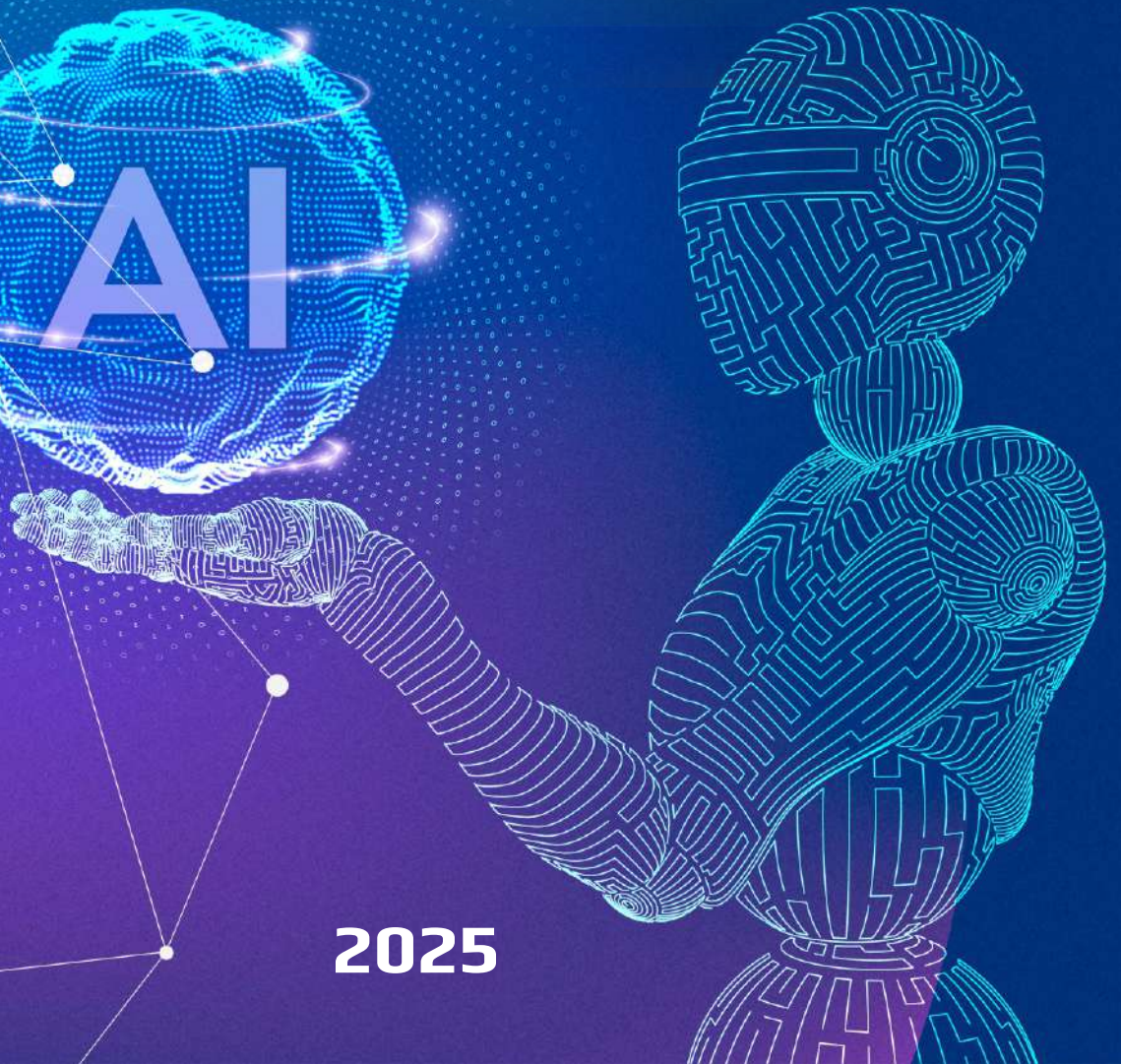




**ALIANSI
JURNALIS
INDEPENDEN**
Alliance of Independent Journalist

KECERDASAN ARTIFISIAL DALAM ARUS INFORMASI DAN MEDIA



2025



KECERDASAN ARTIFISIAL DALAM ARUS INFORMASI DAN MEDIA

**Masduki
Aghnia Adzkia
Adi Marsiela**

**Aliansi Jurnalis Independen (AJI) Indonesia
2025**

KECERDASAN ARTIFISIAL DALAM ARUS INFORMASI DAN MEDIA

Penulis : Masduki, Aghnia Adzkia, Adi Marsiela

Editor : Abdul Manan

Penata Isi & Desain Sampul : Fahrul Rozi

Hak Cipta dilindungi undang-undang. Dilarang memperbanyak atau memindah sebagian atau seluruh isi buku ke dalam bentuk apapun, secara elektronik maupun mekanis, termasuk fotokopi, merekam, atau dengan teknik perekaman lainnya, tanpa izin tertulis dari Penerbit. Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

Diterbitkan pertama kali oleh:



Aliansi Jurnalis Independen (AJI) Indonesia, 2025

Jl. Kembang Raya No.6 Kwitang, Senen, Jakarta Pusat 10420

Telp 021-3151214, Fax 3151261

Email: sekretariat@ajindonesia.or.id

Web: www.aji.or.id

Kecerdasan Artifisial dalam Arus Informasi dan Media

185 hlm, ; 21 x 29,7 cm

ISBN: 978-979-3530-75-8

Cetakan I: Maret 2025

Apabila di dalam buku ini terdapat kesalahan cetak/produksi atau kesalahan informasi, mohon hubungi penerbit.

KATA PENGANTAR

(Ketua Umum AJI Indonesia)

Menciptakan Penggunaan AI yang “Sehat” di Dunia Akademik

Artificial Intelligence (AI) telah menjadi bagian tak terpisahkan dari kehidupan modern, terutama dalam dunia akademik. Bagi akademisi—baik sebagai peneliti maupun pendidik—memahami AI bukan hanya soal menggunakan teknologi ini, tetapi juga mengenali dampaknya yang luas terhadap ilmu pengetahuan, pendidikan, dan masyarakat secara umum.

Pemahaman tentang AI menjadi sangat penting untuk meningkatkan kualitas riset, mengoptimalkan proses pembelajaran, dan menjaga integritas serta etika dalam penggunaannya.

AI memberikan berbagai manfaat besar bagi dunia akademik. Di bidang penelitian, AI dapat menganalisis data dalam jumlah besar, menemukan pola tersembunyi, dan mempercepat proses penemuan ilmiah.

Misalnya, dalam ilmu sosial, AI dapat membantu menganalisis tren sosial yang berkembang di media sosial, sementara dalam ilmu kesehatan, AI mempercepat penemuan obat dan diagnosa penyakit dengan akurasi yang lebih tinggi.

Di bidang pendidikan, AI berperan dalam menciptakan metode pembelajaran yang lebih personal dan efektif. Sistem pembelajaran berbasis AI bisa menyesuaikan materi dengan kemampuan dan kecepatan belajar tiap siswa, menciptakan pengalaman belajar yang lebih adaptif dan dinamis.

Selain itu, AI juga dapat mengotomatiskan berbagai tugas administratif, seperti penilaian tugas dan analisis data akademik. Hal ini memungkinkan dosen dan peneliti untuk lebih fokus pada aspek substansial dalam pengajaran dan penelitian.

Namun, meskipun AI menawarkan banyak potensi, penggunaannya juga menimbulkan sejumlah tantangan etika yang harus diperhatikan dengan serius oleh akademisi. Salah satu isu utama adalah keadilan dan bias dalam AI. Algoritma AI dapat menghasilkan keputusan yang bias jika data yang digunakan untuk melatih sistem tidak representatif atau mengandung prasangka.

Bias ini bisa memperburuk ketidakadilan sosial, terutama jika AI digunakan dalam kebijakan akademik seperti seleksi mahasiswa atau penilaian kinerja dosen.

Selain itu, privasi dan keamanan data menjadi masalah krusial. Penggunaan AI dalam penelitian sering melibatkan pengolahan data pribadi dalam jumlah besar. Akademisi wajib memastikan bahwa data yang digunakan telah memperoleh izin yang sah dan tidak melanggar hak privasi individu. Lebih jauh, data tersebut harus dilindungi agar tidak jatuh ke tangan yang salah atau disalahgunakan.

Isu lain yang tak kalah penting adalah tanggung jawab akademisi dalam menyebarkan informasi. AI dapat digunakan untuk menghasilkan teks, gambar, dan video yang sangat realistis, termasuk deepfake dan berita palsu.

Sebagai pengambil peran penting dalam edukasi, akademisi memiliki kewajiban untuk memastikan bahwa teknologi ini tidak disalahgunakan untuk menyebarkan informasi yang menyesatkan. Oleh karena itu, pendidikan literasi digital dan AI menjadi sangat krusial, agar mahasiswa dan masyarakat mampu membedakan informasi yang valid dan yang menyesatkan.

Oleh karena itu, integrasi AI dalam dunia akademik harus selalu diiringi dengan prinsip transparansi, keadilan, dan etika yang kuat. Dengan demikian, kita bisa memaksimalkan manfaat AI bagi masyarakat tanpa menimbulkan dampak negatif yang merugikan.

Buku ini merupakan lanjutan dari pelatihan literasi AI untuk akademisi yang telah diselenggarakan oleh Aliansi Jurnalis Independen (AJI) pada Februari 2025.

Buku ini ditujukan bagi akademisi dari berbagai disiplin ilmu di Indonesia, dengan fokus utama pada pengajar Ilmu Komunikasi. Tujuannya adalah untuk memahami peran AI dalam mitigasi misinformasi dan disinformasi serta mendukung tujuan akademik lainnya.

AJI mengucapkan terima kasih banyak untuk penulis modul ini yaitu Masduki, Aghnia Adzkia, Adi Marsiela yang sudah memberikan banyak tips dan informasi penting praktek penggunaan AI begitu juga tantangannya untuk para akademisi.

Ucapan yang sama juga ditujukan kepada semua pihak yang sudah mendukung hadirnya buku penting ini.

Semoga buku ini memperkaya literasi Indonesia, terutama berkaitan dengan AI dan bisa menjadi panduan para akademisi yang menjadikan AI sebagai pendukung kerja-kerja akademik mereka.

Jakarta, 25 Maret 2025.

Nany Afrida
Ketua Umum AJI Indonesia



DAFTAR ISI

Kata Pengantar	3
Daftar Isi	6
Bagaimana memahami dan menggunakan buku ini.....	9
Bab I. Perkembangan Teknologi AI dan Penggunaannya.....	11
1.1. AI Dalam Industri Media.....	18
Bab II. Pemanfaatan AI dalam Produksi, Penyebaran, dan Deteksi Misinformasi/Disinformasi	26
2.1. AI dan fenomena disinformasi.....	26
2.2. Definisi	28
2.2.1. Misinformasi	30
2.2.2. Disinformasi.....	31
2.2.3. Malinformasi.....	31
2.3. Pemanfaatan AI dalam Produksi Mis-disinformasi.....	34
2.4. Penyebaran Mis-disinformasi dengan AI	42
2.5. Deteksi Mis-disinformasi dengan AI	46
2.5.1. Pemeriksaan Teks	48
2.5.2. Pemeriksaan Audio.....	56
2.5.3. Memeriksa Foto dan Video yang dibuat AI.....	58
2.5.4. Menginvestigasi Teks AI dan Pemilik Situs Palsu Menggunakan Akun Iklan Digital	69
Bab III. AI dalam Penelitian Akademik dan Industri Media.....	78
3.1. Penggunaan AI dalam Penelitian Akademik	78
3.1.1. Pelaksanaan Riset Akademik.....	79
Publikasi Hasil Riset.....	83
3.2. Penggunaan AI dalam Penelitian di Industri Media	86
3.2.1 Bagaimana jurnalis dan ruang redaksi menggunakan AI?.....	86

3.2.2 Analisis dan visualisasi data menggunakan Gen-AI.....	95
Bab IV. Keamanan Digital di era Artificial Intelligence	105
4.1. Prinsip Keamanan Digital.....	107
4.2. Bentuk-bentuk dari serangan teknis:	109
4.2.1. Malware	109
4.2.2. Spyware	109
4.2.3. Phishing	110
4.2.4. Spear phishing.....	110
4.2.5. Peretasan.....	110
4.2.6. DDoS Attack.....	110
4.2.7. Penyadapan.....	111
4.3. Bentuk-bentuk serangan non-Teknis.....	111
4.3.1. Doxing.....	111
4.3.2. Ujaran Kebencian.....	111
4.3.3. Persekusi daring.....	111
4.3.4. Impersonasi.....	111
4.3.5. Kriminalisasi	111
4.4. Mengapa bisa terjadi serangan digital.....	111
4.5. Aplikasi percakapan	135
4.6. Memilih surat elektronik.....	137
4.7. Berbagi dokumen	137
4.8. Aplikasi pertemuan video	139
Bab V. Etika Penggunaan AI untuk Akademik dan Industri Media	141
5.1 Etika Penggunaan AI dalam Dunia Akademik.....	141
5.1.1. Kontroversi dan Urgensi Etika AI	141
5.1.2. Etika Umum Publikasi Ilmiah	144
5.1.3. Ruang Lingkup Etika AI.....	148

5.1.4. Prinsip UNESCO untuk Penggunaan AI	151
5.2 Etika Penggunaan AI dalam Industri Media.....	153

Bab VI. Pengembangan Kurikulum Literasi Media Memanfaatkan

AI	162
6.1. Urgensi Kurikulum Literasi AI	162
6.2. Standar Perkuliahan Literasi AI	164
6.3. Model Kurikulum Literasi AI	167
6.3.1. Personalisasi	168
6.3.2. Kurikulum Lintas Disiplin	168
6.3.3. Akses Pembelajaran Seumur Hidup	169
DAFTAR PUSTAKA.....	173
Lampiran	
Lembar evaluasi pembelajaran modul (<i>pre-test dan post-test</i>).....	180
BIO DATA PENULIS.....	183

