



Workshop Literasi Digital Berbasis KAP dengan Metode Boardgame bagi Mahasiswa UKWMS, Kampus Madiun

Merlina Maria Barbara Apul¹, Finsensius Yuli Purnama²

¹Program Studi Ilmu Komunikasi, Universitas Katolik Widya Mandala Surabaya

Abstrak

Bermula dari kebutuhan Program Studi Bahasa Inggris (PSDKU) Kampus Madiun Universitas Katolik Widya Mandala Surabaya (UKWMS) untuk memberikan pengetahuan dan skill literasi digital bagi mahasiswa, maka dirancang sebuah program pengabdian masyarakat yang berfokus pada workshop keterampilan cek fakta. Workshop ini berfokus pada tiga keterampilan utama yakni cek fakta, perlindungan data pribadi dan etika bermedia digital. **Pertama**, keterampilan cek fakta, bertujuan untuk memberikan pelatihan kepada peserta agar dapat menjadi agen periksa fakta yang terampil, khususnya dalam mengidentifikasi dan melawan penyebaran hoaks. Peserta akan dibekali pengetahuan dan keterampilan bagaimana melakukan periksa fakta. Narasumber akan mengajak peserta mempelajari pengertian hoaks, motif penyebar hoaks, ciri, dampak, dan cara melakukan periksa fakta (video, foto, dan narasi). **Kedua**, keterampilan perlindungan data pribadi bertujuan agar peserta mampu melindungi data dan perangkat dari ancaman kejahatan online. Banyaknya modus penipuan online di antaranya berkedok pembaruan data dari oknum yang mengaku dari bank, undian berhadiah, lowongan pekerjaan, bahkan modus lainnya seperti pengambilalihan akun pada kartu kredit atau kartu debit dengan mengambil data pribadi. Ketiga, keterampilan etika bermedia digital bertujuan untuk meningkatkan pengetahuan dan pemahaman peserta terhadap netiket. Konflik di media digital dapat terjadi salah satunya ketika seseorang tidak bersikap etis dan terdapat pihak lain yang tidak terima atas sikap atau perilaku tersebut. Bentuk, ragam, motif, dan modus kejahatan semakin beragam dan variatif. Pendekatan yang digunakan adalah metode Komunikasi Antar Pribadi dengan menggunakan permainan *boardgame*. Metode ini cocok digunakan dalam dinamika kelompok agar tidak membosankan. Hasilnya, pesertanya merasa pelatihan lebih dinamis dan mudah dipahami materinya.

Abstact

Starting from the needs of the English Study Program at Madiun Campus of UKWMS to provide knowledge and digital literacy skills to students, a community service program focused on fact-checking skills workshops was designed. This workshop focuses on fact-checking, personal data protection, and digital media ethics. Firstly, the fact-checking skill aims to provide training to participants to become skilled fact-checking agents, especially in identifying and combating hoax dissemination. Participants will be equipped with knowledge and skills on how to fact-check. Speakers will guide participants in understanding the concept of hoaxes, the motives behind hoax dissemination, characteristics, impacts, and methods of fact-checking (videos, photos, and narratives). Secondly, the personal data protection skill aims to enable participants to protect data and devices from online crime threats. Among the various online fraud modes are disguised as data updates from individuals claiming to be from banks, prize draws, job vacancies, and even other modes such as taking over credit card or debit card accounts by obtaining personal data. Thirdly, digital media ethics skills aim to enhance participants' knowledge and understanding of netiquette. Conflicts in digital media can occur when someone behaves unethically and there are others who disagree with such behavior. The forms, varieties, motives, and modes of crime are increasingly diverse and varied. Interpersonal Communication method using board games is suitable for group dynamics to prevent boredom and engage participants in game simulations. As a result, participants find the training more dynamic and the material easier to understand.

Keywords:

Boardgame; Cek Fakta; KAP, Komunikasi Antar Pribadi, Mahasiswa.

Correspondence Author:

Finsensius Yuli Purnama
finsensius@ukwms.ac.id

PENDAHULUAN

Media digital telah bagian tak terpisahkan bagi kaum muda di manapun mereka berada. Di satu sisi, media digital memberi peluang untuk pembelajaran maupun pemberdayaan di bidang

ekonomi, politik, sosial budaya, dan berbagai dimensi kehidupan lain. Di sisi lain, sebaliknya, media digital juga menawarkan banyak tantangan diantaranya etika yang terabaikan saat berinteraksi di media sosial, kecakapan menggunakan media digital yang kurang memadai, keamanan media digital yang belum terjaga dengan baik, dan budaya bermedia digital yang tidak santun (Amihardja, Kurnia, & Monggilo, 2022a). Hal ini jelas membuat pengejawantahan keterampilan literasi digital yang baik menjadi krusial bagi kaum muda saat ini.

Program studi ini terletak di Jln. Manggis No. 15-17, Kejuron, Kec. Taman, Kota Madiun Jawa Timur 63131. Berada di bawah naungan Fakultas Ilmu Komunikasi di Surabaya (FIKOM UKWMS), mahasiswa PSDKU Bahasa Inggris UKWMS Kampus Kota Madiun, belum pernah tersentuh program literasi digital. Padahal, FIKOM UKWMS sendiri sejak tahun 2021 telah menginisiasi kolaborasi bersama komunitas Masyarakat Anti Fitnah Indonesia (MAFINDO).

Kolaborasi ini berfokus pada edukasi dan riset terkait isu literasi digital, khususnya upaya melawan hoaks atau informasi palsu di Indonesia. Dari sisi edukasi, salah satu bentuk kolaborasi ini diwujudkan dengan membentuk Komisariat Masyarakat Anti Fitnah Indonesia (Mafindo) UKWMS sebagai komunitas mahasiswa yang akan menjadi agen literasi digital baik di lingkungan kampus dan masyarakat. Mahasiswa yang bergabung bersama Komindo, merupakan relawan yang akan aktif sebagai pemeriksa fakta dan konten kreator yang selama ini turut aktif dalam kegiatan edukasi literasi digital. Salah satu aspek edukasi yang berkontribusi bagi pengembangan keterampilan literasi digital anak muda telah dilakukan dengan mengembangkan wacana "Bukan Sekadar Paham", yang menjadi prinsip utama program literasi digital yang dilaksanakan oleh Masyarakat Anti Fitnah Indonesia (Mafindo). Hasilnya, program pelatihan literasi digital ini membawa dampak perubahan sikap yang signifikan terutama di ranah kognitif yang dibuktikan dengan meningkatnya kemampuan literasi digital siswa/i SMA dalam melakukan evaluasi kritis melalui pengecekan fakta setelah intervensi pelatihan (Purnama & Apul, 2023).

Meski begitu, kesempatan ini hanya dirasakan mahasiswa Program Studi Ilmu Komunikasi. Padahal, sebagai bagian dari FIKOM UKWMS, mahasiswa PSDKU Bahasa Inggris UKWMS Kampus Kota Madiun seharusnya memiliki kesempatan yang sama untuk mendapatkan pelatihan literasi digital seperti cek fakta, edukasi literasi digital dengan pendekatan komunikasi antar pribadi hingga program Tular Nalar Sekolah Kebangsaan. Namun, semua program ini masih terbatas diselenggarakan di kampus utama UKWMS di Kota Surabaya.

