safeguarding data security and privacy amid the rapid adoption of AI-based technologies. The activity was implemented using an educational and participatory approach through workshops, interactive lectures, discussions, case simulations, and hands-on practice in securing digital accounts. The program involved 20 participants consisting of teachers and staff at SD Negeri 060922 Medan. Evaluation was conducted through pre-tests and post-tests to measure improvements in participants' understanding. The results indicate an average increase in participants' knowledge of 40%, along with heightened awareness of the importance of password management, privacy settings, and vigilance against cyber threats. This activity demonstrates that community-based education on data security and privacy is effective in improving digital literacy and fostering safer and more responsible technology use behaviors. Therefore, similar initiatives should be carried out on a sustained basis to support the development of a secure, ethical, and adaptive digital ecosystem in response to advancements in artificial intelligence.

Keywords: artificial intelligence; community service; data security; digital literacy; digital privacy.

Abstrak: Perkembangan teknologi kecerdasan buatan (Artificial Intelligence [AI]) telah membawa perubahan signifikan dalam berbagai aspek kehidupan. Namun, perkembangan tersebut juga memunculkan tantangan serius terkait keamanan data dan perlindungan privasi pengguna. Rendahnya literasi digital masyarakat, khususnya dalam memahami risiko kebocoran data dan penyalahgunaan informasi pribadi, meningkatkan tingkat kerentanan terhadap kejahatan siber di era digital. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan pengetahuan, kesadaran, serta keterampilan masyarakat dalam menjaga keamanan data dan privasi di tengah pesatnya pemanfaatan teknologi berbasis AI. Metode pelaksanaan kegiatan menggunakan pendekatan edukatif dan partisipatif melalui workshop, ceramah interaktif, diskusi, simulasi kasus, serta praktik langsung pengamanan akun digital. Kegiatan ini melibatkan 20 peserta yang terdiri atas guru dan pegawai di SD Negeri 060922 Medan. Evaluasi kegiatan dilakukan melalui pre-test dan post-test untuk mengukur peningkatan pemahaman peserta. Hasil kegiatan menunjukkan adanya peningkatan rata-rata pengetahuan peserta sebesar 40%, disertai meningkatnya kesadaran terhadap pentingnya pengelolaan kata sandi, pengaturan



privasi, serta kewaspadaan terhadap berbagai ancaman siber. Kegiatan ini menunjukkan bahwa edukasi keamanan data dan privasi berbasis masyarakat efektif dalam meningkatkan literasi digital serta membentuk perilaku penggunaan teknologi yang lebih aman dan bertanggung jawab. Oleh karena itu, kegiatan serupa perlu dilaksanakan secara berkelanjutan guna mendukung terciptanya ekosistem digital yang aman, beretika, dan adaptif terhadap perkembangan kecerdasan buatan.

Kata kunci: kecerdasan buatan; keamanan data; literasi digital; pengabdian kepada masyarakat; privasi digital.

Pendahuluan

Perkembangan teknologi digital yang sangat pesat, khususnya dalam bidang kecerdasan buatan (*Artificial Intelligence/AI*), telah membawa perubahan fundamental dalam berbagai sektor kehidupan manusia, termasuk pendidikan, bisnis, dan pelayanan publik (OECD, 2025). Pemanfaatan teknologi AI dinilai mampu meningkatkan efisiensi, kecepatan pengambilan keputusan, serta kualitas layanan berbasis data di berbagai organisasi (Dwivedi et al., 2021). Dalam konteks kewirausahaan, kehadiran platform digital, media sosial, dan marketplace memungkinkan pelaku usaha memulai bisnis tanpa harus memiliki toko fisik (Gani et al., 2025).

Namun demikian, kemajuan teknologi AI juga memunculkan tantangan serius terkait keamanan data dan perlindungan privasi pengguna (Floridi & Cowls, 2021). Sistem berbasis AI memiliki kemampuan untuk mengumpulkan, menyimpan, dan menganalisis data dalam skala besar, sehingga meningkatkan risiko penyalahgunaan data pribadi apabila tidak diimbangi dengan regulasi dan kesadaran pengguna (ENISA, 2023). Risiko tersebut mencakup kebocoran data, pengawasan berlebihan (*surveillance*), serta eksplorasi data untuk kepentingan komersial tanpa persetujuan pemilik data (Solove, 2021).