Bagaimana memahami dan menggunakan buku ini

1. Penyusunan buku ini merupakan kelanjutan dari pelatihan untuk pelatih (Training of Trainers) literasi AI untuk akademisi yang telah diselenggarakan oleh Aliansi Jurnalis Independen pada bulan Februari 2025.
2. Buku ini ditujukan untuk para akademisi dari berbagai disiplin ilmu di Indonesia, termasuk dan terutama akademisi/pengajar Ilmu Komunikasi, dalam memahami artificial intelligence (AI) sebagai alat dalam melakukan mitigasi terhadap misinformasi/disinformasi dan tujuan akademik lainnya.
3. Buku ini bersifat bahan bacaan awal, bacaan dasar yang harus ditindaklanjuti dengan penelaahan terhadap literatur lain yang lebih lengkap dan memadai.
4. Buku ini harus dibaca secara berurutan sejak Bab I hingga Bab VI sehingga diperoleh pengetahuan sejak informasi dasar, panduan ketrampilan hingga dimensi etisnya.
5. Buku ini terdiri dari empat bagian penting: Pertama, mengupas informasi dan pengetahuan dasar terkait sejarah dan aplikasi AI dihubungkan dengan kerja literasi AI, khususnya mitigasi dan resolusi kasus misinformasi/disinformasi di ruang digital. Kedua, penjelasan isu dan problematika serta ketrampilan terkait AI di dunia akademik dan industri media; Ketiga, diskusi terkait aspek-aspek etika dalam penggunaan AI di dunia akademik dan industri media; Keempat, panduan terkait pengembangan kurikulum pembelajaran AI di kampus-kampus di Indonesia.
6. Buku ini ditulis dengan gaya penulisan yang ringan, tidak terlampau akademik, berpola *how-to* sehingga ramah bagi semua orang, tak terbatas kalangan akademis.
7. Buku ini diperkaya dengan *pre-test* dan *post-test* sebagai instrumen evaluasi bagi peserta dan atau pembaca umum ketika menikmati seluruh isi buku.
8. Buku ini merupakan bagian dari kerja sosialisasi, panduan dari aksi kolaborasi dan aktivisme digital yang bertumbuh, serta bagian dari gerakan literasi digital dan AI di Indonesia. Karena itu, buku ini terbuka untuk masukan lebih lanjut.



**ALIANSI
JURNALIS
INDEPENDEN**
Alliance of Independent Journalist

BAB I.

PERKEMBANGAN TEKNOLOGI AI DAN PENGUNAANNYA

BAB I.

PERKEMBANGAN TEKNOLOGI AI DAN PENGGUNAANNYA

Tujuan: Setelah mempelajari buku ini peserta didik diharapkan memahami titik-titik penting sejarah, konteks pengembangan, ekosistem, hingga pemanfaatan artificial intelligence (AI).

Pertanyaan pemantik:

1. Siapa, bagaimana, dan dari negara mana yang mengembangkannya?
2. Aspek kehidupan mana yang belum tersentuh oleh AI?
3. Apakah kita hanya 'konsumen' dalam pemanfaatan AI?

Metode penyampaian:

- Ceramah
- Diskusi

Apakah ada bagian dari keseharian kita yang tidak bersinggungan dengan teknologi *artificial intelligence* (AI) atau kecerdasan buatan? Mungkin jawabannya semua berhubungan. Apalagi jika kita menggunakan telepon pintar sejak bangun pagi hingga menutup mata.

Misalnya saja saat kita mengatur jadwal pertemuan lewat aplikasi Calendar yang mampu mengingatkan waktu dan tempat pertemuan layaknya asisten pribadi. Belum lagi jika kita kesulitan menemukan lokasi pertemuan dan meminta bantuan Siri atau Google untuk menuntun perjalanan berkendara atau jalan kaki menuju ke lokasi tersebut.

Katakanlah kita menggunakan mobil Tesla. Kita tinggal duduk di dalam kendaraan tanpa harus mengemudi. Untuk masuk ke dalam mobil, tinggal menggunakan perintah suara. Selepas dari acara pertemuan, kita kembali ke kantor. Untuk masuk ke ruangan kerja ada sebuah panel pengenalan wajah yang fungsinya sebagai akses kunci masuk. Saat duduk di kursi, kita membuka telepon pintar dan mengakses media sosial. Konten-konten yang muncul ternyata memang sudah disesuaikan oleh platform, sesuai dengan preferensi dan kegemaran kita.

Ilustrasi di atas rasanya cukup menggambarkan bagaimana sebenarnya AI bersinggungan dengan keseharian kita.

Sudah sejak lama manusia mengetahui apa yang kini dipahami sebagai AI atau kecerdasan artifisial ini melalui mitologi dan fiksi (Manan, 2024) Mitologi Yunani misalnya mengenal Talos, raksasa berbadan perunggu-kreasi Hephaestus, dewa perajin sekaligus pandai besi- yang tugasnya menjaga Pulau Kreta dari penjajah.

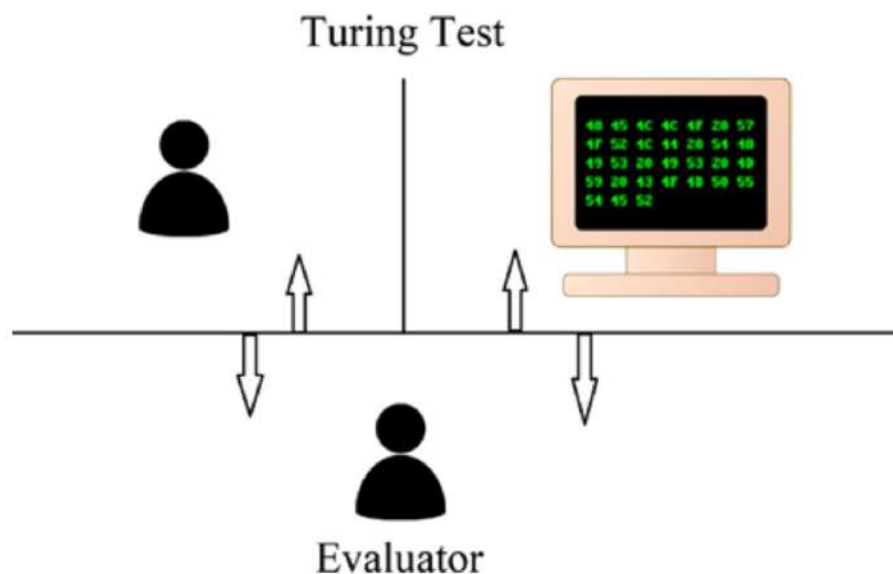
Dalam budaya populer, sutradara Stanley Kubric memperkenalkan HAL (Heuristically Programmed Algorithmic Computer) 9000 lewat film 2001: A Space Odyssey. HAL adalah komputer super yang mengontrol sistem pesawat ruang angkasa *Discovery One* dalam misi ke Jupiter pada film yang diperkenalkan ke publik pada 1968. Itu belum termasuk film Terminator, Blade Runner, dan bahkan Frankenstein (Taulli, 2019)

Perihal pemanfaatannya dalam dunia nyata, sejumlah literatur merujuk pada komputer yang dikembangkan Alan Turing, matematikawan dari Universitas Manchester saat dia berupaya memecahkan kode Enigma buatan Nazi, Jerman di Perang Dunia II. Saat itu, dia membuat makalah bertajuk "Computing Machinery and Intelligence" dan mengajukan pertanyaan: bisakah mesin berpikir? (Turing, 1950).

Sebelumnya, Turing menulis makalah "On Computable Number" pada 1936. Ia mengemukakan konsep inti computer yang kemudian dikenal sebagai 'mesin Turing'. Patut diingat, komputer sesungguhnya baru dikembangkan lebih dari satu dekade kemudian.

Turing fokus pada konsep mesin pintar. Dalam upayanya itu, ada beberapa cara pengukuran. Di sinilah ia menemukan "Uji Turing" atau Turing Test yang terkenal itu. Ini pada dasarnya adalah permainan dengan tiga pemain: dua manusia dan satu komputer. Penilai, seorang manusia, mengajukan pertanyaan terbuka kepada dua pemain lainnya (satu manusia, satu komputer) dengan tujuan menentukan siapa di antara mereka yang manusia. Jika penilai tidak dapat menentukan, maka komputer dianggap cerdas.

Gambar di bawah ini menunjukkan alur kerja dasar Uji Turing (Taulli, 2019).



Istilah “kecerdasan buatan” sendiri baru dikenal pada Dartmouth Summer Research Project on Artificial Intelligence tahun 1956, simposium yang diprakarsai John McCarthy dari Dartmouth College. Ilmuwan komputer ini bertujuan mengeksplorasi kemungkinan pembuatan mesin yang dapat meniru kecerdasan manusia.

Ekspektasi yang terlalu tinggi terkait kemampuan AI yang dapat meniru kecerdasan manusia ini tidak terwujud dalam waktu singkat. Kapasitas atau inovasi perangkat pendukung dan kapasitas daya komputasi masih terlalu lemah pada periode itu.

Sehingga era 1970-1980 disebut masuk dalam era Musim Dingin AI. Pemerintah dan investor kehilangan kepercayaan yang berdampak pada berhentinya beragam proyek AI.

Publikasi matematikawan asal Inggris, James Lighthill pada 1973 menyebut penelitian AI saat itu menghadapi tantangan besar dan tidak sesuai ekspektasi awal. Menurutnya, AI berhasil dalam tugas-tugas spesifik pada lingkup terbatas namun tidak mampu mengerjakan tugas yang lebih kompleks seperti pemahaman bahasa alami (Lighthill, 1973).

Kritik lain Lighthill terkait investasi besar pada pengembangan AI, khususnya di Inggris. Ia menyarankan investasinya dialihkan pada bidang lain yang lebih menjanjikan karena penelitian AI tidak sepadan dengan hasilnya.

Gairah terhadap beragam proyek pengembangan AI kembali menggeliat era 1980-an seiring peningkatan kemampuan komputasinya, selain makin majunya produksi perangkat keras pendukungnya. Beragam proyek seperti sistem pakar, program komputer yang dapat meniru keputusan manusia pada diagnosa medis berdasarkan data dan pola, hingga perencanaan industrinya, mendapatkan dukungan dari investor.

Investasi dari pemerintah turut mendukung perkembangan AI pada periode itu. Contohnya, Pemerintah Jepang meluncurkan proyek AI berbasis logika yang dinamai *Fifth Generation Computer System*. Pemerintah Amerika Serikat memiliki *Strategic Computing Initiative*, pengembangan teknologi AI di bidang militer dan industri.

Pihak swasta dan perguruan tinggi juga menyambutnya dengan pengembangan perangkat keras yang mendukung riset AI.

Salah satu tolak ukur pengembangan AI pada era 1990-an adalah kemenangan komputer Deep Blue –dikembangkan International Business Machines Corporation (IBM)—saat bermain catur dengan Grand Master Garry Kasparov pada 1997.

IBM, perusahaan teknologi multinasional yang bermarkas di Armonk, New York, Amerika Serikat ini merancang komputer yang dapat menganalisa serta mengevaluasi langkah catur sesuai dengan aturan yang dimasukkan dalam programnya. Saat itu pengembangannya tidak memanfaatkan pembelajaran mesin seperti AI yang banyak digunakan publik saat ini.

Dalam perkembangannya, teknologi AI jadi prioritas penting bagi perusahaan tradisional seperti McDonald's yang mengakuisisi Dynamic Yield, perusahaan teknologi rintisan asal Israel senilai 300 juta dolar Amerika pada 2019. Pembelian ini terkait penggunaan AI untuk memberikan pengalaman yang dipersonalisasi bagi pelanggan (Bronner, 2019).

Dynamic Yield, yang didirikan pada 2011, merupakan perintis pemanfaatan AI untuk menciptakan interaksi pelanggan yang dipersonalisasi di seluruh portal, aplikasi, hingga surat elektronik. Beberapa pelanggannya, antara lain, Hallmark Channel, IKEA, dan Sephora.

Lantas bagaimana perkembangan Tes Turing setelah beberapa dekade? Ya, tes ini terbukti sulit dipecahkan. Perlu diingat bahwa ada kontes, seperti

Loebner Prize dan Turing Test Competition, untuk mendorong orang-orang menciptakan sistem perangkat lunak yang cerdas.

Pada tahun 2014, ada kasus di mana Tes Turing tampaknya berhasil. Kasus ini melibatkan komputer yang mengatakan bahwa usianya sudah 13 tahun. Yang cukup menarik, para juri manusia mungkin tertipu karena beberapa jawaban mengandung kesalahan (Guardian, 2014).

Pada Mei 2018, CEO Google, Sundar Pichai dalam acara I/O 2018 mempamerkan kemampuan baru Google Assistant yang mencengangkan. Google Assistant melakukan panggilan telepon atas nama penggunanya. Pichai memutar ulang rekaman panggilan telepon yang katanya dikirim oleh Assistant ke salon rambut.

Suaranya terdengar sangat alami. Orang di ujung telpon tidak tahu bahwa mereka sedang berbicara dengan asisten AI digital. Google Assistant bahkan mengucapkan "mmhmmm" yang sangat santai di awal percakapan.

Pichai menegaskan kembali bahwa ini adalah panggilan sungguhan menggunakan Assistant dan bukan demo yang dibuat-buat. "Yang menakjubkan adalah Assistant benar-benar dapat memahami nuansa percakapan," katanya. "Kami telah mengerjakan teknologi ini selama bertahun-tahun. Namanya Google Duplex." (Welch, 2018)

Selain kemajuan dalam pendekatan konseptual, teori, dan model baru, AI memiliki beberapa pendorong penting lainnya. Berikut ini beberapa pendorong utamanya:

1. Pertumbuhan pesat pengumpulan data

Internet jadi faktor utama bagi AI karena memungkinkan terciptanya kumpulan data yang sangat besar.