Kesenjangan aktivitas literasi ini disadari oleh pengelola PSDKU Bahasa Inggris UKWMS Kampus Kota Madiun. Mereka berharap mahasiswanya dapat memiliki kesempatan yang sama agar dapat menjadi agen-agen penjernih informasi yang dapat memahami, menafsirkan dan menyaring informasi khususnya informasi politik yang beredar di dunia maya.

Berdasarkan hasil observasi dan wawancara tim abdimas, permasalahan literasi politik digital yang dihadapi oleh kalangan mahasiswa PSDKU Bahasa Inggris UKWMS Kampus Kota Madiun mencakup beragam aspek, mulai dari pemahaman, partisipasi hingga evaluasi kritis terhadap konten media. Permasalahan ini dapat dijabarkan dalam poin-poin keterampilan berikut:

1. Keterampilan verifikasi informasi
2. Keterampilan memahami sumber informasi
3. Keterampilan berpikir kritis
4. Keterampilan membedakan fakta dan opini

5. Keterampilan keamanan dan privasi digital
6. Keterampilan memahami isu-isu politik yang kompleks

Enam permasalahan tersebut secara praktis terdiri atas a) mitra belum memiliki skill keterampilan cek fakta melalui berbagai tools secara online, b) mitra belum dapat membedakan informasi fakta dan hoax, c) mitra belum memiliki pengetahuan dan skill melindungi privasi lingkungan dan d) mitra sebagai pemilih muda yang potensial belum memiliki keterampilan literasi digital politik yang memadai. Peningkatan keterampilan dalam literasi politik digital ini menjadi substansial bagi mahasiswa, agar mereka dapat menjadi agen perubahan yang dapat berperan aktif dalam proses politik yang positif di era digital yang semakin kompleks. Mitra yang merupakan generasi Z merupakan *digital native* dalam proses kehidupan sehari-harinya. Hal ini memberikan potensi bagi mitra sebagai berikut:

1. Akses ke informasi politik. Kemampuan literasi digital yang memadai memungkinkan mitra untuk dapat memilah informasi fakta dan hoaks. Workshop keterampilan cek fakta sendiri akan mengembangkan selain keterampilan memilah informasi, juga kemampuan mengidentifikasi sumber terpercaya. Kemampuan ini memungkinkan mitra untuk membuat keputusan politik yang lebih informatif
2. Partisipasi politik digital. Mitra cenderung memiliki tendensi tinggi berpartisipasi atau berinteraksi melalui media sosial, platform daring dan forum diskusi online. Dengan mengikuti workshop cek fakta, mitra dapat lebih kritis dalam memahami isu-isu politik yang kompleks, berdebat, dan berkolaborasi secara efektif dalam lingkungan digital yang sehat.
3. Pemahaman terhadap fenomena atau isu digital. Pemilih muda yang memiliki keterampilan literasi digital yang baik akan memahami isu-isu terkait teknologi dan privasi digital, sehingga dapat mempengaruhi pandangan politik mereka terhadap regulasi maupun kebijakan terkait teknologi.

Keterampilan literasi digital merupakan elemen kunci bagi mitra, agar mereka mampu menjadi agen perubahan yang berperan aktif dalam proses politik positif di era digital yang semakin kompleks. Mitra sebagai *digital native* memiliki potensi besar karena akses mereka yang luas ke informasi politik melalui berbagai platform digital. Tidak hanya itu, permasalahan lain yang kerap dialami anak muda adalah *cyberbullying* (Cortesi, Hasse, Lombana-Bermudez, Kim, & Gasser, 2020; Lailiyah, Yuliyanto, & Pradhana, 2018). *Cyberbullying* sering kali dilakukan oleh mahasiswa. Faktor yang memicu perilaku *cyberbullying* adalah kecanduan menggunakan media sosial, kurangnya rasa empati, dan pernah menjadi korban bullying. Sebuah penelitian yang dilakukan oleh Wangid, menunjukkan bahwa 36,25% dari 497 mahasiswa mengaku pernah melakukan *cyberbullying* (Wangid, 2016). Beberapa studi juga menunjukkan literasi digital secara signifikan mampu menurunkan perilaku *cyberbullying* (Asriani et al., 2021; Rusdy & Fauzi, 2020; Zhao, Wu, Huang, & Zhang, 2022). Artinya, dengan mengikuti workshop cek fakta, maka mahasiswa akan menjadi agen literasi digital yang memiliki kompetensi komperhensif dengan mengoptimalkan penggunaan perangkat digital dan mampu meminimalkan dampak negative yang timbul darinya.

Workshop ini berfokus pada tiga keterampilan utama yakni pemeriksaan fakta, perlindungan data pribadi dan etika bermedia digital. **Pertama**, keterampilan cek fakta, bertujuan untuk memberikan pelatihan kepada peserta agar dapat menjadi agen periksa fakta yang terampil, khususnya dalam mengidentifikasi dan melawan penyebaran hoaks. Peserta akan

dibekali pengetahuan dan keterampilan bagaimana melakukan periksa fakta. Narasumber akan mengajak peserta mempelajari pengertian hoaks, motif penyebar hoaks, ciri, dampak, dan cara melakukan periksa fakta (video, foto, dan narasi). **Kedua**, keterampilan perlindungan data pribadi bertujuan agar peserta mampu melindungi data dan perangkat dari ancaman kejahatan online. Banyaknya modus penipuan online di antaranya berkedok pembaruan data dari oknum yang mengaku dari bank, undian berhadiah, lowongan pekerjaan, bahkan modus lainnya seperti pengambilalihan akun pada kartu kredit atau kartu debit dengan mengambil data pribadi. **Ketiga**, keterampilan etika bermedia digital bertujuan untuk meningkatkan pengetahuan dan pemahaman peserta terhadap netiket. Konflik di media digital dapat terjadi salah satunya ketika seseorang tidak bersikap etis dan terdapat pihak lain yang tidak terima atas sikap atau perilaku tersebut. Sasaran pengabdian yakni mahasiswa/i PSDKU Bahasa Inggris UKWMS Kampus Kota Madiun sebagai peserta.

METODE PENGABDIAN

Menjawab permasalahan mitra, maka kami menerapkan workshop pelatihan literasi digital dengan metode kelas cek fakta dan Komunikasi Antar Pribadi (KAP). Rincian metode pelaksanaan yang telah dilakukan dapat dilihat pada tabel berikut:

Tabel 1. Jadwal pelaksanaan dan penanggung jawab kegiatan

No	Kegiatan	Waktu	Metode	Penanggung Jawab
1.	Kelas Cek Fakta	24 November 2023	Online	Finsensus Yuli Purnama
2.	Kelas Prebunking: boardgame fandom dan unek-unek netizen	25 November 2023	Offline	Merlina Maria Barbara Apul

Pada kelas cek fakta kegiatan dilaksanakan via daring menggunakan *Zoom*, nantinya setiap peserta akan memasuki breakout room dan akan dipandu satu orang fasilitator untuk mengerjakan dan membahas soal cek fakta. Sementara pada pendekatan KAP setiap fasilitator berinteraksi langsung dengan mitra, memahami kebutuhan mereka, serta dapat memberikan informasi yang relevan dan bermanfaat. Karena bersifat antar pribadi, metode dalam workshop di desain secara berkelompok kecil dengan maksimal lima orang yang didampingi satu orang fasilitator dari tim pengabdian.