Di era digital saat ini, data pribadi telah menjadi aset bernilai tinggi yang sering menjadi target kejahatan siber dan penyalahgunaan informasi (Utami et al., 2025). Kasus pelanggaran data pribadi di Indonesia menunjukkan bahwa lemahnya perlindungan data dapat menimbulkan kerugian material, psikologis, dan sosial bagi individu maupun institusi (Utami et al., 2025). Kompleksitas permasalahan ini semakin meningkat seiring dengan kemampuan AI dalam melakukan analisis prediktif terhadap perilaku pengguna (Zuboff, 2022).

Keamanan data juga memiliki dimensi strategis dalam konteks keamanan nasional karena ancaman siber dapat berasal dari aktor negara maupun non-negara lintas batas wilayah (Ramadhan & Atmam, 2025). Oleh karena itu, penguatan keamanan siber tidak hanya menjadi tanggung jawab pemerintah, tetapi juga membutuhkan partisipasi aktif masyarakat sebagai pengguna teknologi (OECD, 2025).

Sayangnya, tingkat literasi digital masyarakat Indonesia, khususnya pada aspek keamanan data dan privasi, masih tergolong rendah (Kementerian Kominfo RI, 2023). Banyak pengguna teknologi digital belum memahami pentingnya pengelolaan kata sandi yang kuat, pengaturan privasi akun, serta risiko memberikan izin akses data pada aplikasi yang tidak terpercaya (Saputra, 2024). Rendahnya literasi digital tersebut berkontribusi langsung terhadap meningkatnya potensi kebocoran data dan manipulasi informasi (Park, 2023).

Berdasarkan kondisi tersebut, kegiatan pengabdian kepada masyarakat ini dilaksanakan untuk meningkatkan kesadaran dan pemahaman masyarakat mengenai keamanan data dan privasi di era kecerdasan buatan (UNESCO, 2023). Edukasi keamanan digital dipandang sebagai pendekatan yang efektif untuk membangun perilaku penggunaan teknologi yang aman, etis, dan bertanggung jawab (Rahardjo, 2022).

Artikel pengabdian kepada masyarakat ini memberikan kontribusi praktis berupa model edukasi literasi digital yang aplikatif dan sesuai dengan karakteristik siswa sekolah dasar dalam meningkatkan pemahaman keamanan data dan privasi di era kecerdasan buatan (AI). Selain itu, secara akademik, artikel ini berkontribusi dengan menyediakan instrumen pre-test dan post-test yang terstruktur, serta menyajikan bukti empiris peningkatan literasi digital siswa melalui pendekatan edukasi berbasis sekolah dasar. Temuan dalam artikel ini

diharapkan dapat menjadi referensi bagi peneliti, pendidik, dan pelaksana PKM dalam mengembangkan program literasi digital serupa yang berkelanjutan dan adaptif terhadap perkembangan teknologi.

Metode

Kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan edukatif dan partisipatif karena metode tersebut terbukti efektif dalam meningkatkan literasi digital masyarakat (UNESCO, 2023). Pendekatan partisipatif memungkinkan peserta tidak hanya menerima informasi secara pasif, tetapi juga terlibat aktif dalam memahami risiko dan solusi keamanan digital (Park, 2023). Materi pelatihan dirancang mencakup konsep dasar keamanan data, perlindungan privasi, serta ancaman siber yang umum terjadi di era AI (ENISA, 2023). Praktik langsung seperti pembuatan kata sandi yang kuat dan pengaturan privasi akun dipilih karena sesuai dengan prinsip *privacy by design* (Cavoukian, 2022).

Evaluasi kegiatan dilakukan melalui pre-test dan post-test untuk mengukur peningkatan pengetahuan peserta secara kuantitatif (World Economic Forum, 2024). Metode evaluasi ini lazim digunakan dalam program literasi digital berbasis komunitas karena mampu menunjukkan efektivitas intervensi edukatif (Rahardjo, 2022).