2. Infrastruktur

Barangkali perusahaan yang paling berpengaruh bagi AI selama 15 tahun terakhir atau lebih adalah Google. Untuk mengimbangi pengindeksan Web—yang tumbuh dengan kecepatan yang mengejutkan—perusahaan harus menemukan pendekatan kreatif untuk membangun sistem yang dapat diskalakan. Hasilnya adalah inovasi dalam kluster server komoditas, virtualisasi, dan perangkat lunak sumber terbuka. Google juga merupakan salah satu pengadopsi awal pembelajaran mendalam, dengan peluncuran proyek "Google Brain" pada tahun 2011.

3. GPU (Graphics Processing Unit)

Teknologi chip ini, yang dipelopori oleh NVIDIA, awalnya ditujukan untuk grafis berkecepatan tinggi dalam game. Namun arsitektur GPU pada akhirnya juga ideal untuk AI. Perhatikan bahwa sebagian besar penelitian pembelajaran mendalam dilakukan dengan chip ini. Alasannya adalah, dengan pemrosesan paralel, kecepatannya berkali-kali lipat lebih tinggi daripada CPU tradisional. Ini berarti bahwa komputasi model ini mungkin memerlukan waktu hanya satu atau dua hari, bukan hitungan minggu atau bahkan bulan.

Semua faktor ini saling memperkuat atau menambah bahan bakar bagi pertumbuhan AI. Terlebih lagi, faktor-faktor ini kemungkinan akan tetap aktif selama tahun-tahun mendatang (Taulli, 2019).

Agar memahami proses perkembangan AI, penting juga bagi kita untuk mengetahui serta mengidentifikasi negara-negara mana saja yang kemudian mengembangkan dan memanfaatkannya dalam konteks geopolitik.

Kemunculan Chat GPT pada 2020 menjadi salah satu pencapaian besar pengembangan teknologi AI. Keberadaannya menjadi sangat populer dalam hitungan kurang dari dua tahun sejak diperkenalkan. Apalagi, penggunaannya terbilang sangat mudah.

Riset awalnya dilakukan sekelompok peneliti dari OpenAI, seperti Ilya Sutskever, Greg Brockman, Alec Radford, dan Dario Amodei pada 2015. Misinya adalah membuat model bahasa AI yang akan merevolusi interaksi manusia-komputer dan mengubah cara kita berkomunikasi dengan mesin.

Mereka melatih model mereka, yang sekarang dikenal sebagai ChatGPT, pada sejumlah besar data teks, menyempurnakan kemampuannya untuk menghasilkan respons seperti manusia. AI tersebut menunjukkan pemahaman yang luar biasa tentang bahasa, terlibat dalam percakapan, dan memberikan informasi yang mendalam.

Pada tahun 2019, tim tersebut mengungkapkan kreasi mereka ke dunia, dan dengan demikian lahirlah ChatGPT. ChatGPT menjadi teman terpercaya yang menyediakan informasi, hiburan, dan bahkan dukungan emosional bagi mereka yang berinteraksi dengannya (Teja, 2023).

Dalam perkembangannya kini, AI sudah memiliki banyak variasi. Secara fungsional, AI bisa dimasukkan dalam tiga kategori besar. Pertama, Narrow AI, di mana salah satu bentuknya adalah chat-GPT untuk teks. Kedua, General AI. Ketiga, super AI. Kategori terakhir ini dianggap masih sepenuhnya sebatas konsep (Manan, 2024).

Secara teori Narrow AI dapat menjalankan tugas-tugas tertentu dan tidak dapat melakukan pembelajaran di luar tugasnya. Pengenalan wajah, pemroses bahasa alami, dan generator gambar merupakan bentuk dari kecerdasan buatan tipe ini. Siri, Google Assistant, dan Alexa merupakan salah satu contohnya. Mereka dapat memahami dan memberi respon pada perintah suara, tetapi tidak dapat memberi diagnosis medis secara akurat.

Apa yang kita kenal sebagai Generatif AI saat ini adalah bagian dari Narrow AI. AI tipe ini kerap digambarkan seperti komposer di balik layar, yang menciptakan karya musik baru (atau bentuk konten lainnya) dari awal.

Generatif AI juga dapat menghasilkan keluaran yang orisinal dan realistis, baik itu mengubah musik, membuat gambar, atau bahkan menyusun cerita.

Varian lain dari Narrow AI adalah non-Generatif AI. Tipe ini, yang juga dikenal sebagai AI diskriminatif atau AI analitis, mencakup berbagai teknik yang berfokus pada tugas-tugas seperti klasifikasi, prediksi, dan pengambilan keputusan. Beberapa contoh umum dari non-generatif AI antara lain:

- Filter spam.
Algoritma ini menganalisis konten email dan metadata untuk menentukan apakah pesan masuk adalah spam atau bukan, membantu menjaga kotak masuk kita tetap rapi.
- Sistem rekomendasi.
Aplikasi seperti Netflix, Amazon, dan Spotify menggunakan AI non-generatif untuk menyarankan konten atau produk yang dipersonalisasi berdasarkan preferensi dan perilaku pengguna.
- Deteksi penipuan.
Lembaga keuangan menggunakan model AI jenis ini untuk mengidentifikasi transaksi yang mencurigakan dan mencegah aktivitas penipuan, serta melindungi aset nasabah (Manan, 2024)

1.1. AI Dalam Industri Media

Lantas bagaimana pemanfaatan AI itu dalam industri media?

Industri media sebenarnya sudah mulai memanfaatkan AI jauh sebelum GPT mulai dikenalkan pada tahun 2020. Menurut studi yang dilakukan Peter N. Amponsah dan Atianashie Miracle Atianashie dalam *Navigating the New Frontier: A Comprehensive Review of AI in Journalism*¹⁰, pada tahun 1980-an dan 1990-an itu penggunaan AI dalam jurnalisme sudah dimulai tapi masih dalam tahap awal.

Fokus utama pemanfaatannya saat itu adalah pada pelaporan dengan bantuan komputer. Jurnalis mulai menggunakan basis data penting dan perangkat digital untuk mengumpulkan dan mengatur data dengan lebih efisien. Pada periode ini memang belum ada aplikasi AI yang canggih tetapi sangat penting untuk menetapkan fondasi bagi perkembangan teknologi ini pada masa berikutnya (Bahroun et al., 2023).

Awal tahun 2000-an menjadi saksi lahirnya pembuatan konten otomatis dalam jurnalisme. Algoritma dikembangkan untuk menghasilkan laporan sederhana, seperti pembaruan cuaca, ringkasan olahraga, dan berita keuangan. Pengenalan teknologi Natural Language Generation (NLG) merupakan langkah maju yang signifikan. Periode ini menandai dimulainya peran AI dalam mengurangi beban kerja jurnalis dalam menghasilkan laporan berita rutin (Bahroun et al., 2023).

Dari pertengahan tahun 2000-an hingga 2010-an, algoritma pembelajaran mesin menjadi bagian integral dari pekerjaan jurnalisme. Algoritma ini dapat menyaring kumpulan data besar, mengidentifikasi pola, dan bahkan memprediksi tren, yang terbukti sangat berguna untuk jurnalisme investigasi. (Manan, 2024)

Era ini juga melihat alat AI digunakan untuk menganalisis tren dan opini publik di media sosial. Jurnalis mulai mengandalkan alat ini untuk mendapatkan wawasan tentang sentimen publik, yang itu bisa membantu mengungkap cerita yang muncul dan memahami reaksi audiens (Li et al., 2023a).

Pada akhir tahun 2010-an, personalisasi konten menjadi fokus utama dalam jurnalisme, yang didorong oleh AI. Platform organisasi berita mulai menggunakan algoritma AI untuk menyesuaikan distribusi konten dengan pengguna individu, meningkatkan keterlibatan dan relevansi kontennya.

Mesin rekomendasi diterapkan untuk menyarankan artikel dan konten berdasarkan perilaku dan preferensi pengguna (Jerbi, 2023).

Pada tahun 2023, saat Centre for Media Transition pada University of Technology Sydney, Australia, melakukan investigasi skala besar terhadap Generatif AI dalam produk berita, ditemukan bahwa ruang redaksi bereksperimen dengan teknologi ini secara hati-hati. Mereka melihat keuntungan besar bagi produksi berita, khususnya seputar penyerapan tugas-tugas kasar yang muncul akibat digitalisasi, dengan syarat mempertahankan proses editorial yang kuat.

Hasil studi itu juga menyatakan, editor menyadari kerugian signifikan dari penggunaan generatif AI jika akurasi, keaslian, dan bias tidak ditangani dengan baik. Juga soal pentingnya transparansi dan pengawasan manusia dalam pemanfaatannya. Ruang redaksi juga khawatir tentang penggunaan arsip berita mereka untuk melatih sistem AI oleh perusahaan teknologi tanpa manfaat balik (berupa keuntungan secara ekonomi) untuk mereka.

Keterbatasan generatif AI berasal dari cara kerja model dan data yang digunakan untuk melatihnya. Banyak model generatif AI yang dilatih pada data yang bersumber dari internet dan tidak diperbarui setelahnya, yang secara efektif memberikan tanggal batas atau batasan keterkinian pada informasi yang dapat disintesis dalam *output*-nya.

Madhumita Murgia, editor AI di Financial Times, mengatakan, 'Berdasarkan kondisinya saat ini, model tersebut tidak orisinal. Model tersebut tidak membuat sesuatu yang baru. Model tersebut didasarkan pada informasi yang sudah ada' (Adami, 2023).

Karena itu, generatif AI tidak dapat memenuhi permintaan audiens untuk adanya analisis lebih lanjut atau pandangan yang lebih mendalam tentang suatu subjek. Keterbatasan tersebut muncul dari sifat teknologi itu sendiri yang pembuatan teksnya dirancang untuk menghasilkan teks yang terdengar alami dengan mensintesis struktur leksikal dari berbagai sumber, bukan untuk memberikan respons yang akurat atau faktual dengan menilai kepastian klaim tertentu.

Risiko kesalahan diperburuk jika output terkait dengan peristiwa terkini atau *real time*. Hal ini menunjukkan bahwa alat generatif AI masih dinilai belum cocok untuk pelaporan berita terkini (*breaking news*), operasinya yang rumit dan mahal, serta memerlukan pemeriksaan fakta dan referensi silang atas informasinya secara cermat (Adami, 2023).

Saat lembaga Polis, pusat penelitian jurnalisme di London School of Economics, melakukan survei global tentang keterlibatan ruang redaksi dengan AI pada paruh pertama tahun 2023, ditemukan bahwa penggunaan non-generatif AI yang luas dan semakin cepat di ruang redaksi, khususnya untuk fungsi skala besar tetapi relatif mendasar seperti pengikisan media sosial, analisis data, dan pembuatan konten otomatis sederhana (Beckett, 2019).

Dalam pengumpulan berita, penggunaan non-generatif AI yang paling umum adalah dalam analisis teks seperti pengenalan karakter optik dan transkripsi audio, dan dalam penambangan data untuk penemuan dan investigasi berita.

Pengikis web dan media sosial membantu jurnalis mengidentifikasi topik yang sedang tren dan cerita yang potensial dicari banyak orang. Banyak yang melihat ini sebagai area keberhasilan terbesar untuk alat AI analitis yang ada. Pada tingkat yang lebih rinci, alat AI ini dapat membantu mengisolasi tren di antara audiens dan demografi tertentu.

Sebagian besar ruang redaksi menggunakan alat pihak ketiga, meskipun beberapa telah mengembangkan sistem internal yang dilatih pada data tertentu (Beckett & Yaseen, 2023).

Dalam tahap produksi, penggunaan umum meliputi pengambilan data untuk verifikasi dan pengecekan fakta, pemeriksaan akhir dan analisis informasi menggunakan pemrosesan bahasa alami (NLP), dan pembuatan konten berdasarkan data terstruktur seperti informasi keuangan, olahraga, dan cuaca (Beckett & Yaseen, 2023).

Jangkauan penggunaan terluas adalah dalam distribusi, termasuk distribusi media sosial bertenaga AI dan SEO (Search Engine Optimisation), respons terhadap pertanyaan pengguna melalui chatbot, kustomisasi konten, sistem personalisasi dan rekomendasi, dan konversi media ucapan ke teks (Beckett & Yaseen, 2023).

Secara ringkas bisa dikatakan, manfaat non-generatif AI berpusat pada efisiensi dan otomatisasi tugas-tugas yang membosankan dan berulang, yang membebaskan jurnalis untuk fokus pada pelaporan. Analisis data skala besar adalah area tempat alat AI dapat menghasilkan wawasan yang mungkin tidak terdeteksi oleh manusia. (Beckett & Yaseen, 2023).

Reuters menggunakan pembelajaran mesin untuk membuat transkrip, menerjemahkan audio, dan mengidentifikasi tokoh masyarakat pada video yang diunggah ke layanan distribusinya.

The Washington Post pada July 2024 lalu memperkenalkan inisiatif bertajuk *Climate Answer* yang berbasis AI generatif dalam format percakapan interaktif dengan pembacanya. Tim *The Washington Post* memanfaatkan antarmuka obrolan interaktif ini guna memudahkan pembaca mendapat jawaban atas pertanyaan mereka seputar isu iklim.

Di China, kantor berita *Xinhua* sudah meluncurkan presenter virtual berbasis AI, yang pertama di dunia, meniru presenter aslinya pada 2018 silam. Organisasi berita lainnya yang melakukan hal sama adalah *India Today* dengan presenter virtualnya “Sana”, *Kuwait News* dengan “Fedha”, yang sama-sama diperkenalkan pada tahun 2024 (Giovanni & Ganinda, 2023).

Secara ringkas, pemanfaatan AI oleh organisasi berita global dapat dikategorikan dalam empat tahapan di bawah ini:

Pengumpulan Konten

Sebagian besar media telah mengintegrasikan alat ‘social listening’ ke dalam proses redaksi mereka untuk melacak berita yang beredar daring, mengumpulkan informasi, dan menghasilkan ide berita. Alat *social listening* adalah perangkat lunak yang memantau percakapan daring, biasanya di media sosial, dan memilih kata kunci, tagar, frasa, penyebutan, nama, serta tingkat keterlibatan audiens.