HASIL DAN PEMBAHASAN

Pelaksanaan program workshop cek fakta mahasiswa PSDKU Bahasa Inggris Universitas Katolik Widya Mandala Surabaya Kampus Madiun (UKWMS) dilakukan dalam dua tahap secara online dan luring. Berikut uraian lengkap tiap tahap tersebut.

WORKSHOP 1: *Kelas Cek Fakta*

Kegiatan pengabdian kelas cek fakta dilaksanakan pada Jumat, tanggal 24 November 2023 secara daring melalui *Zoom*. Kegiatan ini diikuti oleh 30 orang peserta yang terdiri dari mahasiswa dan dosen. Kelas cek fakta sendiri merupakan hasil kolaborasi Masyarakat Anti Fitnah Indonesia (MAFINDO), Aliansi Jurnalis Independen (AJI), dan Asosiasi Media Siber Indonesia (AMSI). Kelas Cek Fakta Muda & Guru ini bertujuan untuk menciptakan masyarakat yang mempunyai daya pikir kritis, khususnya anak-anak, remaja dan para pendidik di seluruh wilayah Indonesia. Serta memiliki pengetahuan dan keterampilan melakukan pengecekan fakta untuk

menjadi duta perlawanan hoaks (Mafindo, 2022a). Tabel berikut merupakan uraian metode pelaksanaan kelas cek fakta:

Tabel 2. Metode Pelaksanaan Kelas Cek Fakta

Permasalahan Mitra	Tolak Ukur	Metode Pelaksanaan	Capaian
Keterampilan Cek Fakta			
Belum memiliki keterampilan verifikasi informasi	Mampu mengevaluasi konten	✓ Peserta akan diajarkan keterampilan menggunakan tools cek fakta	a) Keterampilan menggunakan tools cek fakta
		✓ Peserta dibagi dalam setiap kelompok kecil berjumlah 5 orang dan didampingi 1 orang fasilitator	b) Keterampilan mencari artikel klarifikasi c) keterampilan verifikasi konten editan dan foto
Kurang memiliki keterampilan memahami sumber informasi	Dapat mencari sumber informasi	✓ Peserta akan diajarkan keterampilan untuk memahami dan mencari sumber informasi untuk mencegah penyebaran hoaks	d) keterampilan verifikasi konten video dan lokasi
		✓ Peserta dibagi dalam setiap kelompok kecil berjumlah 5 orang dan didampingi 1 orang fasilitator	e) Keterampilan memahami sumber informasi f) Keterampilan membedakan informasi fakta dan palsu
Kurang memiliki keterampilan membedakan informasi fakta dan hoaks	Mendeteksi apakah sebuah informasi sudah mengandung fakta atau tidak	✓ Peserta akan diajarkan keterampilan untuk memahami dan mencari sumber informasi untuk mencegah penyebaran hoaks	
		✓ Peserta dibagi dalam setiap kelompok kecil berjumlah 5 orang dan didampingi 1 orang fasilitator	

Tabel ini secara umum merangkum jalannya pelaksanaan kelas cek fakta yang dilakukan secara daring. Ruang virtual zoom di setting agar peserta lebih aktif dan terdorong berdiskusi. Alur kelas cek fakta dapat dilihat pada gambar berikut:



Gambar 1. Alur kelas cek fakta

Alur ini dirancang dengan tujuan agar peserta peserta aktif berinteraksi dengan pemateri dan fasilitator. Peserta juga diharapkan menggunakan Laptop/PC dengan *Google Chrome* terpasang, smartphone bisa digunakan untuk belajar tools khusus mobile. Adapun *timeline* dari kelas cek fakta dapat dilihat pada gambar berikut:



Gambar 2. *Timeline* kelas cek fakta

Gambar 2 ini merangkum timeline dari materi yang diberikan kepada peserta. Pada sesi ini pemateri akan memberikan ceramah dan berdiskusi bersama peserta.

Tampil sebagai pembicara adalah Finsensius Yuli Purnama sebagai salah satu tim pengabdian. Materi yang dibawakan berfokus pada empat topik yakni pada tataran konseptual tentang hoaks, trik mencari artikel klarifikasi, verifikasi konten editan dan foto serta verifikasi video dan lokasi. Materi yang disampaikan bersifat interaktif. Diawali dengan pemutaran video 'sekilas terlihat' yang bertujuan mengajak peserta untuk memahami bahwa konten yang dilihat di media sosial belum tentu terbukti kebenarannya. Sebab banyak jenis informasi atau palsu yang beredar di internet seperti satire/parodi (konten ejekan dan ironi untuk mengkritik elemen masyarakat tanpa maksud untuk menyakiti), hubungan palsu (judul, gambar, atau keterangan tidak mengkonfirmasi konten), konten yang menyesatkan (penggunaan informasi yang menyesatkan untuk membingkai sebuah isu atau individu), konteks yang salah (konten asli yang dibagikan dengan informasi kontekstual yang salah), konten penipu (ketika sumber yang asli ditiru), konten yang dimanipulasi (konten asli yang dimanipulasi), konten yang dibuat-buat (konten yang 100% palsu untuk menipu dan menyakiti), konten yang dibuat-buat, konten yang dimanipulasi, konten yang dibuat-buat untuk membahayakan), *clickbait* (berita utama tabloid atau yang menyesatkan), dan propaganda (informasi yang benar atau salah yang disebarakan untuk membujuk audiens dengan tujuan ekonomi, politik, agama, rasis (Herrero-Diz, Conde-Jiménez, & Reyes de Cózar, 2020).

Berbagai jenis informasi atau berita palsu tersebut ditampilkan dan dicontohkan agar dapat dibedakan oleh peserta. Dalam tataran konseptual peserta juga dikenalkan pada jenis gangguan informasi yang terdiri atas tiga jenis. Pertama, misinformasi, dimana informasi yang salah namun orang yang membagikannya percaya itu benar. Kedua, disinformasi yakni Informasi yang salah dan orang yang membagikannya tahu itu salah. Informasi palsu yang sengaja dibagikan. Ketiga, malinformasi yaitu informasi yang memiliki unsur kebenaran, baik dalam penggalan atau keseluruhan fakta objektif. Namun penyajiannya dikemas sedemikian rupa untuk melakukan tindakan yang merugikan bagi pihak lain (Adams, Osman, Bechlivanidis, & Meder, 2023; Hussain & Soomro, 2023).

Tataran konseptual lain yang diajarkan kepada peserta adalah terkait *cyberbullying* dan *cyberstalking/doxing*. *Cyberbullying* adalah tindakan perundungan dengan menggunakan teknologi digital. Hal ini dapat terjadi di media sosial, platform chatting, platform bermain game dan ponsel. *Cyberbullying* merupakan perilaku berulang yang ditujukan untuk menakuti, membuat marah, atau mempermalukan mereka yang menjadi sasaran (Cortesi et al., 2020; Zhao et al., 2022). Sementara *cyberstalking/doxing* merupakan pemantauan konstan seseorang melalui

akun media sosial mereka dan mengawasi aktivitas sehari-hari mereka dengan motif untuk menyakiti orang tersebut, menciptakan ketakutan pada korban atau untuk membalas dendam. Adapun faktor penyebab *cyberbullying* diantaranya sebagai wujud pembalasan atau penindasan yang diterima sebelumnya, untuk mencari kesan keren dan tangguh hingga dipicu rasa iri kepada orang lain yang akan dijadikan target *bullying* (Novianty, Wijayanti, & Muamar, 2023; Trottier, 2020).