Instrumen yang digunakan dalam kegiatan pengabdian kepada masyarakat ini berupa kuesioner pre-test dan post-test yang terdiri dari 20 butir pernyataan dengan skala Likert lima tingkat. Instrumen tersebut dirancang untuk mengukur empat aspek utama, yaitu pemahaman keamanan data, kesadaran privasi digital, literasi dasar kecerdasan buatan (AI), serta sikap dan perilaku aman dalam penggunaan teknologi digital. Pre-test diberikan sebelum pelaksanaan kegiatan edukasi untuk mengidentifikasi tingkat pemahaman awal siswa, sedangkan post-test dilaksanakan setelah kegiatan untuk mengetahui peningkatan pemahaman dan perubahan sikap sebagai dampak dari program literasi digital berbasis sekolah dasar yang dilaksanakan. Adapun keterbatasan metode dalam kegiatan ini antara lain jumlah peserta yang relatif terbatas serta cakupan lokasi kegiatan yang masih bersifat lokal, sehingga hasil yang diperoleh belum dapat digeneralisasikan secara luas. Selain itu, pengukuran dilakukan dalam jangka waktu yang relatif singkat, sehingga belum sepenuhnya mencerminkan keberlanjutan perubahan perilaku siswa dalam jangka panjang. Meskipun demikian, temuan yang dihasilkan tetap memberikan gambaran empiris awal mengenai efektivitas edukasi keamanan data dan privasi di era kecerdasan buatan (AI) pada tingkat sekolah dasar.

Sasaran Kegiatan

Sasaran kegiatan ini adalah guru dan pegawai SD Negeri 060922 Medan yang memiliki aktivitas penggunaan teknologi digital dalam pekerjaan dan kehidupan sehari-hari, khususnya yang berisiko terhadap keamanan data dan privasi digital.

Tahapan Pelaksanaan

Kegiatan ini terdiri atas beberapa tahapan sebagai berikut:

a. Tahap Persiapan

Pada tahap ini tim pelaksana melakukan koordinasi dengan pihak mitra untuk menentukan sasaran peserta dan kebutuhan teknis kegiatan. Disiapkan pula materi pelatihan yang mencakup konsep dasar keamanan data, kebijakan privasi digital, serta ancaman siber yang sering terjadi di era AI. Tim juga menyiapkan alat bantu seperti laptop, proyektor, dan modul pelatihan.

b. Tahap Pelaksanaan

Pelaksanaan kegiatan dilakukan dalam bentuk workshop dan edukasi interaktif yang mencakup beberapa sesi berikut:

1. Sesi I – Pengenalan Keamanan Data dan Privasi Digital

- Menjelaskan tentang pentingnya melindungi data pribadi, jenis-jenis data sensitif, serta dampak kebocoran data di era kecerdasan buatan.
2. Sesi II – Ancaman Siber dan Etika Penggunaan AI
Membahas bentuk-bentuk ancaman seperti *phishing*, *malware*, *data scraping*, dan penyalahgunaan algoritma AI terhadap privasi individu.
 3. Sesi III – Praktik Keamanan Digital Dasar
Peserta dilatih secara langsung untuk membuat kata sandi kuat, mengaktifkan autentikasi dua langkah, memverifikasi sumber informasi, serta mengatur privasi pada akun media sosial.
 4. Sesi IV – Diskusi dan Tanya Jawab
Peserta diberikan kesempatan untuk berdiskusi mengenai pengalaman mereka dalam menghadapi permasalahan digital serta mencari solusi bersama dengan fasilitator.

Tahap Evaluasi

Evaluasi kegiatan dilakukan melalui pre-test dan post-test untuk mengukur peningkatan pengetahuan peserta sebelum dan sesudah pelatihan. Selain itu, dilakukan juga survei kepuasan untuk mengetahui efektivitas kegiatan serta harapan peserta terhadap pelatihan serupa di masa mendatang.

Tahap Tindak Lanjut

Sebagai tindak lanjut, tim pelaksana menyediakan materi digital dan panduan keamanan data yang dapat diakses oleh peserta. Peserta juga diarahkan untuk membentuk kelompok kecil sebagai agen literasi digital di lingkungan masing-masing, guna menyebarluaskan pemahaman tentang keamanan data dan privasi.