Di antara alat ‘social listening’ yang paling banyak digunakan adalah CrowdTangle, Dataminr, Newswhip, Tweetdeck, Hootsuite, dan Google Trends. Dalam beberapa kasus, alat-alat ini mulai membentuk ‘irama’ editorial media. Jurnalis semakin sering diminta oleh editor untuk meliput berita atau ide berita yang kemungkinan besar akan menghasilkan lebih banyak lalu lintas. Hal ini menunjukkan bahwa editor mendorong jurnalisnya menyelaraskan berita mereka dengan apa yang menarik minat publik daripada berita yang mengandung unsur kepentingan publik.

Memproses Konten

Salah satu alat pemrosesan konten paling populer yang digunakan oleh beberapa organisasi media adalah Chartbeat. Sebagian besar organisasi berita menggunakannya untuk pengujian tajuk berita dan pengoptimalan

konten. Ada juga penggunaan alat pengecekan fakta berbasis AI seperti Reverse Search, TinEye, RevEye, InVID, dan Citizen Evidence Lab.

Pengecekan fakta tampaknya telah terintegrasi dengan kuat ke dalam proses ruang redaksi dengan sebagian besar organisasi media memiliki tim pengecekan fakta sendiri. Organisasi media yang tidak memiliki tim tersebut secara teratur bekerja dengan organisasi pengecekan fakta yang lebih besar seperti Africa Check, Pesa Check, Namibia Fact Check, Zim Fact, dan Dubawa.

Beberapa organisasi media juga telah bermitra dengan komunitas teknologi lokal untuk membangun bot pengecekan fakta. Misalnya, Code for Africa membuat Debunk Bot, yang memeriksa fakta klaim yang dibagikan di media sosial. Media di Afrika Barat, Dubawa, mengembangkan Dubawa Audio. Sebagian besar organisasi media juga melihat pemeriksaan fakta sebagai cara untuk memperkuat kredibilitas merek media mereka.

Perusahaan lain seperti PesaCheck tidak hanya mengembangkan chatbot untuk pengecekan fakta, tetapi juga alat berbasis data lainnya bagi media dan publik untuk mendapatkan akses ke, misalnya, anggaran pemerintah dan data sensus/demografi (PesaYetu), bagaimana pemerintah membelanjakan pajak publik (TaxClock) dan memeriksa janji pelaksanaan oleh politisi sebagai cara untuk meminta pertanggungjawaban mereka (Wajibisha atau PromiseTracker). (Ogola & Mare, 2023)

Distribusi Berita dan Keterlibatan Pembaca

Pada tahapan ini, perusahaan media, baik yang besar maupun kecil, paling banyak memanfaatkan perangkat AI. Hal ini terkait model bisnis yang mereka terapkan. Sebagian besar organisasi media telah mengadopsi penggunaan berbagai perangkat analisis audiens, baik yang premium maupun dari sumber terbuka.

Perangkat yang paling banyak digunakan termasuk Chartbeat, SmartOcto, dan Google Analytics. Di Afrika Selatan, perangkat seperti Content Insights, Eco-Box, Alexa, Brightcove, dan Disqus digunakan oleh sebagian besar ruang redaksi. Perangkat dan platform ini memberikan beberapa wawasan tentang audiens, misalnya, apa yang mereka baca, berapa lama mereka terlibat dengan konten, pada platform apa, dan profil mereka berdasarkan usia, minat, dan sebagainya.

Dasbor Chartbeat telah menjadi hal yang wajib dimiliki oleh sebagian besar ruang redaksi. Minat terhadap bot keterlibatan audiens juga meningkat. Di Tanzania, Dau Technologies telah mengembangkan pembaca (teknologi AI teks ke suara) yang digunakan oleh pelanggan untuk membaca surat kabar berbahasa Inggris dan Kiswahili.

TTS Mozilla, meskipun tidak dikembangkan di Afrika, juga telah digunakan oleh beberapa organisasi media di benua itu. NMG mengembangkan bot keterlibatan audiens yang disebut Kiki, meskipun saat ini bot tersebut belum beroperasi. Beberapa surat kabar di tiga wilayah tersebut kini memiliki chatbot keterlibatan audiens yang beroperasi di berbagai platform, termasuk Facebook, Telegram, dan WhatsApp. (Ogola & Mare, 2023)

Di industri media, menurut Peter N. Amponsah dan Atianashie Miracle Atianashie, secara garis besar pemanfaatan AI bisa dijelaskan dengan timeline seperti ini:

Timeline Pemanfaatan AI di Organisasi Berita

Era	Phase	Key Developments
1980s-1990s	The Early Days of AI in Journalism	Basic computer-assisted reporting; Emergence of digital tools and databases.
Early 2000s	The Emergence of Automated Content	Automated content generation for routine reports; Introduction of NLG technologies.
Mid-2000s to 2010s	Integration of Machine Learning	Use of machine learning for data analysis and trend prediction; Social media analysis.
Late 2010s	The Rise of Personalization and Recommendation Systems	AI-driven personalization algorithms; Implementation of recommendation engines.
Recent Years	Advanced AI Capabilities and Ethical Considerations	Enhanced capabilities with deep learning; Focus on fact-checking, combating misinformation and deep fakes; Ethical considerations become prominent.

Bahan: Peter N. Amponsah dan Atianashie Miracle Atianashie dalam *Navigating the New Frontier: A Comprehensive Review of AI in Journalism*

Lantas bagaimana pemanfaatan AI di industri media dalam negeri?

Aliansi Jurnalis Independen (AJI) Indonesia sudah membuat laporan bertajuk **“Asesmen Penggunaan Kecerdasan Buatan (AI) dalam Media di Indonesia: Tantangan, Peluang, dan Pengembangan Standar Etika”** pada akhir 2024 yang dapat diunduh lengkapnya di tautan ini: <https://aji.or.id/data/asesmen-penggunaan-kecerdasan-buatan-ai-dalam-media-di-indonesia-tantangan-peluang-dan>.

Penggunaannya beragam dalam proses produksi hingga distribusi konten seperti terlihat dalam tabel berikut:

Tabel 1.

NAMA MEDIA	Pencarian data/informasi awal	analisis tren	analisis audiens	pencarian/penyusunan ide liputan	penyaringan informasi	penyuntingan bahan	susun kerangka laporan	analisis data	personalisasi konten	diseminasi laporan
Zona Utara	V			V	V	V		V	V	
Narasi	V	V	V	V	V	V	V	V	V	V
Suara	V	V	V		V			V		
iNews	V	V	V	V	V	V	V	V	V	V
Kompas.com	V	V	V	V	V	V	V	V	V	V
Babad.id	V	V		V		V				
KBR Media	V			V	V	V	V		V	
Suara Surabaya	V								V	V
Katadata	V	V	V	V					V	
Tribun	V		V	V		V			V	V
Berita Jatim	V					V				

Berkaca dari studi pustaka dan diskusi terpumpun yang dilakukan oleh AJI Indonesia tersebut, dapat disimpulkan pemanfaatan teknologi AI pada ruang redaksi merupakan sebuah keniscayaan.

Para pengelola media juga memaklumi dan sepakat untuk menggunakan AI sebagai alat bantu dalam rantai produksi berita. Penggunaannya harus disertai pengawasan ketat oleh manusia guna menjaga integritas, kepercayaan, hingga menghindari bias.

Sebagai bentuk pertanggungjawaban terhadap publik, redaksi juga harus terbuka kepada pembaca terkait pemanfaatan AI dalam alur produksinya. Pada saat bersamaan, pengelola media juga perlu membuat panduan spesifik terkait penggunaan AI serta sanksi dan pelatihan berkala bagi jurnalis di organisasi medianya.

Mengenai tantangan dalam pemanfaatan AI, perusahaan media menghadapi hal yang sama dengan pihak-pihak lain. Mulai dari isu bias dan diskriminasi, transparansi algoritma, dampaknya pada lapangan pekerjaan, serta isu hak cipta.



**ALIANSI
JURNALIS
INDEPENDEN**
Alliance of Independent Journalist

BAB II.

PEMANFAATAN AI DALAM PRODUKSI, PENYEBARAN, DAN DETEKSI MISINFORMASI/ DISINFORMASI

BAB II. PEMANFAATAN AI DALAM PRODUKSI, PENYEBARAN, DAN DETEKSI MIS/DISINFORMASI

Tujuan: Setelah mempelajari buku ini, peserta latih diharapkan memahami fenomena mis-disinformasi serta pemanfaatan AI dalam proses produksi dan penyebaran informasi, hingga cara mendeteksinya.

Pertanyaan pemantik:

1. Apa perbedaan antara hoaks, misinformasi, disinformasi?
2. Gerakan cek fakta sudah berlangsung lebih dari lima tahun, kenapa tidak berhasil meredam peredaran disinformasi?
3. Kehadiran AI membantu deteksi atau memperburuk penyebaran disinformasi?

Metode penyampaian:

- Ceramah
- Praktik
- Diskusi

2.1. AI dan fenomena disinformasi

Kehadiran internet memudahkan pencarian, penyebaran, serta pertukaran informasi tanpa batasan fisik, waktu, ras, gender, kelas ekonomi, hingga geografis. Baik itu informasi yang berbasis fakta lengkap, fakta yang sudah dimodifikasi, hingga informasi yang sama sekali tidak berbasis fakta.

Secara umum pemeriksaan fakta merupakan bagian dari prinsip kerja jurnalistik. Semua jurnalis, penulis atau editor, bertanggungjawab memastikan akurasi dari informasi yang akan dipublikasikan kepada publik (Graves, 2016). Aktivitas pemeriksaan atau cek fakta pada lanskap digital dimulai pada 2003 saat FactCheck.org didirikan (Nieminen & Rapeli, 2019).

Inisiatif cek fakta erat kaitannya dengan isu politik, yang lebih menitikberatkan pada upaya pemeriksaan klaim politik (Young, Jamieson & Goldring, 2018). Selain FactCheck.org, ada portal Politifact sebagai pionir cek fakta di Amerika Serikat (Nieminen & Sankari, 2021).

Politifact yang didirikan pada 2007 memanfaatkan Truth-O-Meter, sebuah skala 'kebenaran' dengan enam titik ukur mulai dari 'True' hingga 'Pants on Fire,' sebagai cara mengkategorisasi klaim politisi. Inisiatif cek fakta ini meluas ke berbagai belahan dunia lain seiring pencalonan awal Donald Trump sebagai Presiden Amerika Serikat, isu keluarnya Inggris dari Uni Eropa (Brexit), serta meningkatnya isu geo-politik (Fischer, 2020).

Perkembangan dan inisiatif gerakan cek fakta ini juga mewarnai negara-negara di belahan selatan khatulistiwa seperti Brazil, Filipina, dan Indonesia yang dipicu oleh situasi politik pada negara-negara tersebut yang diiringi peningkatan 'perang informasi', kampanye hitam, informasi bohong, dan penyebaran konten yang bias politik (Moore, 2018).

Untuk konteks Indonesia, inisiasi cek fakta dipicu oleh wacana politik. Inisiatornya adalah Masyarakat Antifitnah Indonesia (Mafindo) yang berdiri pada 2015. Komunitas ini bermula dari Forum Anti Fitnah, Hasut, dan Hoaks (FAFHH) di Facebook. Mereka terbentuk seiring peningkatan sebaran informasi bohong pada Pemilihan Presiden 2014 yang diikuti oleh Pemilihan Kepala Daerah DKI Jakarta pada 2017 (Tomsa & Setijadi, 2018).

Pada lanskap media digital, *Tirto.id* – media daring yang berbasis di Jakarta dan Yogyakarta— melakukan upaya pemeriksaan fakta secara langsung saat Debat Calon Gubernur dan Wakil Gubernur DKI Jakarta 2017 (Kresna, 2017). Setahun setelahnya, *Tirto* menjalankan kegiatan cek fakta secara formal usai menerima sertifikasi dari International Fact-Checking Network/IFCN. Selain *Tirto*, saat itu hanya *VeraFiles* dan *Rappler* dari Filipina yang mengantongi sertifikasi IFCN di Asia Tenggara (Yuniar, 2018).

Gerakan cek fakta ini membesar seiring terbentuknya Koalisi Cek Fakta pada 5 Mei 2018. Koalisi yang diinisiasi Aliansi Jurnalis Independen (AJI), Asosiasi Media Siber Indonesia (AMSI), Masyarakat Antifitnah Indonesia, serta 24 media ini terbentuk guna mengurangi efek disruptif dari penyebaran informasi salah menjelang Pemilihan Umum 2019.

Bermula dari melatih 15 jurnalis dan pemeriksa fakta pada Februari 2018, kolaborasi ini sudah menjangkau setidaknya 5 ribu jurnalis, pers mahasiswa, serta komunitas di Indonesia. Mitra koalisi juga sudah mencapai 104 media saat Pemilihan Umum 2024.

Beragam modul atau panduan cek fakta serta literasi digital juga sudah diterbitkan untuk publik. Pendekatan melawan penyebaran informasi bohong yang semula fokus pada pembongkaran kebohongan, diperluas dengan produksi konten pre-bunking—pendekatan melawan informasi

bohong dengan memberikan peringatan bagi orang-orang sebelum mereka mendapatkan informasi bohong serupa.

Kolaborasi cek fakta sudah menjadi gerakan global. Inisiatif serupa dapat ditemui di berbagai benua lain seperti Eropa, Afrika, Amerika, hingga lintas benua. Termasuk di dalamnya pendirian organisasi pemeriksa fakta independen. Semua upaya ini mendapatkan tantangan baru sejalan dengan perkembangan teknologi AI.