Selanjutnya materi difokuskan pada temuan tim Litbang Mafindo yang menemukan tema politik sebagai tema terbanyak menghasilkan informasi hoaks pada tahun 2022 yakni sebesar 32,3%, disusul tema kesehatan sebanyak 14,3%. Sementara sebanyak 1,698 hoaks beredar selama tahun 2022. Facebook menjadi platform tertinggi penyebaran hoaks yakni 36,9%, diikuti Twitter 24,5%, dan WhatsApp sebesar 13,3% (Mafindo, 2022b). Hoaks sendiri mudah menyebar karena keterampilan Literasi digital dan berpikir kritis belum merata. Gen Z sebagai digital native pun belum cakap dalam memilah sumber informasi yang terpercaya.

Padahal, faktor penting yang dapat melindungi anak muda dari bahaya pengalaman online negatif adalah keterampilan literasi digital yang mumpuni. Literasi digital berfungsi sebagai sumber daya yang berharga untuk kesejahteraan di berbagai bidang kehidupan, dengan memberikan peluang di berbagai bidang seperti kontak sosial atau pengembangan profesional, dan yang juga dapat melindungi dari potensi hasil negatif dari pengalaman risiko online terhadap kesejahteraan. Keterampilan digital merupakan bagian penting dari literasi digital (Vissenberg, D'Haenens, & Livingstone, 2022).

Beberapa pengalaman telah menunjukkan bahwa pelatihan yang komprehensif untuk melawan hoaks memiliki dampak positif bagi penerimanya (Newman & Fletcher, R Kalogeropoulos, A Nielsen, 2019). Dalam kasus remaja, mereka mengaku lebih memperhatikan asal-usul informasi di jejaring sosial dan belajar untuk mempertanyakan teman-teman yang membagikan berita yang tidak akurat. Selain itu, penyelenggaraan lokakarya pelatihan untuk anak-anak di Inggris menegaskan bahwa pelatihan memberikan kepercayaan diri yang lebih besar dalam mengidentifikasi informasi yang dapat diandalkan dan tidak dapat diandalkan (Trust, 2018).

"Penangkal" terbaik terhadap ancaman yang ditimbulkan oleh berita palsu adalah pendidikan (Larkin, 2017; McDougall, Brites, Couto, & Lucas, 2019). Jelas bahwa kurangnya proses pendidikan formal atau informal dalam penggunaan media baru" memengaruhi persepsi kita terhadap dampaknya. Institusi pendidikan sangat penting dalam membantu anak-anak dan remaja untuk secara efektif membedakan kebenaran ketika mereka mencari informasi dan berita secara online (Purnama & Apul, 2023).

Namun, kapan sebaiknya kita mulai bertindak? Profesor Beth Hewitt menganggap bahwa mendidik anak-anak sejak dini adalah hal yang tepat (Tickle, 2018). Sebab tidak pernah ada yang lebih penting bagi anak muda untuk mengembangkan pemikiran kritis, pengetahuan berita, dan keterampilan untuk membedakan kebohongan dan kebenaran, terutama di jejaring sosial mereka (Cooke, 2017). Alhasil, dengan menanamkan rasa tanggung jawab untuk mencegah peredaran dan penyebaran berita bohong merupakan langkah besar untuk menjadi konsumen yang sadar akan informasi.

WORKSHOP 2: *Boardgame Fandom dan Unek-Unek Netizen*

Pelatihan kedua literasi digital diselenggarakan secara luring di UKWMS Kampus Madiun pada Sabtu, 25 November 2023. Dengan sasaran peserta yang sama, setting workshop dibuat

lebih interaktif dalam dinamika kelompok bersama fasilitator. Kegiatan ini diawali oleh penyampaian materi oleh Merlina Maria Barbara Apul sebagai tim pengabdian tentang tips dan trick selamat berinternet. Adapun gambaran metode pelaksanaan dengan pendekatan KAP dapat dilihat dari tabel berikut:

Tabel 3. Metode Pelaksanaan KAP

Permasalahan Mitra	Tolak Ukur	Metode Pelaksanaan	Capaian
<i>Komunikasi Antar Pribadi: 'Boardgame Fandom dan Unek-Unek Netizen'</i>			
Tidak memiliki keterampilan menjaga privasi dan keamanan akun digital	Mampu memberi perlindungan akun dan perangkat digital	Peserta akan diajarkan keterampilan keamanan berinternet: <ul style="list-style-type: none"> - Perlindungan akun dan perangkat - Menjelajahi internet dengan aman - Phising - Pertolongan pertama: peretasan 	Peserta pelatihan memiliki kompetensi melindungi akun dan perangkat digital serta mampu menjelajahi internet dengan aman
Kurang mampu berpikir kritis dalam mengelola informasi di jagad maya	Mampu mempertanyakan kebenaran informasi dan melakukan klarifikasi informasi	✓ <i>Boardgame Fandom</i> : Dalam permainan Boardgame Fandom ini, peserta dibagi menjadi kelompok dengan masing-masing kelompok terdiri dari delapan orang dan satu master game yang memandu permainan. Selama permainan, peserta menggunakan berbagai kartu, termasuk 20 kartu fakta, 6 kartu misinformasi, 14 kartu disinformasi, 5 kartu periksa fakta, dan 3 kartu prebunking. Melalui permainan ini, peserta dapat belajar tentang konsep debunking (periksa fakta) dan cara memeriksa informasi yang beredar. ✓ Peserta dibagi dalam setiap kelompok kecil dan didampingi fasilitator	<ul style="list-style-type: none"> - Peserta dapat memahami terciptanya tentang bagaimana misinformasi dan disinformasi - Peserta mampu memahami konsep dan cara debunking atau periksa fakta dari informasi yang beredar - Peserta memiliki keterampilan netiket di dunia maya
Tidak memahami dan memiliki keterampilan netiket	Mampu menerapkan netiket	✓ Peserta akan diajarkan dan berdiskusi tentang: <ul style="list-style-type: none"> - <i>Toxic Behavior Game Online</i> - <i>Phising</i> - <i>Love Scamming</i> ✓ Peserta dibagi dalam setiap kelompok kecil dan didampingi fasilitator	

Era digital memungkinkan penguasaan terhadap data pribadi, memengaruhi pola perilaku masyarakat dan mengubah alur komunikasi di antara mereka di dunia virtual. Imbasnya, hampir seluruh aktivitas kita di dunia digital berujung pada pola kapitalisme serta sosial bermodel penguasaan data. Artinya, jika bisa menguasai data, semuanya akan lebih mudah, dan sang pemilik data bisa melakukan apapun yang disukai. Oleh karena itulah, isu mengenai keamanan dan privasi di dunia digital menjadi sebuah diskusi panjang yang sangat relevan, baik untuk saat ini maupun yang akan datang (Mardjianto, Wedhaswary, Monggilo, Ningtyas, & Budiarto, 2022). Sebagai digital native, kehidupan mahasiswa erat kaitannya dengan teknologi. Meskipun unsur konvensional masih ada, namun bagi Gen Z, nyaris 95% kehidupan mereka dikuasai oleh teknologi (Pasha, Rasheed, & Ali, 2021). Terlebih saat aktualisasi diri, mereka membutuhkan perangkat dan zona digital, yang erat kaitannya dengan isu keamanan dan privasi. Inilah yang menjadi alasan pentingnya memberikan keterampilan melindungi data pribadi bagi mitra.