Metode Pendekatan

Metode yang digunakan dalam kegiatan ini meliputi:

1. Ceramah interaktif, untuk memberikan pemahaman konseptual.
2. Demonstrasi langsung, untuk memperlihatkan langkah-langkah perlindungan data.
3. Diskusi kelompok dan simulasi kasus, agar peserta mampu mengidentifikasi dan mengatasi ancaman digital secara nyata.

Pendampingan dan konsultasi, untuk membantu peserta dalam mengimplementasikan praktik keamanan digital di perangkat masing-masing.

Hasil

Pelaksanaan Kegiatan

Kegiatan pengabdian kepada masyarakat ini dilaksanakan dengan tujuan untuk meningkatkan kesadaran dan pemahaman masyarakat mengenai pentingnya keamanan data dan privasi di tengah pesatnya perkembangan teknologi kecerdasan buatan (AI). Kegiatan pengabdian kepada masyarakat ini diikuti oleh sekitar 20 peserta yang terdiri dari guru dan pegawai SD Negeri 060922 Medan .

Kegiatan dimulai dengan sesi pembukaan oleh pihak panitia dan sambutan dari kepala sekolah SD Negeri 060922 Medan. Setelah itu dilanjutkan dengan pemaparan materi oleh tim pelaksana. Materi disampaikan secara interaktif melalui ceramah, diskusi, simulasi, dan praktik langsung, sehingga peserta tidak hanya memahami teori tetapi juga memperoleh pengalaman praktis dalam menjaga keamanan data pribadi di dunia digital.

Selama pelatihan, peserta diberikan materi edukatif seperti:

1. Pengertian dan jenis data pribadi yang perlu dijaga.
2. Cara mengenali situs atau aplikasi yang tidak aman.
3. Strategi membuat kata sandi yang kuat dan mengelola akun digital.
4. Teknik pengaturan privasi di media sosial.

5. Penjelasan tentang dampak negatif penyalahgunaan data oleh sistem berbasis AI.

Hasil Kegiatan

Hasil dari kegiatan pengabdian ini menunjukkan beberapa capaian penting, antara lain:

1. Peningkatan Pengetahuan Peserta

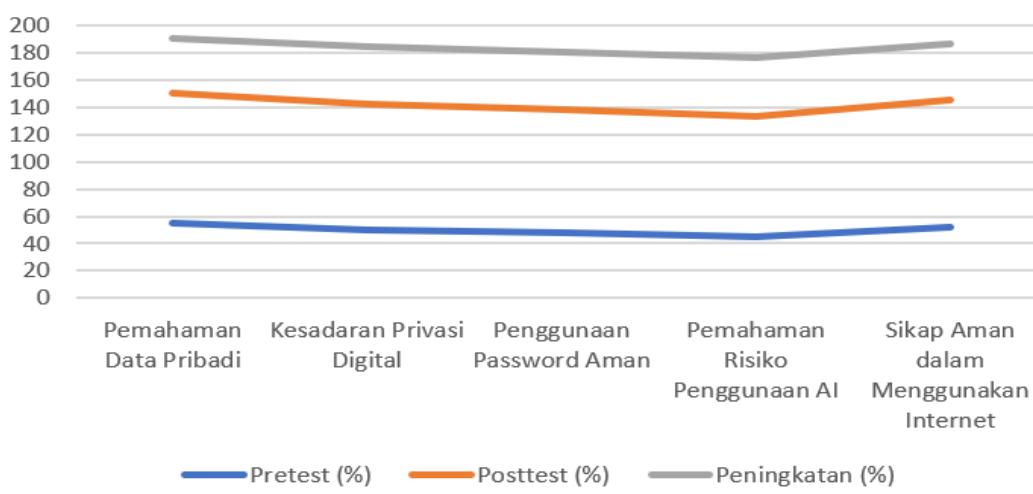
Berdasarkan hasil pre-test dan post-test, terjadi peningkatan pengetahuan peserta sebesar rata-rata 40% setelah mengikuti kegiatan. Hal ini menunjukkan bahwa pelatihan berhasil meningkatkan literasi digital masyarakat terkait keamanan data dan privasi.