2.2. Definisi

First Draft, sebuah organisasi nirlaba yang mendukung jurnalis, akademisi, dan teknologi dalam upaya pemberantasan informasi bohong di era digital, mendefinisikan tujuh jenis informasi palsu seperti di bawah ini:

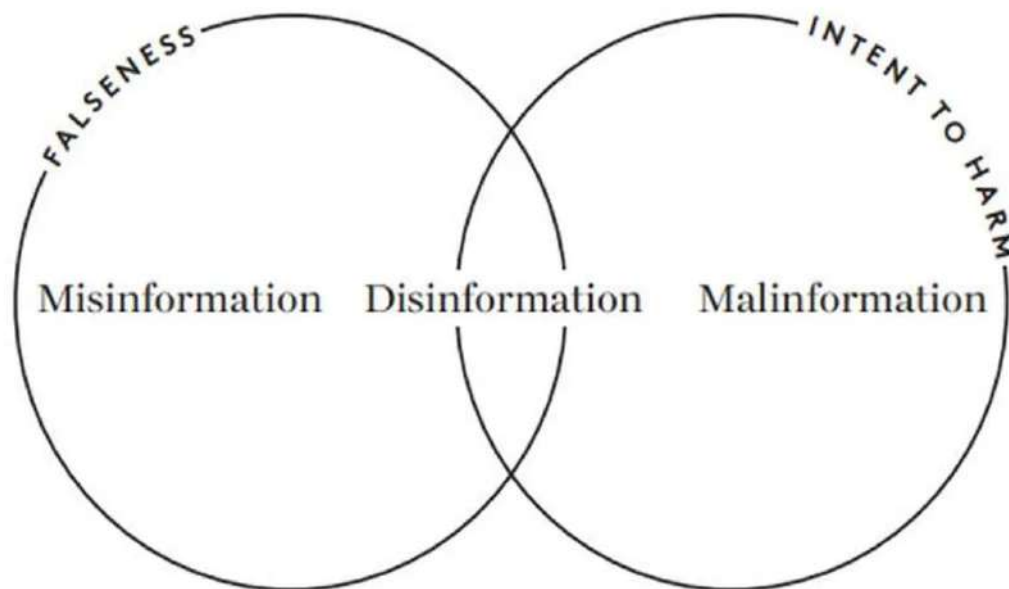
Tabel 2.

Jenis	Keterangan
Satir atau Parodi (<i>satire</i>)	<p>Konten jenis ini biasanya tidak memiliki potensi atau kandungan niat jahat, namun bisa mengecoh.</p> <p>Satir merupakan konten yang dibuat untuk menyindir atau mengkritik pihak atau kondisi tertentu. Kemasan konten berunsur parodi, ironi, bahkan sarkasme.</p> <p>Sebenarnya, satir tidak termasuk konten yang membahayakan. Akan tetapi, sebagian masyarakat masih banyak yang menanggapi informasi dalam konten tersebut sebagai sesuatu yang serius dan menganggapnya sebagai kebenaran.</p>
Koneksi yang salah (<i>false connection</i>)	Ciri paling gamblang dalam mengamati konten jenis ini adalah ditemukannya judul yang berbeda dengan isi berita. Konten jenis ini biasanya diunggah demi memperoleh keuntungan seperti

	<p>viralitas demi monetasi atau publikasi berlebih dari konten sensasional.</p>
<p>Konten yang menyesatkan (<i>misleading content</i>)</p>	<p>Konten pada jenis ini dibentuk dengan nuansa pelintiran untuk menjelekkan seseorang maupun kelompok. Konten jenis ini dibuat secara sengaja dan diharapkan mampu menggiring opini sesuai dengan kehendak pembuat informasi.</p> <p>Proses produksinya memanfaatkan informasi asli, seperti gambar, pernyataan resmi, atau statistik, akan tetapi diedit sedemikian rupa sehingga tidak memiliki hubungan dengan konteks aslinya.</p>
<p>Konten yang salah (<i>false context</i>)</p>	<p>Konten pada jenis ini disajikan dengan narasi dan konteks yang salah. Biasanya, konten ini memuat pernyataan, foto, atau video peristiwa yang pernah terjadi sebelumnya, namun klaim yang disampaikan tidak sesuai dengan fakta yang ada.</p>
<p>Konten tiruan (<i>imposter content</i>)</p>	<p>Konten yang dibuat menyerupai orang tertentu, misalnya tokoh berpengaruh, untuk mengelabui orang lain. Ini bisa juga berupa tiruan dengan mendompleng ketenaran suatu pihak atau lembaga, seperti menyaru format portal berita atau akun media sosial lembaga yang kredibel.</p>
<p>Konten yang dimanipulasi (<i>manipulated content</i>)</p>	<p>Konten jenis ini biasanya berisi hasil editan dari informasi yang pernah diterbitkan media arus utama. Gampangnya, konten jenis ini</p>

	dibentuk dengan cara mengedit konten yang sudah ada dengan tujuan untuk mengecoh publik.
Konten palsu (<i>fabricated content</i>)	Konten ini dibentuk dengan kandungan 100% tidak bisa dipertanggung-jawabkan faktanya.

Ketujuh jenis informasi palsu di atas masuk dalam tiga kategori besar sebagai berikut:



2.2.1. Misinformasi

Informasi tidak akurat atau tidak benar yang disebarluaskan tanpa adanya maksud menipu penerima informasi disebut dengan misinformasi. Informasi tersebut dibagikan oleh seseorang tidak dimaksudkan untuk kejahatan, namun ingin membantu memberikan informasi.

Pemberi informasi biasanya didorong oleh faktor sosiopsikologis di mana ia memiliki keinginan terhubung dengan orang yang beridentitas sama, seperti satu suku atau satu minat yang sama. Tetapi informasi yang diberikannya tidak melalui tahap verifikasi informasi terlebih dahulu sebelum disebarluaskan sehingga ada informasinya yang keliru atau salah.

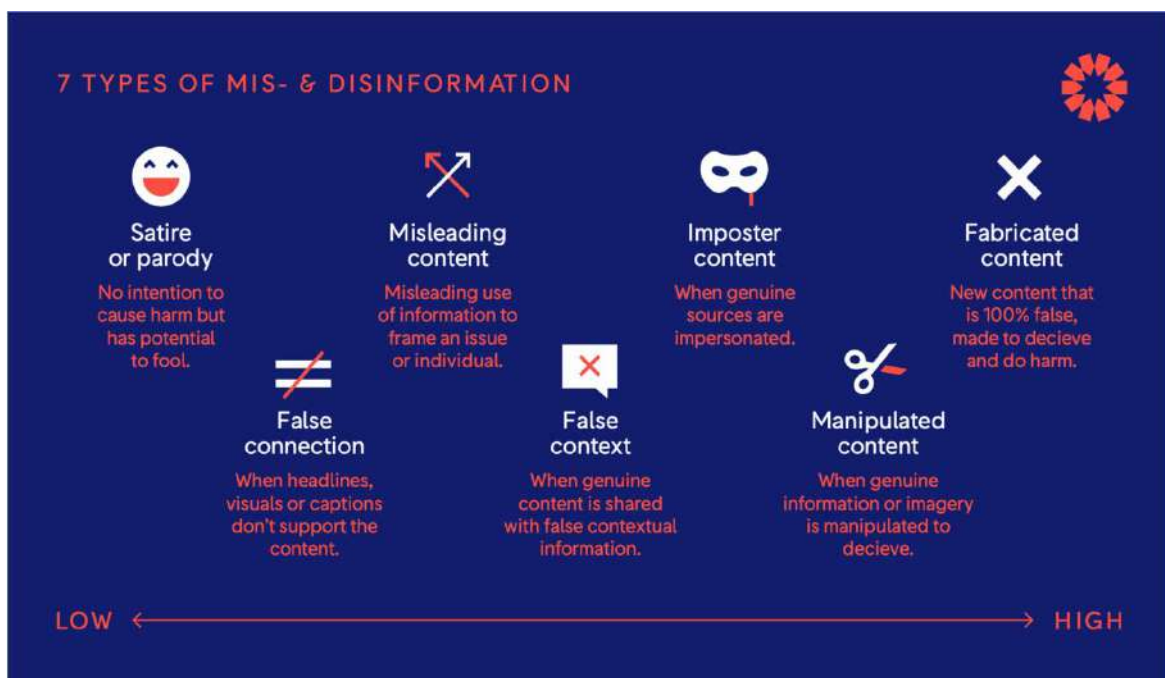
2.2.2. Disinformasi

Disinformasi merupakan informasi salah yang sengaja dibuat dan disebar dengan tujuan untuk mengelabui penerima pesan. Pemberi informasi sadar bahwa informasi yang disebar palsu (*fabricated*) dan tetap menyebarkan informasi tersebut untuk mempengaruhi opini publik sehingga ia mendapat keuntungan tertentu dari usahanya menyebarkan informasi palsu tersebut.

2.2.3. Malinformasi








Malinformasi merupakan informasi yang benar berdasarkan penggalan atau keseluruhan fakta obyektif. Tetapi, cara pengemasan informasinya dibuat sedemikian rupa agar merugikan pihak lain. Biasanya informasi ini digunakan untuk pelecehan (verbal), ujaran kebencian dan diskriminasi, serta penyebaran informasi hasil pelanggaran privasi dan data pribadi.

Terkait dengan intensinya, First Draft mengkategorikan informasi palsu tersebut sebagai berikut:



Jenis konten satir atau parodi dianggap memiliki intensi merusak atau menyakiti yang paling rendah. Sementara konten palsu (sengaja dibuat), termasuk disinformasi, memiliki intensi merusak atau menyakiti paling tinggi.

First Draft juga menerbitkan matriks perihal informasi palsu sebagai berikut:

FIRSTDRAFT		MISINFORMATION MATRIX					
	 SATIRE OR PARODY	 FALSE CONNECTION	 MISLEADING CONTENT	 FALSE CONTEXT	 IMPOSTER CONTENT	 MANIPULATED CONTENT	 FABRICATED CONTENT
POOR JOURNALISM		✓	✓	✓			
TO PARODY	✓				✓		✓
TO PROVOKE OR TO 'PUNK'					✓	✓	✓
PASSION				✓			
PARTISANSHIP			✓	✓			
PROFIT		✓			✓		✓
POLITICAL INFLUENCE			✓	✓		✓	✓
PROPAGANDA			✓	✓	✓	✓	✓

Berdasarkan matriks di atas, jenis-jenis informasi palsu itu dapat dipicu oleh beragam hal, seperti lemahnya kualitas jurnalisme, keisengan atau kehendak memparodikan fenomena atau kejadian tertentu, keinginan mendapatkan keuntungan, pengaruh politik, hingga kebutuhan melakukan propaganda.

Meski ada beragam jenis dan kategorisasi informasi palsu, publik di Indonesia kerap menyebutnya dengan satu istilah saja, hoaks. Penggunaan istilah ini jadi sangat umum bagi warganet atau publik Indonesia dan media arus utama ikut mempopulerkannya.

Riset “Pengaturan Konten Ilegal dan Berbahaya di Media Sosial” oleh Pemantau Regulasi dan Regulator (PR2) Media memperlihatkan konten misinformasi atau kebohongan menjadi kedua terbanyak soal jenis konten yang sering ditemui di media sosial, setelah ujaran kebencian (Wendratama dkk, 2023)

Mengapa orang masih mudah percaya informasi bohong, berkaca pada gerakan kolaboratif pemeriksaan fakta yang sudah ada sejak 2018 lalu?

Penelitian Engage Media --lembaga nirlaba yang mendukung hak-hak digital, teknologi terbuka dan aman, dan dokumenter isu sosial—bertajuk “Ekonomi Politik Cek Fakta di Indonesia” (2024) mencatat, penyelesaian

misinformasi perlu dilihat dalam praktik yang lebih luas lewat ekosistem informasi.

Studi ini menyatakan bahwa praktik cek fakta perlu ditunjang pemahaman mengenai ekosistem informasi di Masyarakat. Sehingga nantinya yang dikaji bukan sekadar penilaian dan literasi media, melainkan strategi membentuk ekosistem informasi yang sehat (Garnesia et all, 2024).

Penelitian tersebut juga menyoroti perkembangan teknologi AI yang dapat menjadi pedang bermata dua bagi pemeriksa fakta. Pertama, teknologi AI membantu proses *fact-checking* menjadi lebih cepat dan efisien. Tetapi di sisi lain *deepfake* dan *cheap fake* yang dihasilkan dari teknologi AI juga menyulitkan kerja-kerja pemeriksa fakta. Penggunaan teknologi ini membuat *deepfake* dan *cheap fake* semakin sulit dibedakan dengan konten original. Belum lagi potensi teknologi AI yang kerap digunakan sebagai alat propaganda atau *influence operation* di media sosial.

Kekhawatiran ini benar-benar terjadi. Setidaknya itulah temuan para peneliti dari Universitas Boras, Universitas Lund, dan Universitas Ilmu Pertanian Swedia. Mereka mendapati 139 dari 229 jurnal makalah yang diduga diproduksi menggunakan kecerdasan artifisial generatif. Makalah-makalah itu dengan mudah ditemukan pada layanan Google Scholar (Haider, 2024)

Ahmed Abdeen-Hamed, peneliti tamu di Universitas Binghamton Thomas J. Watson College of Engineering and Applied Science dan kolaboratornya, Xindong Wu dari Universitas Teknologi Hefei, memproduksi xFakeSci, algoritma pembelajaran baru yang dapat membedakan artikel yang dihasilkan generatif AI hingga 94 persen dari total 3.942 sampel artikel pada rentang 2010-2024 (Hamed, A.A., Wu, 2024).

Kembali pada konteks mis-disinformasi, kita perlu memahami bagaimana raksasa teknologi memanfaatkan data-data penggunaannya. Secara sadar atau tidak, pengguna beragam aplikasi digital, jika kita tidak menyebut diri sebagai konsumen, sudah pasti menyetorkan data. Mulai dari data pribadi, kebiasaan berinteraksi di internet, hingga preferensi terkait topik hingga pilihan berbelanja daring saat memanfaatkan aplikasi-aplikasi tersebut.