Adapun tujuan dari materi terkait keamanan dan privasi digital: 1. Agar publik bisa tahu dengan jelas tentang apa itu keamanan dan privasi digital. 2. Publik memahami tentang bagaimana menyelaraskan pengetahuan dunia digital dengan sisi teknis keamanan serta privasi digital. 3. Publik mengerti beberapa tools yang berkaitan dengan keamanan dan privasi digital. 4. Publik tahu bagaimana caranya melakukan pengaduan terhadap konten kejahatan digital dan hoaks. 5. Publik tahu cara mengelola informasi pribadi di platform digital tertentu. Ada pengelompokan terhadap ancaman digital, yakni data mining dan jenis ancaman tradisional. Unsur ancaman tradisional yang perlu masyarakat tahu antara lain phishing, malware, serangan sibil dan profil palsu. spamming, serangan de-anonimisasi, serangan kloning profil, *cyber-bullying* dan *cyber-stalking* (Okditazeini & Irwansyah, 2018).

Sementara itu, data peretasan akun yang berawal dari pencurian data pribadi di Indonesia juga semakin meningkat, di mana dalam lima tahun terakhir laporan pencurian data pribadi dari 20 laporan pada tahun 2016 meningkat menjadi 183 laporan pada tahun 2020 (Antaraneews.com, 2020). Oleh sebab itu aman bermedia digital ini merupakan salah satu pilar kemampuan literasi digital masyarakat Indonesia. Aman bermedia digital adalah pilar yang melihat kemampuan pengguna media digital untuk jaga aman dan tangguh di dunia digital (Ameliah, Negara, & Rahmawati, 2022).

Sayangnya, indeks literasi aman bermedia digital yang secara umum diperoleh dari indikator terkait tingkat kesadaran masyarakat akan perlindungan data pribadi masih tergolong rendah. Ini ditunjukkan dengan perilaku masyarakat yang masih mencantumkan nomor handphone pribadi dan tanggal lahir pada platform digitalnya. Selain itu, ada sekitar 35% responden yang menambahkan info lokasi terkini, unduh aplikasi tanpa tahu siapa pembuatnya, serta mengunggah foto KTP. Dari data terkait perlindungan data pribadi tersebut, disimpulkan ada 53,6% masyarakat yang memiliki tingkat perlindungan data pribadi rendah. Nilai indeks keamanan digital adalah 3,10 dan menduduki posisi di bawah rata-rata indeks literasi digital nasional yaitu 3,49 (Amihardja, Kurnia, & Monggilo, 2022b).

Topik-topik yang diajarkan disarikan berdasarkan Modul P3KD Safer With Google

1. Beri Perlindungan kuat untuk akun dan perangkat mu

'Buat sandi yang kuat & unik': Membuat sandi yang kuat dan unik untuk setiap akun merupakan salah satu langkah terpenting dalam melindungi privasimu.



Tabel 3. Tips membuat sandi yang kuat dan unik

Tips #1	Sandi harus terdiri dari minimal 8 karakter.
Tips #2	Gunakan kombinasi huruf besar, huruf kecil, angka, dan simbol.
Tips #3	Jangan gunakan informasi pribadi dalam sandimu, seperti: nama, alamat, email, nomor ponsel, nomor KTP, nama ibu/ayah, hari ulang tahun atau nama binatang peliharaan, dll.
Tips #4	Jangan gunakan sandi yang mudah ditebak, misalnya nomor berurutan, seperti "123456" atau "password123"!

'Jaga sandimu tetap aman': Menjaga keamanan sandi sama pentingnya dengan membuat sandi yang kuat. Ikuti tips praktis ini untuk melindungi sandi dengan mudah!

Tabel 4. Tips melindungi sandi

Tips #1	Jangan pernah menyimpan sandi di tempat yang bisa ditemukan orang lain atau membagikan sandimu dengan siapa pun.
Tips #2	Gunakan sandi yang berbeda untuk setiap akunmu
Tips #3	Gunakan Pengelola Sandi Google untuk membantumu membuat, menyimpan, dan mengelola sandimu, serta memperingatimu bila ada sandi yang disusupi.
Tips #4	Seperti halnya kesehatan yang perlu check-up berkala, begitu juga dengan sandimu! Gunakan Pemeriksaan Sandi Google untuk mendeteksi jika ada sandimu yang telah disusupi, sandi yang lemah (baik di akunmu mau pun di situs pihak ketiga), serta mengubah sandimu dengan mudah.

Contoh kalimat: *Aku suka makan nasi goreng dan naik dinosaurus.* Dari kalimat ini kamu dapat membuat password berikut:

Tabel 5. Contoh membuat password

Ambil huruf pertama dari setiap kata dalam kalimat. Contoh: asmngdnd
Tambahkan huruf besar & huruf kecil: asmNGdnd → Supaya gampang diingat, huruf besar diletakkan pada inisial " nasi goreng " dan " dinosaurus ".
Terakhir, tambahkan angka & simbol: 45mNG&nD → Ubah beberapa huruf dengan angka, ganti kata "dan" dengan simbol "&".
Kamu bisa menerapkan formula yang sama setiap membuat sandi untuk akun baru. Contoh: Aku suka makan mie ayam dan naik kuda! → 45mMA&nK!

Salah satu cara terbaik untuk melindungi akunmu dari upaya pembobolan, yaitu dengan mengaktifkan Verifikasi 2 Langkah:

Tabel 6. Tips verifikasi 2 langkah

<p>Gunakan Verifikasi 2 Langkah</p> <p>Contoh penerapan Verifikasi 2 Langkah Saat kamu mencoba login ke akun bankmu, selain sandi/pin, biasanya kamu akan diminta memasukkan kode</p>	<p>Tips #1</p> <p>Aktifkan Verifikasi 2 Langkah di menu Pengaturan akunmu.</p>
	<p>Tips #2</p> <p>Saat mengaktifkan Verifikasi 2 Langkah, pastikan kamu menghubungkannya dengan nomor ponsel dan perangkat yang paling sering kamu gunakan, karena fitur ini akan mengirimkan notifikasi ke perangkat tersebut untuk menyelesaikan login.</p>
	<p>Tips #3</p>

verifikasi yang dikirimkan via SMS ke nomor ponselmu.	Jika kamu kehilangan perangkat atau mengganti nomor ponselmu, lalu tidak bisa login dengan Verifikasi 2 Langkah, masuk ke pusat bantuan google untuk memulihkan akun.
---	---

Melindungi akunmu dari upaya kejahatan dimulai dari dasar, seperti halnya pagar yang melindungi rumah. Ikuti tips ini untuk belajar melindungi keamanan dirimu di internet!