Berikut tabel dan grafik perbandingan nilai pretest dan posttest:

Tabel 1. Hasil Pretest dan Posttest Literasi Keamanan Data dan Privasi Siswa SD

No	Komponen Penilaian	Pretest (%)	Posttest (%)	Peningkatan (%)
1	Pemahaman Data Pribadi	55	95	40
2	Kesadaran Privasi Digital	50	92	42
3	Penggunaan Password Aman	48	90	42
4	Pemahaman Risiko Penggunaan AI	45	88	43
5	Sikap Aman dalam Menggunakan Internet	52	93	41
	Rata-rata	50,0	91,6	41,6

Sumber: Data Olahan



Gambar 1. Perbandingan Hasil Pre-test dan Post-test

2. Peningkatan Kesadaran terhadap Privasi Digital

Sebelum kegiatan, sebagian besar peserta belum memahami bahwa data pribadi seperti foto, lokasi, dan riwayat pencarian dapat dimanfaatkan oleh pihak ketiga. Setelah mengikuti kegiatan, peserta mengaku lebih berhati-hati dalam memberikan izin akses data kepada aplikasi dan lebih selektif dalam membagikan informasi pribadi secara online.

3. Kemampuan Praktis Peserta

Peserta mampu mempraktikkan langkah-langkah perlindungan dasar seperti mengaktifkan autentikasi dua langkah, mengelola kata sandi, dan mengatur privasi akun media sosial. Beberapa peserta juga mulai menerapkan kebiasaan baru seperti rutin mengganti kata sandi dan memverifikasi sumber informasi sebelum membagikannya.

4. Dampak Sosial

Kegiatan ini juga berdampak positif terhadap peningkatan kesadaran kolektif masyarakat sekitar. Setelah pelatihan, beberapa peserta berinisiatif membentuk kelompok kecil untuk berbagi pengetahuan tentang keamanan digital di lingkungan

sekolah dan kantor desa mereka.



Gambar 2. Ketua Tim Pengabdian memberikan arahan

Diskusi

Kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan edukatif dan partisipatif karena metode tersebut terbukti efektif dalam meningkatkan literasi digital masyarakat (UNESCO, 2023). Pendekatan ini dirancang untuk menciptakan suasana pembelajaran yang interaktif, sehingga peserta tidak hanya berperan sebagai penerima informasi, tetapi juga sebagai subjek aktif dalam proses pembelajaran. Melalui keterlibatan langsung, peserta didorong untuk mengidentifikasi permasalahan keamanan digital yang mereka hadapi serta mendiskusikan solusi yang sesuai dengan konteks penggunaan teknologi sehari-hari.

Pendekatan partisipatif memungkinkan peserta tidak hanya menerima informasi secara pasif, tetapi juga terlibat aktif dalam memahami risiko dan solusi keamanan digital (Park, 2023). Keterlibatan aktif tersebut diharapkan dapat meningkatkan daya serap materi sekaligus membangun kesadaran kritis peserta terhadap pentingnya perlindungan data pribadi dan privasi digital. Dengan demikian, peserta mampu mengaitkan materi yang disampaikan dengan pengalaman nyata yang mereka alami dalam aktivitas digital sehari-hari.

Materi pelatihan dirancang mencakup konsep dasar keamanan data, perlindungan privasi, serta ancaman siber yang umum terjadi di era AI (ENISA, 2023). Penyampaian materi disusun secara bertahap dan sistematis agar mudah dipahami oleh peserta dengan latar belakang pengetahuan yang beragam. Materi juga disesuaikan dengan kebutuhan praktis peserta sehingga dapat langsung diterapkan dalam penggunaan perangkat digital, baik di lingkungan kerja maupun dalam kehidupan pribadi.

Praktik langsung seperti pembuatan kata sandi yang kuat dan pengaturan privasi akun dipilih karena sesuai dengan prinsip *privacy by design* (Cavoukian, 2022). Melalui praktik ini, peserta tidak hanya memahami konsep secara teoritis, tetapi juga memperoleh pengalaman langsung dalam menerapkan langkah-langkah pengamanan data. Pendekatan praktik ini diharapkan mampu membentuk kebiasaan baru yang lebih aman dalam pengelolaan akun dan informasi pribadi.