2.3. Pemanfaatan AI dalam Produksi Mis-Disinformasi

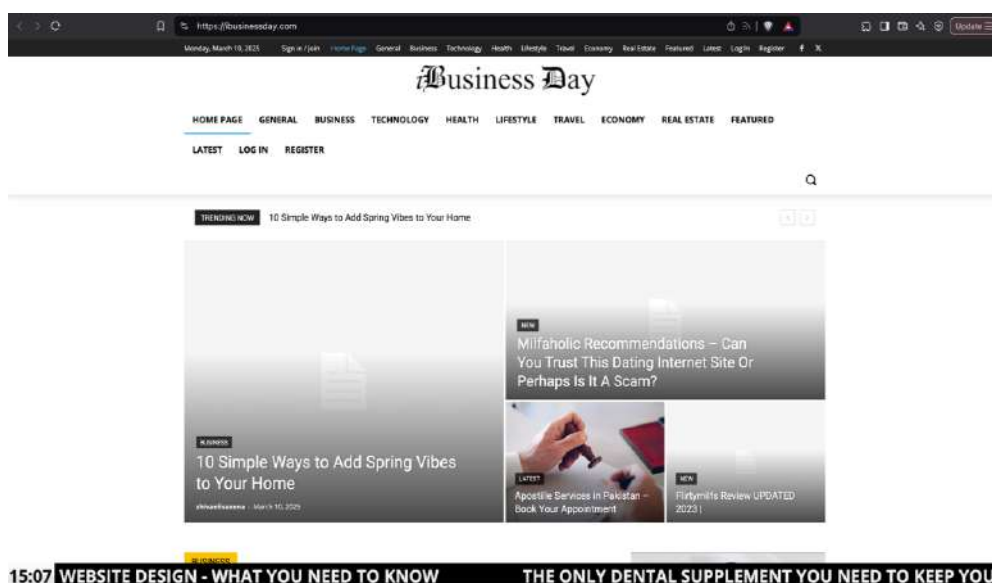
Secara umum pemanfaatan kecerdasan artifisial untuk produksi konten di media sosial dapat terbagi menjadi empat jenis:

- Teks : produksi artikel memanfaatkan pembangkit AI.
- Audio : produksinya berupa suara dan disebarakan via media sosial.
- Foto : produksi berupa gambar (sebagian rekayasa atau sama sekali baru) yang disebarakan via media sosial.
- Video: produksi berupa gambar dan suara (sebagian rekayasa atau sama sekali baru) yang disebarakan via media sosial.

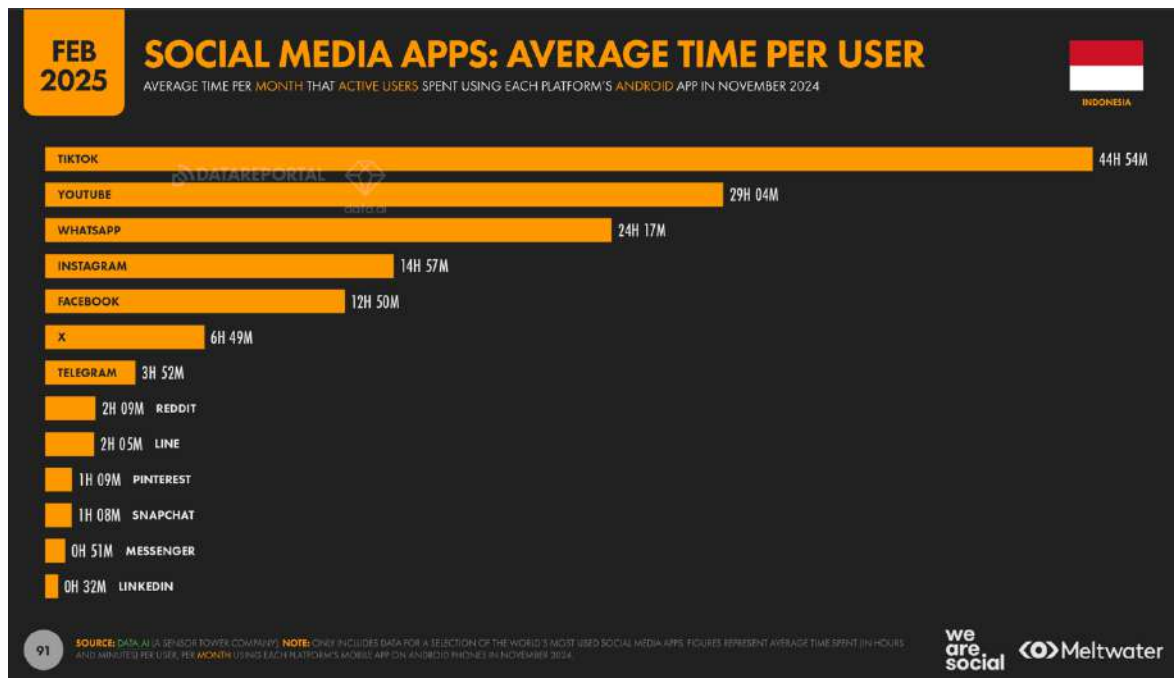
Pemanfaatan konten-konten yang dikembangkan dengan AI dan dipublikasikan dalam portal yang menyerupai portal berita itu sudah terjadi.

Hal itu terdeteksi oleh NewsGuard, sebuah alat yang dikembangkan untuk membantu publik mengidentifikasi ancaman misinformasi pada portal-portal berita. Pemantauan sejak awal 2023 menemukan 1.254 portal berita yang kontennya diproduksi AI dengan keterlibatan manusia yang sangat minim atau sama sekali tanpa manusia dalam 16 bahasa, masing-masing: Arab, Cina, Ceko, Belanda, Inggris, Perancis, Jerman, Indonesia, Italia, Korea, Portugis, Rusia, Spanyol, Tagalog, Thailand, dan Turki (NewsGuard, 2025).

Salah satu portal yang teridentifikasi dan masih dapat diakses publik adalah [ibusinessday.com](https://businessday.com). Sekilas, tata letak dan penempatan artikel atau kontennya menyerupai portal media arus utama. Namun saat ditelisik lebih dalam, hampir seluruh kontennya diproduksi atau dibangkitkan AI.



Temuan serupa di Indonesia belum banyak diungkap dan ini membuka peluang untuk adanya penelitian lanjutan. Namun, produksi konten yang menggunakan AI itu bisa ditemukan pada beragam media sosial, termasuk TikTok, aplikasi yang rata-rata lama penggunaannya di Indonesia lebih dari 44 jam dalam sebulan (WeAreSocial, 2025).



Konten-konten yang mengandung disinformasi itu juga cukup luas isunya, tidak hanya terkait dengan isu politik lokal namun juga isu luar negeri. Berikut contohnya:



Konten disinformasi berupa video ini menampilkan salah satu calon gubernur Jawa Barat, Dedi Mulyadi (kiri) yang katanya akan membagikan hadiah uang kepada warganet menjelang peringatan Hari Kemerdekaan 17 Agustus 2024. Video tersebut sudah dimanipulasi dengan menghilangkan suara asli dan menggantinya dengan audio seolah-olah Dedi Mulyadi yang berbicara hendak membagikan hadiah. Manipulasi itu diperkuat dengan teks di dalam kontennya.



Dua konten disinformasi ini merupakan tangkapan layar dari sebuah konten video yang mengangkat isu kebakaran di California, Amerika Serikat pada awal 2025. Video tersebut sudah dimanipulasi menggunakan AI sehingga menampilkan kejadian kebakaran yang melebihi faktanya, seperti terbakarnya tulisan 'Hollywood'.

Pemanfaatan AI dalam format *deep fake* untuk produksi konten disinformasi ini juga terpantau pada proses pemilihan umum tahun 2024 di berbagai negara, termasuk Indonesia. *Deep fake* adalah video, gambar atau klip suara yang dibuat menggunakan kecerdasan artifisial dan terlihat atau terdengar seperti aslinya.



Tangkapan layar dari siaran Metro TV pada 30 Oktober 2023 ini menayangkan Presiden ke-7 Indonesia, Joko Widodo berpidato dalam bahasa Mandarin. Ini merupakan informasi bohong. Produksi videonya menggunakan AI dengan cara mengganti suara aslinya menjadi suara berbahasa Mandarin.



Tangkapan layar yang menampilkan Presiden ke-2 Indonesia, Soeharto, ini juga diproduksi menggunakan AI dan digunakan oleh Partai Golkar untuk mempromosikan partainya pada Pemilihan Umum 2024. Jika dicermati

videonya, maka karakter yang tampil itu mendorong masyarakat Indonesia akan menggunakan hak pilihnya pada 14 Februari 2024. Seperti kita ketahui bersama, tokoh dalam video tersebut sudah meninggal sejak 27 Januari 2008. Dalam video ini, penampilan visual tokoh serta suaranya dimanipulasi dengan bantuan AI.

Pemanfaatan AI ini terjadi juga pada isu politik luar negeri, seperti contoh tangkapan layar di bawah ini:



Tangkapan layar dari unggahan jurnalis Eliot Higgins di akun X miliknya memperlihatkan karakter yang mirip Donald Trump melarikan diri dan ditangkap polisi. Manipulasi gambar memanfaatkan AI ini muncul seiring dengan adanya dakwaan terhadap Trump terkait kasus hubungan seksnya dengan bintang porno Stormy Daniels pada 2006. Trump diadili karena

diduga menyuap korban untuk bungkam agar tidak menghambat proses pencalonannya sebagai presiden.

Slew of deepfake video adverts of Sunak on Facebook raises alarm over AI risk to election

Research finds more than 100 paid ads impersonating PM were promoted on social media platform in last month

● UK politics live - latest updates



▶ The deepfake videos of Rishi Sunak originated from 23 countries and may have been seen by as many as 400,000 people on Facebook. Photograph: Jeff Owers/BBC/AFP/Getty Images

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

AI and deepfakes blur reality in India elections

18 May 2024

Share Save

Meryl Sebastian
BBC News, Kochi



Fact-checkers say an avatar of Duwaraka was created digitally for a YouTube stream

In November last year, Muralikrishnan Chinnadurai was watching a livestream of a Tamil-language event in the UK when he noticed something odd.

Tangkapan layar berikut ini memperlihatkan video *deep fake* yang meniru identitas Perdana Menteri Inggris, Rishi Sunak (kiri). Lebih dari 100 iklan video *deepfake* Rishi Sunak dipromosikan di Facebook dalam sebulan. Iklan ini menghabiskan lebih dari £12.929 atau sekitar Rp240 juta untuk 143 iklan, yang berasal dari 23 negara, termasuk Amerika, Turki, Malaysia dan Filipina.

Sementara tangkapan layar di sisi kanan memperlihatkan Duwaraka, putri Velupillai Prabhakaran, pemimpin militan Macan Tamil, tampak mendesak warga Tamil di seluruh dunia untuk berjuang secara politik demi kebebasan mereka. Video itu muncul menjelang Pemilu di India. Masalahnya adalah Duwaraka sudah meninggal lebih dari satu dekade sebelumnya. Penggunaan video seperti ini mirip dengan kasus di Indonesia, di mana video *deepfake* Presiden Soeharto digunakan untuk mengkampanyekan Golkar.

NOVIAN READER BUSINESS OCT 3, 2023 7:00 AM

Slovakia's Election Deepfakes Show AI Is a Danger to Democracy

Fact-checkers scrambled to deal with faked audio recordings released days before a tight election, in a warning for other countries with looming votes.



PHOTOGRAPH: ZUZANA OBOJVA/GETTY IMAGES

Pemanfaatan *deep fake* juga teridentifikasi pada Pemilu Slovakia 2023. Hanya dua hari sebelum Pemilu Slovakia, yakni saat masa tenang, sebuah rekaman audio diunggah ke Facebook. Di dalamnya terdapat dua suara, yaitu Michal Šimečka, yang memimpin partai liberal Progresif Slovakia, dan Monika Tódová, wartawan dari surat kabar harian Denník N.

Mereka tampak mendiskusikan cara melakukan kecurangan dalam pemilu, antara lain dengan membeli suara dari kelompok minoritas di negara tersebut. Audio ini kemudian menjadi kontroversi. Beberapa pakar berpendapat audio ini juga berkontribusi pada anjloknya suara Michal terhadap kompetitornya yang juga merupakan representasi dari partai sosialis pro-Rusia, Robert Fico.

Kembali ke konteks Indonesia, pemanfaatan *deep fake* yang didukung teknologi AI ini diyakini turut mempengaruhi integritas Pemilu 2024. Generative-AI dinilai dapat meningkatkan produksi dan penyebaran mis/disinformasi selama Pemilu 2024, kata Saferinternetlab dari [Centre for Strategic and International Studies](#) yang menggelar survei terhadap 189 responden dan melakukan wawancara dengan ahli pada November-Desember 2024. Video deepfake (49,47 persen) dan gambar berbasis AI (27,66 persen) dianggap menjadi ancaman terbesar bagi integritas pemilu.