Tabel 7. Tips menjaga keamanan perangkat digital

Menjaga keamanan perangkat	Tips #1: Jangan abaikan notifikasi software update! Update software dan aplikasi yang kamu gunakan secara berkala, serta pastikan perangkatmu menggunakan update terbaru yang tersedia.
	Tips #2: Lindungi keamanan datamu dari aplikasi berbahaya <ul style="list-style-type: none"> • Pastikan kamu selalu download aplikasi dari sumber resmi dan tepercaya, seperti Google Play. • Hapus aplikasi yang sudah tidak digunakan. • Aktifkan update otomatis pada aplikasi. • Batasi akses aplikasi ke data sensitif, seperti lokasi dan foto
	Tips #3: Gunakan kunci layer Saat tidak menggunakan komputer, laptop, tablet, atau ponsel, kunci layar agar orang lain tidak dapat login ke perangkatmu. Untuk keamanan tambahan, atur perangkatmu agar mengunci layar secara otomatis saat perangkat beralih ke mode tidur.

2. Menjelajah internet dengan aman

Di internet ada situs-situs tidak aman yang dapat mencuri informasi yang kamu masukkan. Pelajari cara memastikan keamanan situs dan jaringan yang kamu gunakan dengan mengikuti tips berikut.

Tabel 8. Tips berjelajah aman di internet

Pastikan URL situs web aman	Tips #1: Cek ikon gembok terkunci dan "https" pada URL Hindari memasukkan informasi sensitif, seperti sandi atau nomor kartu kredit sebelum memastikan situs tersebut aman. Cek URL situsnya. Pada browser Google Chrome, jika situs tersebut aman, di kolom URL akan muncul ikon gembok terkunci dan diawali dengan "https" (perhatikan adanya huruf "s" = "secure").
Pastikan koneksi aman	Tips #2: Berhati-hati saat menggunakan Wi-Fi publik Jaringan Wi-Fi publik atau gratis, mungkin tidak dienkripsi—sekalipun dibutuhkan sandi untuk mengaksesnya, sehingga saat terhubung ke jaringan tersebut, siapa pun yang berada di sekitar jaringan dapat memantau aktivitas internetmu.

3. Phising

Phishing merupakan tindak kejahatan siber, di mana pelaku memperdayai dan membujuk korban via email, media sosial, dll. untuk membagikan data sensitif, seperti informasi login, bank, kartu kredit, dll.

Tabel 9. Pertanyaan untuk mencegah phising

Guna menghindari perusahaan	Pertanyaan #1: Sebelum mengklik suatu URL (link), cari tahu sendiri secara online nama dan URL resmi bisnisnya . Bandingkan, apakah sesuai dengan yang kamu terima? Hal ini
------------------------------------	--



yang benar, tanpa kesalahan ejaan? phishing, tanyakan pertanyaan berikut sebelum kamu mengklik link atau merespon pesan	karena penipu kadang membuat URL dan halaman situs web yang mirip dengan perusahaan resminya untuk menipumu.
	Pertanyaan #2: Cek apakah tampilan pesan atau situs terlihat profesional , dengan produk atau logo perusahaan yang benar, tanpa kesalahan ejaan?
	Pertanyaan #3: Apakah ada peringatan? Gmail menandai email mencurigakan dan memindai lampiran bervirus secara otomatis. Perhatikan peringatan yang diberikan sistem seperti "tandai sebagai spam" atau "virus terdeteksi".
	Pertanyaan #4: Apakah pesan atau hal yang ditawarkan terdengar mustahil? Misalnya, kesempatan untuk menghasilkan uang yang sangat banyak atau memenangkan sesuatu. Kemungkinan besar ini adalah upaya penipuan.
	Pertanyaan #5: Apakah pesannya terdengar aneh? Misalnya, apakah pengirim menyebut adanya situasi gawat darurat yang membuatmu panik atau mengatakan bahwa dia mengenalmu, tapi kamu tidak yakin?

4. Pertolongan pertama

Saat kamu mengalami peretasan atau pencurian perangkat, cek langkah cepat yang bisa kamu lakukan, guna memulihkan atau meminimalisir kerugian.

Tabel 10. Tips pertolongan pertama jika akun diretas dan perangkat dicuri

Tips #1: Jika akunmu diretas	<p>Login segera dan gantilah sandimu. Bila pelaku telah mengganti sandi Akun Google-mu, masuk di pusat bantuan google, lalu klik pilihan mengamankan akun google yang diretas atau disusupi.</p> <p>Kemudian, lakukan Pemeriksaan Keamanan Google untuk melihat apakah ada akun lainnya yang turut disusupi, lalu ikuti rekomendasi yang disarankan untuk meningkatkan keamanan akun.</p>
Tips #2: Jika ponselmu hilang atau dicuri	Kunjungi menu Temukan ponsel Anda untuk mencegah siapa pun mengakses datamu. Kamu bisa menemukan lokasi perangkat dari jarak jauh dan mengunci ponselmu (baik Android maupun iOS).

5. Tips Privasi Data

a. Saring Sebelum Sharing (3S)

Di era digital, kita sering berbagi informasi tanpa mempertimbangkan siapa saja yang bisa melihat konten tersebut saat itu, mau pun di masa mendatang. Simak tips berikut ini untuk memastikan kamu selalu saring sebelum sharing.

Tabel 11. Tips pertolongan pertama jika akun diretas dan perangkat dicuri

Tips #1: Jejak online-mu bisa bertahan selamanya	Setelah diposting, sulit untuk mengontrol suatu konten. Orang-orang bisa saja salah paham akan niatmu, membuat salinan (copy), menangkap layar (screenshot), atau membagikannya kembali. Maka, saringlah sebelum sharing!
Tips #2: Minta izin sebelum sharing	Apakah kamu pernah merasa kesal saat teman atau keluarga memposting foto/informasi pribadimu secara online tanpa izin?

Menghormati privasi orang lain sama pentingnya dengan menjaga privasimu. Maka, pastikan kamu selalu minta izin orang lain, sebelum membagikan konten yang melibatkan mereka, contoh: kontak, foto, berita kehamilan, wajah anak-anak, dll.

b. Batasi Akses Aplikasi dan Layanan ke Data Pribadi

Produk seperti *Google Maps*, *Search*, dan *YouTube* memerlukan data agar layanannya lebih bermanfaat. Namun, kamu punya kontrol untuk memilih data yang ingin dibagikan. Cek tips berikut.