Evaluasi kegiatan dilakukan melalui pre-test dan post-test untuk mengukur peningkatan pengetahuan peserta secara kuantitatif (World Economic Forum, 2024). Instrumen evaluasi disusun untuk menggambarkan tingkat pemahaman peserta sebelum dan sesudah kegiatan berlangsung. Hasil evaluasi digunakan untuk menilai efektivitas pelaksanaan kegiatan serta sebagai bahan refleksi dalam perbaikan dan pengembangan program serupa di masa mendatang.

Metode evaluasi ini lazim digunakan dalam program literasi digital berbasis komunitas karena mampu menunjukkan efektivitas intervensi edukatif (Rahardjo, 2022). Pendekatan evaluasi tersebut memberikan gambaran yang objektif mengenai dampak kegiatan terhadap peningkatan literasi digital peserta. Selain itu, hasil evaluasi menjadi dasar dalam merumuskan rekomendasi keberlanjutan kegiatan pengabdian kepada masyarakat di bidang keamanan data dan privasi digital.

Berdasarkan hasil pelaksanaan kegiatan, program edukasi keamanan data dan privasi di era kecerdasan buatan (AI) direkomendasikan untuk direplikasi di sekolah dasar lain dengan mengadopsi model pelaksanaan yang terstruktur, yaitu melalui tahapan pre-test, penyampaian materi interaktif, simulasi kasus sederhana, dan post-test. Replikasi kegiatan dapat dilakukan dengan menyesuaikan materi pada tingkat kelas serta memanfaatkan media pembelajaran yang kontekstual dan ramah anak, seperti video edukatif, permainan edukasi digital, dan studi kasus sederhana yang relevan dengan aktivitas digital siswa sehari-hari.

Selain itu, diperlukan peran aktif pemangku kepentingan dalam mendukung keberlanjutan program literasi digital. Pihak sekolah berperan dalam mengintegrasikan materi keamanan data dan privasi ke dalam kegiatan pembelajaran atau ekstrakurikuler, guru sebagai fasilitator pendamping, serta orang tua dalam melakukan pengawasan dan penguatan perilaku aman digital di lingkungan rumah. Pemerintah daerah dan dinas pendidikan diharapkan dapat mendukung melalui penyusunan kebijakan, pelatihan guru, serta penyediaan modul literasi digital berbasis usia. Kolaborasi antara perguruan tinggi, sekolah, dan pemerintah daerah menjadi kunci untuk memperluas dampak program serta membangun kesadaran keamanan data dan privasi digital secara berkelanjutan sejak usia dini.

Kesimpulan

Kegiatan pengabdian kepada masyarakat dengan tema Edukasi Keamanan Data dan Privasi di Era Kecerdasan Buatan telah berhasil meningkatkan pengetahuan, kesadaran, dan keterampilan masyarakat dalam menjaga keamanan informasi pribadi di dunia digital. Melalui kegiatan ini, peserta memahami bahwa data pribadi merupakan aset penting yang harus dilindungi dari penyalahgunaan oleh pihak yang tidak bertanggung jawab. Kegiatan ini berhasil meningkatkan pengetahuan, kesadaran, dan keterampilan peserta dalam menjaga keamanan data pribadi di era kecerdasan buatan. Edukasi keamanan data terbukti menjadi instrumen penting dalam membangun masyarakat yang cakap digital dan tangguh terhadap risiko siber.

Hasil evaluasi menunjukkan adanya peningkatan signifikan dalam pemahaman peserta terhadap konsep dasar keamanan digital, jenis ancaman siber, serta langkah-langkah preventif seperti penggunaan kata sandi yang kuat, autentikasi ganda, dan pengaturan privasi di media sosial. Selain itu, peserta juga mampu menerapkan praktik keamanan dasar secara mandiri setelah mengikuti pelatihan. Peningkatan literasi digital diharapkan mampu mengurangi potensi penyalahgunaan data serta mendukung terciptanya ekosistem digital yang aman dan beretika. Dengan demikian, peran perguruan tinggi dalam kegiatan edukasi keamanan digital menjadi sangat strategis dalam menghadapi tantangan transformasi digital berbasis AI.

Kegiatan ini sekaligus menegaskan pentingnya peran perguruan tinggi dalam meningkatkan literasi digital masyarakat, terutama dalam menghadapi tantangan era kecerdasan buatan yang semakin kompleks dan dinamis. Edukasi mengenai keamanan data dan privasi tidak hanya bermanfaat untuk melindungi individu, tetapi juga untuk membangun ekosistem digital yang aman, beretika, dan bertanggung jawab.