Selain dalam konteks pemilu, Gen-AI juga digunakan untuk progranda. Kelompok teroris ISIS dan Al-Qaeda sudah menyelenggarakan pelatihan AI

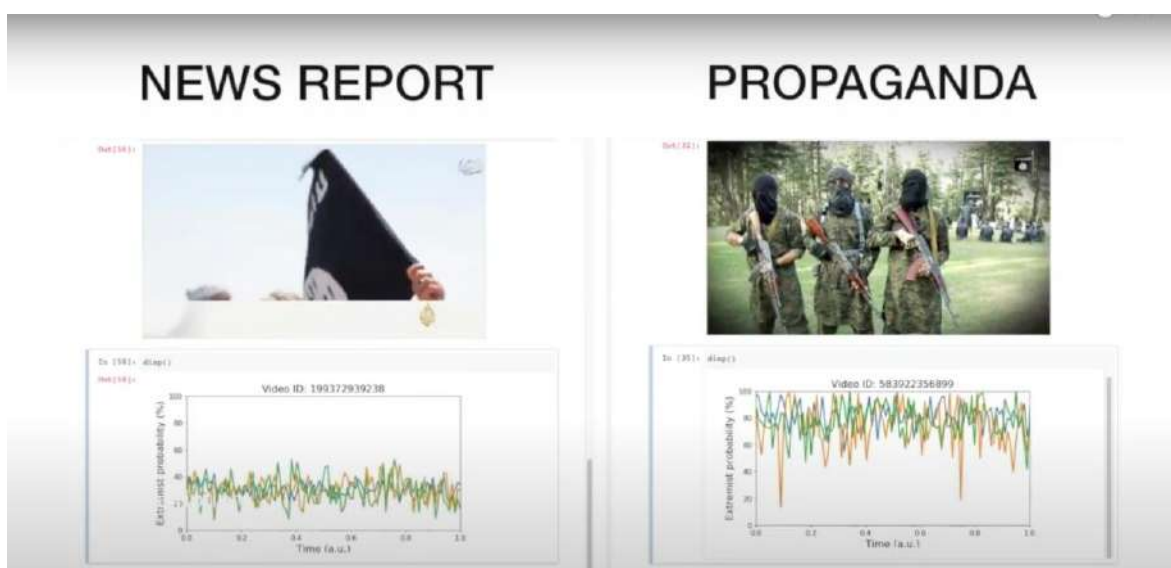
dan menerbitkan panduan pembuatan konten AI sejak 2024, kata laporan [The Washington Post](#).

Seruan untuk menggunakan perangkat AI makin gencar, seperti diutarakan oleh salah satu pendukung ISIS dalam ruang diskusi privat mereka, Al Kurdi 500. Ini menggambarkan soal bagaimana penyebaran propaganda lewat berita. Teknologi AI memudahkan proses produksinya.

Tujuh hari sejak pesan tersebut dilayangkan pada 22 Maret 2024, ISIS menyerang sebuah konser di Moskow. Salah satu pendukungnya, Hasad, segera menyerukan pembuatan video berbasis AI.

Selang empat hari, Hasad merilis *News Harvest*, program siaran harian dari ISIS berbasis AI, menggunakan video dan gambar AI. Namun perdebatan muncul, apakah haram atau halal memunculkan foto wajah. Sehingga, perubahan dilakukan dalam konten yang disiarkan, yang tadinya memuat foto dengan raut muka utuh, kini, di-*blur*.

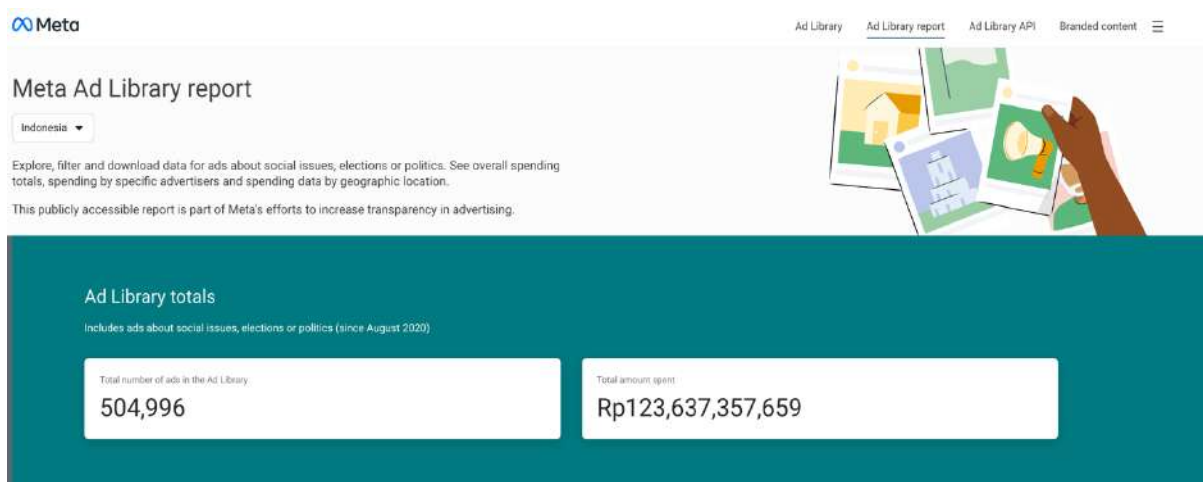
Untuk menangkal konten-konten propaganda berbasis AI, sejumlah program sudah dilakukan di berbagai negara. Tangkapan layar di bawah ini menunjukkan alat berbasis AI dan algoritma untuk mendeteksi propaganda yang dikembangkan oleh [pemerintah Inggris dan konsultan ASI Data Science](#). Secara otomatis, alat ini dapat membedakan visual dan narasi yang dirilis oleh kelompok teroris atau individu dengan berita valid yang dipublikasikan oleh media.



2.4. Penyebaran Mis-Disinformasi dengan AI

Sebelum membahas perihal penyebaran AI, kita perlu memahami dulu bagaimana sebenarnya AI dapat membaca seluruh data 'kita' yang berseliweran di internet. Data tersebut berkaitan dengan aktivitas kita selama terkoneksi internet. Mulai dari permohonan data saat kita memasukkan kata pencarian di mesin pencari (search engine), penelusuran kita pada peramban (browser), hingga interaksi kita di beragam media sosial. Termasuk beragam konten yang kita lihat, kita sebar, kita respon hingga konten yang kita lewatkan. Data ini juga termasuk informasi perangkat, penyedia layanan internet, sampai identitas daring kita yang teridentifikasi lewat *internet protocol address*.

Salah satu contoh pemanfaatan data itu bisa dilihat pada perpustakaan iklan Meta yang kompilasi datanya bisa diakses publik via tautan: [Meta Library Ad](#) seperti tangkapan layar di bawah ini:



Perpustakaan iklan Meta ini juga membedakan jenis iklan politik dan iklan lainnya. Khusus untuk isu politik, mereka juga mencantumkan pemasang iklannya siapa, besaran nilainya, sebaran iklan, hingga preferensi kelompok usia pengguna media sosial Facebook atau Instagram (bagian dari grup Meta).

Berikut contoh tampilan iklan politik yang sudah tidak aktif masa pemasangan iklan politik dengan studi kasus kata kunci "Atalia" dari nama Atalia Praratya, anggota Komisi VIII-DPR RI asal Jawa Barat, yang meraih suara tertinggi sebagai calon anggota DPR dari Provinsi Jawa Barat:

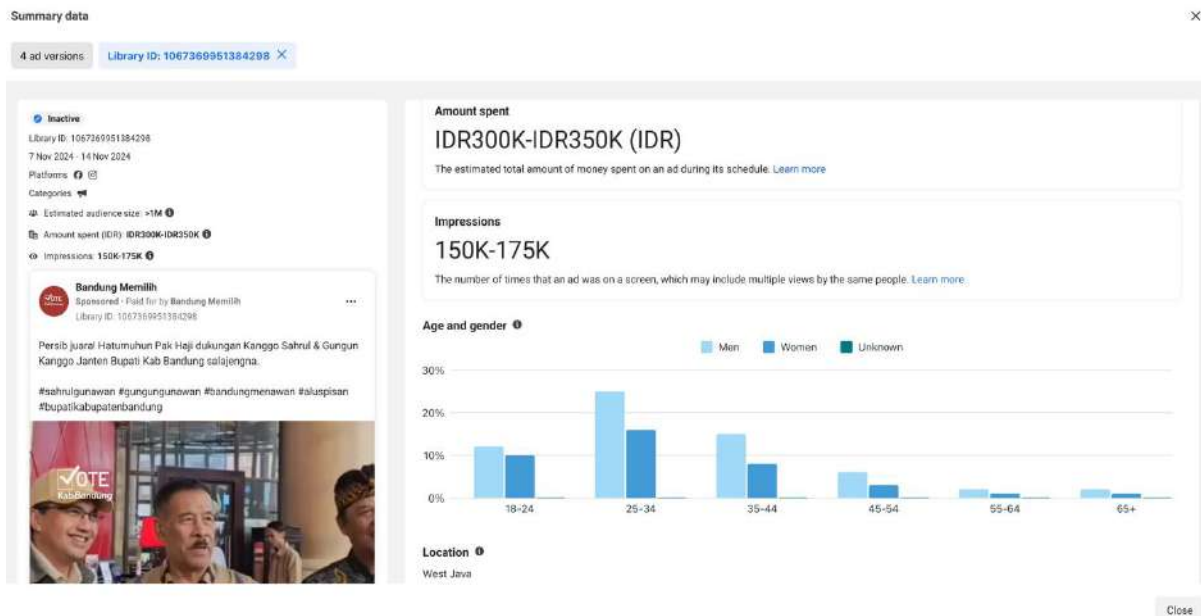
Meta Ad Library interface showing two ad entries. The first ad is from 'Bandung Memilih' with Library ID 1067369951384298, launched on Nov 13, 2024. The second ad is from 'Barisan Kang Ridwan Solichin' with Library ID 1067369951384298, launched on Nov 7, 2024. Both ads are categorized as 'Issues, elections or politics' and are inactive.

Identitas pemasang iklan pada perpustakaan iklan ini adalah akun Bandung Memilih yang juga tercatat identitasnya melalui rangkaian angka yang disebut Library ID. Durasi pemasangan iklan politik juga teridentifikasi, serta pemasangan konten berupa iklan politik itu tayang di Facebook, Instagram, atau keduanya.

Summary data for Library ID: 1067369951384298. The ad is from 'Bandung Memilih' and is categorized as 'Issues, elections or politics'. The advertiser's contact information includes a phone number (+6285221107198), email address (akunprakteksaja@gmail.com), website (https://www.facebook.com/kabbandungmemilih/), and address (BANDUNG, Jawa Barat). The ad content includes the text: 'Perebut juaral! Haturnuhun Pak Haji dukungan Kanggo Sahrul & Gunung Kanggo Janten Bupati Kab Bandung salajengna.' and hashtags: #sahrulgunawan #gununggunawan #bandungmenawan #aluspisan #bupatikabupatenbandung.

Tangkapan layar ini memberikan informasi lebih detail dari pemasang iklan dengan kata kunci "Atalia" tadi. Nampak dalam tangkapan layar ada nomor kontak hingga alamat surat elektronik dari akun "Bandung Memilih". Lantas mengapa kontennya di sisi kiri tangkapan layar tidak berhubungan dengan kata kunci "Atalia"?

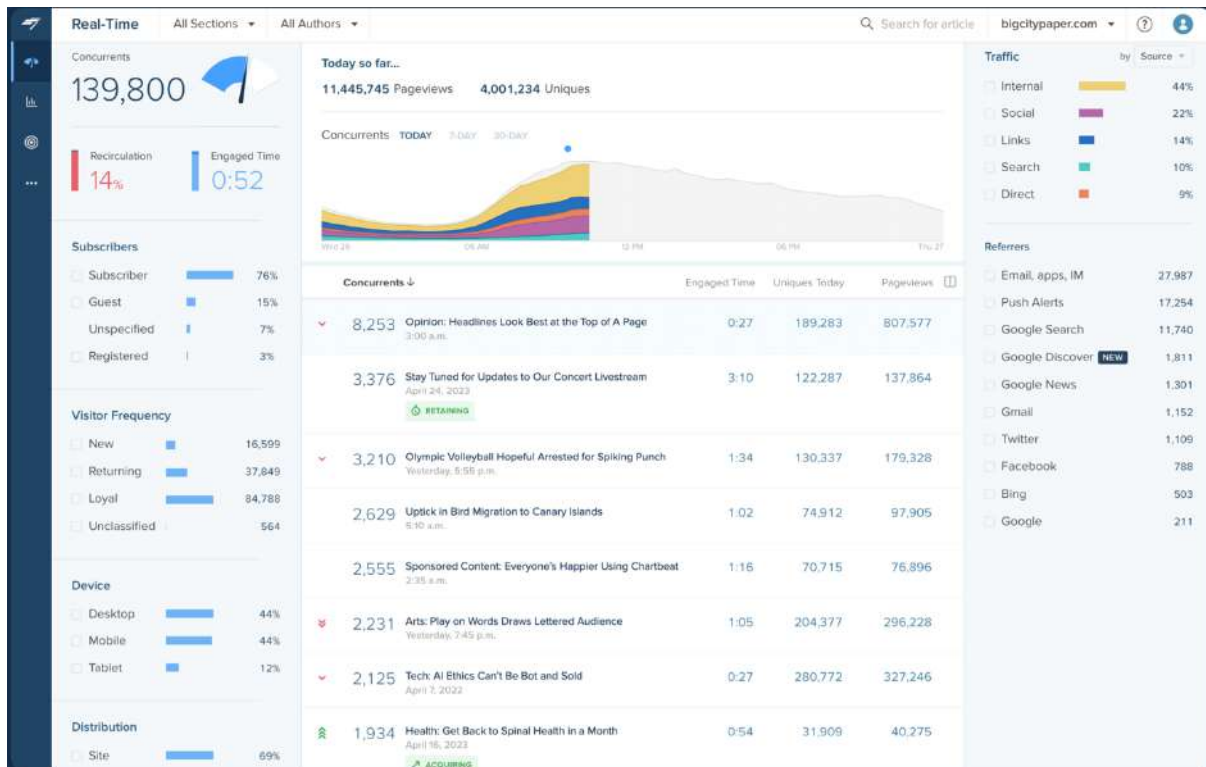
Melalui penelusuran di perpustakaan iklan ini kita juga dapat mengetahui akun “Bandung Memilih” juga memasang iklan pada konten lain. Pada contoh ini akun tersebut juga mengkampanyekan calon kepala daerah Kabupaten Bandung, Syahrul Gunawan. Hal itu terlihat pada caption di sisi kiri tangkapan layar.