Tabel 12. Tips membatasi akses aplikasi dan layanan ke data pribadi

Tetapkan tanggal kadaluarsa untuk datamu	<p>Google menyediakan fitur hapus otomatis untuk datamu, karena kami percaya produk hanya perlu menyimpan informasi, selama masih bermanfaat untukmu.</p> <p>Terdapat opsi hapus data otomatis setiap 18 bulan yang aktif secara default pada:</p> <ul style="list-style-type: none"> • Histori Lokasi saat pertama kalinya diaktifkan. • Aktivitas Situs & Aplikasi pada akun-akun baru. <p>Kamu selalu bisa menonaktifkan fitur atau memilih periode waktu penghapusan yang berbeda.</p> <p>Kunjungi Kontrol Aktivitas di akun Google-mu untuk mengatur bagaimana datamu digunakan dan disimpan.</p>
Lakukan Pemeriksaan Keamanan	<p>Pemeriksaan Keamanan bisa membantu mengecek siapa saja aplikasi pihak ketiga yang memiliki akses ke data Akun Google-mu, bahkan mungkin kamu akan menemukan beberapa aplikasi yang sudah lama tidak digunakan.</p>

c. Kontrol Privasi Melalui Aplikasi yang Digunakan

Semua orang punya preferensi privasi masing-masing, sehingga tidak ada satu solusi yang sama untuk semua. Maka, tips berikut dapat menghadirkan kontrol yang memungkinkan kamu memilih pengaturan privasi yang tepat.

Tabel 13. Tips membatasi akses aplikasi dan layanan ke data pribadi

Tips #1: Aktifkan mode Samaran di Chrome, Maps, Search, dan YouTube	<p>Cukup dengan mengklik foto profilmu, kamu bisa mengaktifkan mode Samaran secara mudah.</p> <p>Saat mode Samaran diaktifkan, histori browsing, cookies, dan aktivitasmu tidak akan disimpan di Akun Google-mu.</p>
Tips #2: Kontrol datamu, langsung dari Akun Google	<p>Kamu bisa meninjau dan menghapus aktivitas pencarianmu, mengakses kontrol privasi yang relevan langsung di Akun Google-mu dengan cepat, tanpa perlu mengunjungi halaman pengaturan terpisah.</p>
Tips #3: Lakukan Pemeriksaan Privasi	<p>Pemeriksaan Privasi memungkinkanmu memilih jenis data yang ingin disimpan di Akun Google, menentukan siapa saja yang bisa mengaksesnya, serta mengatur jenis iklan yang ingin kamu lihat.</p> <p>Kamu bisa mengubah pengaturan ini kapan saja dan mengaktifkan pengingat untuk mengelola pengaturan secara berkala.</p>

d. Data Pribadi

Data pribadi pada dasarnya adalah data personal yang unik dan bisa berupa identitas, kode, simbol, huruf atau penanda lainnya. Karena sifatnya privat ini, data pribadi diperlakukan sebagai informasi perseorangan yang bersifat privat harus disimpan, dikelola dan dilindungi kerahasiaannya untuk mencegah terjadinya kejahatan digital (Kurnia & Wijayanto, 2020).

Tabel 14. Jenis-jenis data pribadi

Nama	Alamat rumah	Alamat email	Tempat dan tanggal lahir	Nama ibu kandung
Nomor KTP/NIK	Nomor telepon	Nomor password	Nomor induk pegawai	Nomor rekening bank
Nomor kartu ATM	Nomor kartu kredit	Penghasilan	Data kesehatan	Sidik jari
Retina mata	Data biometrik	Preferensi politik	Tanda tangan	lainnya

Yuk antisipasi kejahatan digital! Sebab, kejahatan digital tidak hanya mengganggu aktivitas kita pada platform digital yang kita miliki, tetapi kerugian juga dapat bersifat material, rekam jejak digital yang negatif bahkan berdampak pada kesehatan mental kita, karenanya kompetensi literasi digital dalam hal ini kompetensi aman digital mutlak dibutuhkan.

Selain pelatihan cara aman dan selamat berinternet, peserta juga diajak berdinamika dalam kelompok bersama fasilitator. Kegiatan dalam kelompok diawali dengan Boardgame Fandom. Permainan ini dapat melihat bagaimana perilaku berbudaya di media digital yang kompleks, khususnya terkait perilaku etis para netizen di jagad maya.



Gambar 3 Boardgame fandom

Kelompok usia milenial dan generasi Z menempati peringkat paling banyak mendapat perundungan siber (*cyberbullying*) yakni sebesar 54% untuk milenial dan 47% usia generasi Z yang mendapat perundungan. *Nyesek banget kan?* Oleh sebab itu kaum muda perlu memiliki kompetensi literasi digital yang baik supaya tidak menjadi korban perundungan siber.

Sering kali juga kita tergoda melakukan hal yang sama. Apabila kita mengalami perundungan, mula-mula hanya kita bicarakan terbatas dengan sesama teman atau keluarga secara offline. Tapi, akhirnya kita juga menjadi semakin jengkel, panas, dan membalas bullying di

media sosial dengan *bullying* pula, sehingga terjadi “perang *bullying*” di media sosial. Seperti pertarungan antara ‘Warnas Baharu’ dan ‘Warnas Bahari’. Akhirnya, suasana di ruang digital menjadi gaduh. Ibaratnya, *bullying* itu seperti “lingkaran setan” dan *bullying* hanyalah salah satu dari perilaku yang tidak etis.



Gambar 4. Rule boardgame fandom

Kontribusi Mitra Terhadap Pelaksanaan

Kegiatan pengabdian ini sepenuhnya dibantu oleh mitra dalam menyediakan dan mengakomodir peserta. Mitra juga membantu penyediaan ruangan untuk pelaksanaan workshop cek fakta berbasis pendekatan KAP.

PENUTUP

Media digital adalah bagian tak terpisahkan bagi generasi muda atau akrab disebut Gen Z. Sebab media digital memberikan peluang pembelajaran, sekaligus pemberdayaan di bidang ekonomi, politik, sosial, budaya serta berbagai dimensi kehidupan manusia. Namun, kehadiran media digital tidak terlepas dari banyaknya tantangan mulai dari persoalan etika saat berinteraksi di dunia maya, kecakapan atau keterampilan menggunakan media digital yang belum memadai, hingga keamanan media digital yang masih diabaikan. Kegiatan pengabdian dengan fokus pada workshop literasi digital cek fakta bagi mahasiswa sebagai kaum muda, diharapkan mampu meningkatkan keterampilan sekaligus membentuk berpikir kritis pada mahasiswa sebagai agen perubahan di masa depan. Saran untuk kegiatan selanjutnya adalah bahwa kegiatan pengabdian dengan memberdayakan keterampilan literasi digital harus semakin ditingkatkan, dengan tidak hanya menasar anak muda tetapi penting pula pengajar dan lansia menjadi target sasaran pelatihan kedepannya.

DAFTAR PUSTAKA

Adams, Z., Osman, M., Bechlivanidis, C., & Meder, B. (2023). (Why) Is Misinformation a Problem?