Ucapan Terima Kasih

Penulis menyampaikan terima kasih kepada Kepala Sekolah SD Negeri 060922 Medan beserta seluruh guru dan pegawai yang telah berpartisipasi aktif dan memberikan dukungan penuh dalam pelaksanaan kegiatan pengabdian kepada masyarakat ini. Ucapan terima kasih juga disampaikan kepada institusi Politeknik Unggul LP3M yang telah memfasilitasi dan

mendukung pelaksanaan kegiatan, sehingga seluruh rangkaian kegiatan dapat berjalan dengan baik dan lancar.

Pernyataan Konflik Kepentingan

Penulis menyatakan tidak terdapat konflik kepentingan, baik keuangan, profesional, maupun pribadi, yang dapat memengaruhi pelaksanaan kegiatan pengabdian kepada masyarakat dan penulisan artikel ini. Kegiatan ini didanai secara mandiri oleh penulis tanpa melibatkan pihak pendana eksternal, dan seluruh proses pelaksanaan serta pengajuan artikel dilakukan secara independen.

Daftar Pustaka

- Cavoukian, A. (2022). Privacy by design in the age of artificial intelligence. *IEEE Security & Privacy*, 20(2), 90–95. <https://doi.org/10.1109/MSEC.2022.3151354>
- Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., & Williams, M. D. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges. *International Journal of Information Management*, 57, Article 102110. <https://doi.org/10.1016/j.ijinfomgt.2020.102110>
- European Union Agency for Cybersecurity. (2023). *Cybersecurity challenges of artificial intelligence*. <https://www.enisa.europa.eu/topics/artificial-intelligence>
- Floridi, L., & Cowls, J. (2021). A unified framework of five principles for AI in society. *Harvard Data Science Review*, 3(1). <https://doi.org/10.1162/99608f92.8cd550d1>
- Gani, A., Nasution, M., Fadli, Z., & Roy, A. P. S. (2025). *Digitalpreneurship: Create your future: Konsep dan panduan kewirausahaan di era digital marketing*. Global Aksara Pers.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Indeks literasi digital Indonesia 2023*.
- OECD. (2025). *Governing with artificial intelligence*. OECD Publishing. <https://www.oecd.org/digital/artificial-intelligence/>
- Park, Y. J. (2023). Digital literacy and cybersecurity awareness in the AI era. *Telecommunications Policy*, 47(2), Article 102438. <https://doi.org/10.1016/j.telpol.2022.102438>
- Rahardjo, B. (2022). Keamanan informasi di era transformasi digital. *Jurnal Keamanan Siber Indonesia*, 4(1), 1–10.
- Ramadhan, W. P., & Atmam, W. (2025). Peran artificial intelligence dalam meningkatkan keamanan siber suatu negara. *Jurnal Ilmu Sosial*, 21(1), 55–67.
- Saputra, D. F. (2024). Literasi digital untuk perlindungan data pribadi masyarakat. *Jurnal Ilmu Kepolisian*, 18(2), 145–156.
- Solove, D. J. (2021). The myth of privacy in the digital age. *Harvard Law Review Forum*, 134, 1–15. <https://harvardlawreview.org/2021/01/the-myth-of-privacy/>
- UNESCO. (2023). *Ethical implications of artificial intelligence*. <https://www.unesco.org/en/artificial-intelligence/ethics>
- Utami, T. K., Putri, K. A., Suryanto, S. O., & Asriani, F. (2025). Personal data breach cases in Indonesia: Perspective of personal data protection law. *Journal of Customary Law*, 2(2), 21–30. <https://doi.org/10.47134/jcl.v2i2.3742>
- van der Sloot, B. (2022). Data protection and privacy in AI systems. *Computer Law & Security Review*, 45, Article 105112. <https://doi.org/10.1016/j.clsr.2022.105112>
- World Economic Forum. (2024). *Global risks report 2024*. <https://www.weforum.org/reports/global-risks-report-2024>
- Zuboff, S. (2022). Surveillance capitalism and artificial intelligence. *Journal of Information Technology*, 37(1), 1–9. <https://doi.org/10.1177/02683962211044424>