- Perspectives on Psychological Science*, 18(6), 1436–1463.
<https://doi.org/10.1177/17456916221141344>
- Ameliah, R., Negara, R. A., & Rahmawati, I. (2022). *Status Literasi Digital di Indonesia 2021*. Jakarta. Retrieved from
https://cdn1.katadata.co.id/media/microsites/litdik/Status_Literasi_Digital_diIndonesia_2021_190122.pdf
- Amihardja, S., Kurnia, N., & Monggilo, Z. M. Z. (2022a). *Lentera Literasi Digital Indonesia: Panduan Literasi Digital Kaum Muda Indonesia Timur*. Malang: Tiga Serenada.
- Amihardja, S., Kurnia, N., & Monggilo, Z. M. Z. (2022b). *Lentera Literasi Digital Indonesia: Panduan Literasi Digital Kaum Muda Indonesia Timur*. Malang: Tiga Serenada.
- Antaraneews.com. (2020). Tren kejahatan siber meningkat. Retrieved from Antaraneews.com website: <https://www.antaraneews.com/infografik/1571604/tren-kejahatan-siber-meningkat>
- Asriani, D. D., Yulianti, K. Y., Priwati, A. R., Kirana, A. P., Darmawan, P., & Kusumaningtyas, A. P. (2021). *TEENAGER-RELATED CYBERBULLYING CASE IN INDONESIA*. Yogyakarta. Retrieved from <https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2021/09/Digitimes-35.pdf>
- Cooke, N. A. (2017). Posttruth, Truthiness, and Alternative Facts: Information Behavior and Critical Information Consumption for a New Age. *The Library Quarterly*, 87(3), 211–221. <https://doi.org/10.1086/692298>
- Cortesi, S. C., Hasse, A., Lombana-Bermudez, A., Kim, S., & Gasser, U. (2020). *Youth and digital citizenship+ (plus): Understanding skills for a digital world*. Massachusetts. Retrieved from <https://cyber.harvard.edu/publication/2020/youth-and-digital-citizenship-plus>
- Google. (2023). *Perlindungan Pertama Perkuat Keamanan Digital*. Jakarta: Google. Retrieved from https://safety.google/intl/id_id/
- Herrero-Diz, P., Conde-Jiménez, J., & Reyes de Cózar, S. (2020). Teens' Motivations to Spread Fake News on WhatsApp. *Social Media + Society*, 6(3), 205630512094287. <https://doi.org/10.1177/2056305120942879>
- Hussain, M., & Soomro, T. R. (2023). Social Media: An Exploratory Study of Information, Misinformation, Disinformation, and Malinformation. *Applied Computer Systems*, 28(1), 13–20. <https://doi.org/10.2478/acss-2023-0002>
- Kurnia, N., & Wijayanto, X. . (2020). Perlindungan identitas digital dan data pribadi di platform digital. In *Kolaborasi sajadahhijaulawan (hoaks) COVID-19: Kampanye, riset dan pengalaman japelidi di tengah pandemic* (pp. 1–34). Yogyakarta: UGM.
- Lailiyah, N., Yuliyanto, M., & Pradhana, G. A. (2018). Youthizen, Political Literacy, and Social Media. *E3S Web of Conferences*, 73, 14005. <https://doi.org/10.1051/e3sconf/20187314005>
- Larkin, J. P. (2017). *Ignorance Isn't Strength: The Need for Secondary Education to Address Fake News* (State University of New York). State University of New York. Retrieved from <http://hdl.handle.net/20.500.12648/5089>
- Mafindo. (2022a). Highlight Kelas Cek Fakta: Muda dan Guru. Retrieved from Mafindo.or.id website: <https://www.mafindo.or.id/2022/05/28/highlight-kelas-cek-fakta-muda-dan-guru/>
- Mafindo, L. (2022b). *Laporan Hoaks Februari 2022-1*. Jakarta. Retrieved from <https://www.mafindo.or.id/wp-content/uploads/2023/02/Laporan-Hoaks-Februari-2022-1-1.pdf>



- Mardjianto, F. L. D., Wedhaswary, I. D., Monggilo, Z. M. Z., Ningtyas, I., & Budiarto, M. N. (2022). *LITERASI DIGITAL MODUL Disusun oleh: Aliansi Jurnalis Independen 2022* (I. Ningtyas, Ed.). Jakarta: Aliansi Jurnalis Independen. Retrieved from https://aji.or.id/upload/article_doc/MODUL_Literasi_Digital_untuk_Perguruan_Tinggi-compressed.pdf
- McDougall, J., Brites, M.-J., Couto, M.-J., & Lucas, C. (2019). Digital literacy, fake news and education / Alfabetización digital, fake news y educación. *Cultura y Educación, 31*(2), 203–212. <https://doi.org/10.1080/11356405.2019.1603632>
- Newman, N., & Fletcher, R Kalogeropoulos, A Nielsen, R. (2019). Reuters Institute Digital News Report 2019. Retrieved from Reuters Institute Digital website: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-06/DNR_2019_FINAL_0.pdf
- Novianty, S. M., Wijayanti, S., & Muamar, J. (2023). ETHICAL DISCOURSE OF DOXING IN INDONESIAN TWITTER USERS. *Jurnal InterAct, 12*(1), 1–13. <https://doi.org/10.25170/interact.v12i1.4134>
- Okditazeini, V., & Irwansyah, I. (2018). Ancaman Privasi dan Data Mining di Era Digital: Analisis Meta-Sintesis pada Social Networking Sites (SNS). *Jurnal Studi Komunikasi Dan Media, 22*(2), 109. <https://doi.org/10.31445/jskm.2018.220202>
- Pasha, S. A., Rasheed, A., & Ali, S. (2021). YouTube Usage Motivation among Students: Uses and Gratification Analysis. *Global Social Sciences Review, VI*(II), 318–329. [https://doi.org/10.31703/gssr.2021\(VI-II\).32](https://doi.org/10.31703/gssr.2021(VI-II).32)
- Purnama, F. Y., & Apul, M. M. B. (2023). “Bukan Sekadar Paham”: A Quasi-Experimental Study on High School Students in Surabaya. *Ultimacomm, 15*(1), 95–110. <https://doi.org/https://doi.org/10.31937/ultimacomm.v15i1.3146>
- Rusdy, M., & Fauzi, F. (2020). DIGITAL LITERACY AND CYBERBULLYING BEHAVIOR OF YOUTHS IN INSTAGRAM. *KOMUNIKE, 12*(2), 122–145. <https://doi.org/10.20414/jurkom.v12i2.2699>
- Tickle, L. (2018). Fake news: Teaching children the difference between Trump and truth. Retrieved from Theguardian.com website: <https://www.theguardian.com/education/2018/jun/12/fake-news-schools-trump-truth>
- Trottier, D. (2020). Denunciation and doxing: towards a conceptual model of digital vigilantism. *Global Crime, 21*(3–4), 196–212. <https://doi.org/10.1080/17440572.2019.1591952>
- Trust, N. L. (2018). *News Wise pilot report 2018*. Retrieved from <https://literacytrust.org.uk/research-services/research-reports/newswise-pilot-report-2018/>
- Vissenberg, J., D’Haenens, L., & Livingstone, S. (2022). Digital Literacy and Online Resilience as Facilitators of Young People’s Well-Being? *European Psychologist, 27*(2), 76–85. <https://doi.org/10.1027/1016-9040/a000478>
- Wangid, M. N. (2016). CYBERBULLYING: STUDENT’S BEHAVIOR IN VIRTUAL WORLDS. *GUIDENA: Jurnal Ilmu Pendidikan, Psikologi, Bimbingan Dan Konseling, 6*(1), 38. <https://doi.org/10.24127/gdn.v6i1.412>
- Zhao, L., Wu, Y., Huang, X., & Zhang, L. (2022). Network Anonymity and Cyberbullying among Chinese Adolescents: A Moderated Mediation Model. *International Journal of Environmental Research and Public Health, 19*(2), 637. <https://doi.org/10.3390/ijerph19020637>