Pada tangkapan layar berikutnya kita dapat mengetahui berapa besar nominal konten ‘iklan politik itu dibelanjakan. Berdasarkan informasi di tangkapan layar, kita mengetahui untuk konten seperti di sisi kiri, pengiklan membayar antara Rp300.000-Rp350.000 untuk iklan tersebut. Belanja iklan politik itu menyasar pengguna Facebook dan Instagram berusia antara 18-44 tahun, dengan sasaran terbesar adalah kelompok usia 25-34 tahun. Target dari iklan tersebut adalah seluruh pengguna Facebook dan Instagram dalam rentang usia tertentu di seluruh wilayah Jawa Barat.

Beragam informasi yang dapat kita akses dalam laporan iklan tersebut memanfaatkan AI dalam proses pengumpulan datanya. Melalui laporan tersebut, kita juga mengetahui pemasang iklan dapat menyasar target pasarnya sesuai dengan preferensi yang diinginkannya, berkat AI.

Praktik membaca data seperti ini juga bisa dipakai oleh perusahaan media dalam berita dan informasi yang banyak diakses. Salah satunya bisa dengan memanfaatkan layanan seperti Chart Beat.



Pemanfaatan layanan seperti ini juga lazim menggunakan dashboard atau monitor yang dibuat oleh tim internal dari perusahaan media. Dengan fasilitas ini, tim redaksi dapat mengetahui konten pemberitaan mana yang diminati warganet, bagaimana cara warganet mengakses konten tersebut, hingga berapa lama mereka bertahan dan melanjutkan penelusuran di portal pemberitaan media tersebut.

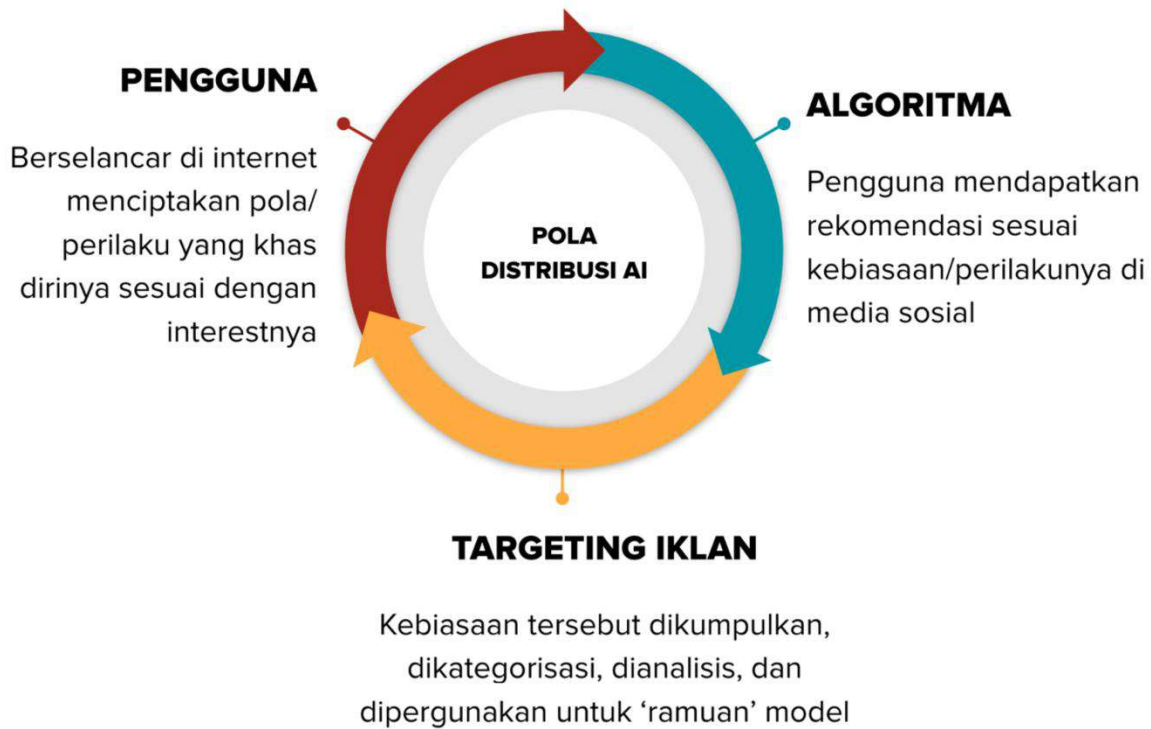
Dengan memanfaatkan data-data tersebut, pengelola media dapat memilih dan memprioritaskan konten tertentu untuk ditindaklanjuti. Termasuk di dalamnya adalah untuk kebutuhan distribusi konten.

Aktor-aktor jahat yang memiliki agenda tersendiri juga mampu memanfaatkan AI guna memaksimalkan penyebaran konten disinformasinya. Mereka menggunakan akun robot dalam penyebaran kontennya. Salah satu contoh kasusnya adalah pemanfaatan akun robot pada platform Twitter (sekarang X) agar sebuah tagar menjadi viral di media sosial menjelang Pemilihan Presiden 2019 (Fahmi, 2019).

Kemunculan akun-akun robot atau palsu ini kontribusinya mencapai 26,76 persen, atau yang paling tinggi sebagai sumber produksi disinformasi setelah influencer atau selebriti (saferinternetlab.org, 2024).

Dalam konteks distribusi informasi atau konten pada media sosial, pengguna akan mendapat konten-konten sejenis yang memang tercatat

atau terbaca oleh AI disukai pengguna. Kondisi seperti ini yang bakal menyebabkan algoritma konten yang muncul di satu akun berbeda dengan akun lainnya, karena dipengaruhi oleh perilaku dan interaksi pengguna. Secara sederhana, pola ini terlihat pada ilustrasi berikut:



2.5. Deteksi Mis-Disinformasi dengan AI

Sebelum mempelajari cara memanfaatkan AI guna mendeteksi mis-disinformasi, ada baiknya memahami dulu beberapa percabangan AI. Dengan memahaminya kita dapat memaksimalkan penggunaan AI secara tepat untuk memecahkan atau mendeteksi konten yang mengandung mis-disinformasi dengan lebih akurat.

1. Natural Language Processing (NLP)

NLP termasuk salah satu bentuk awal AI, yang fokusnya pada pemrosesan dan pemahaman bahasa manusia oleh komputer. Tujuan NLP adalah membuat mesin bisa memahami, menganalisis, menghasilkan, dan merespons bahasa alami seperti manusia. Selain itu, NLP dapat dipergunakan juga untuk menganalisa sentimen (Tauli, 2019).

Contoh produk yang memanfaatkan NLP, antara lain, Google Translate untuk menerjemahkan bahasa, Siri serta Google Assistant yang dapat

memahami dan merespon perintah suara, serta aplikasi pengecekan tata bahasa seperti Grammarly.

2. Large Language Models (LLM)

LLM adalah model AI berbasis *deep learning* yang dilatih menggunakan jumlah data teks yang sangat besar untuk memahami dan menghasilkan teks dengan cara yang sangat mirip manusia. LLM adalah bagian dari NLP, tetapi lebih spesifik karena menggunakan arsitektur transformer (seperti GPT-3, GPT-4, BERT, T5, dll.).

Jenis model ini mempertimbangkan semua teks sekaligus dan efektif dalam memahami rangkaian kata. Model-model ini juga secara umum menjadi lebih baik karena menggunakan lebih banyak parameter (Taulli, 2023).

Contoh LLM:

- GPT-4 (OpenAI): Dapat menghasilkan teks berdasarkan input pengguna.
- BERT (Google): Digunakan untuk memahami konteks kata dalam pencarian Google.
- LLaMA (Meta AI): Model open-source yang bisa digunakan untuk berbagai tugas NLP.

LLM berbeda dari NLP secara umum. NLP mencakup banyak teknik, sementara LLM adalah model besar yang menggunakan NLP untuk memahami dan menghasilkan bahasa.

3. Analisis jaringan sosial

Teknologi AI bekerja berdasarkan data yang mereka dapatkan dari pengembangnya. Salah satunya adalah data yang berseliweran di internet, termasuk data pengguna media sosial saat mengakses atau bereaksi terhadap konten tertentu. Bagi pengembang AI, data-data tersebut dapat dikategorisasikan berdasarkan akun, sentimen, serta interaksi antar akun, termasuk tren dalam rentang waktu tertentu.

4. Pengenalan teks, foto, dan video

Teknologi AI yang memanfaatkan sumber data terbuka, seperti data pengguna internet, dapat melakukan kategorisasi hingga verifikasi informasi. Namun salah satu tantangan dalam pemanfaatan AI untuk

mendeteksi konten berbasis visual adalah terbatasnya layanan verifikasi visual yang tidak berbayar.

2.5.1. Pemeriksaan Teks

Di awal sesi, tanpa bantuan perangkat apa pun, peserta diminta untuk mengidentifikasi [dua teks berbasis AI](#) dan diminta menjelaskan apa saja ciri-cirinya.

Contoh teks 1

We are dedicated journalists, reporters, and storytellers committed to showcasing the unique fabric of our community. Through our diligent efforts, we aim to reflect the diversity, resilience, and spirit that define us.

At County Local News, we are the voice that amplifies the accomplishments and milestones achieved by our fellow residents. From highlighting the achievements of local entrepreneurs, artists, and innovators, to shedding light on the extraordinary individuals who make a positive difference in our midst, our mission is to celebrate and honor the remarkable people who call this county home.

We are the bridge that connects neighbors and builds a sense of unity. Whether it's reporting on local events, community initiatives, or important civic matters, we strive to keep our readers informed and engaged. We encourage discussions, foster connections, and nurture a strong sense of belonging within our county by facilitating open dialogue.

We are the lens that captures the beauty of our surroundings. From the breathtaking landscapes to the hidden gems within our neighborhoods, we provide a visual narrative reminding us of our extraordinary world. Through vivid imagery and captivating storytelling, we transport our readers through our county's many facets, fostering an appreciation for the place we call home.

Contoh teks 2

Konflik di Sigi, Sulawesi Tengah, terjadi pada November 2020. Insiden ini melibatkan serangan yang diduga dilakukan oleh kelompok teroris Mujahidin Indonesia Timur (MIT) yang berbasis di Poso. Berikut adalah beberapa detail penting mengenai konflik tersebut:

1. Serangan di Desa Lembantongoa:
 - o Pada 27 November 2020, terjadi serangan di Desa Lembantongoa, Kabupaten Sigi.
 - o Serangan tersebut menewaskan empat orang dan menyebabkan beberapa rumah dibakar.
2. Pelaku:
 - o Serangan ini diduga dilakukan oleh kelompok MIT, yang dipimpin oleh Ali Kalora.
 - o MIT adalah kelompok militan yang berafiliasi dengan ISIS dan telah lama terlibat dalam berbagai aksi kekerasan di Sulawesi Tengah.
3. Respon Pemerintah:
 - o Pemerintah Indonesia melalui TNI dan Polri segera melakukan operasi pengejaran terhadap pelaku.
 - o Operasi Tinombala, yang sudah berlangsung lama untuk memberantas MIT, ditingkatkan intensitasnya setelah adanya serangan ini.
4. Dampak Terhadap Masyarakat:
 - o Serangan ini menciptakan rasa takut di kalangan masyarakat setempat.
 - o Beberapa warga terpaksa mengungsi karena khawatir akan adanya serangan lanjutan.
5. Latar Belakang Konflik:
 - o MIT telah aktif di wilayah Sulawesi Tengah selama bertahun-tahun.
 - o Kelompok ini terkenal karena keterlibatannya dalam serangkaian serangan teror, pembunuhan, dan bentrokan dengan pasukan keamanan Indonesia.

Konflik ini menunjukkan tantangan yang dihadapi Indonesia dalam menangani kelompok-kelompok militan di wilayah terpencil. Pemerintah terus berusaha untuk menegakkan keamanan dan stabilitas di daerah tersebut, namun masih banyak pekerjaan yang perlu dilakukan untuk mengatasi akar permasalahan dan mencegah kekerasan lebih lanjut.

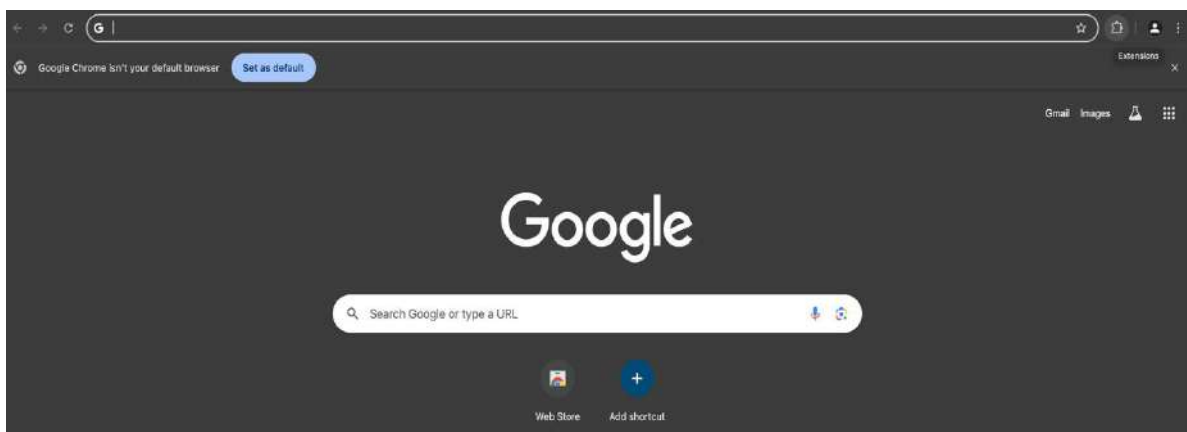
Di akhir diskusi, tutor menjelaskan bahwa keduanya merupakan teks buatan AI. Ciri-ciri yang sering muncul, di antaranya:

- Kosakata yang digunakan seringkali berbunga-bunga (*sophisticated*).
- Banyak pengulangan kalimat.
- Bentuk paragraf tidak terstruktur.
- Untuk beberapa perangkat tertentu, seperti *ChatGPT*, struktur penulisan seringkali dimulai dengan ringkasan dalam bentuk beberapa kalimat, kemudian dilanjutkan dengan penomoran atau *bullet points*.

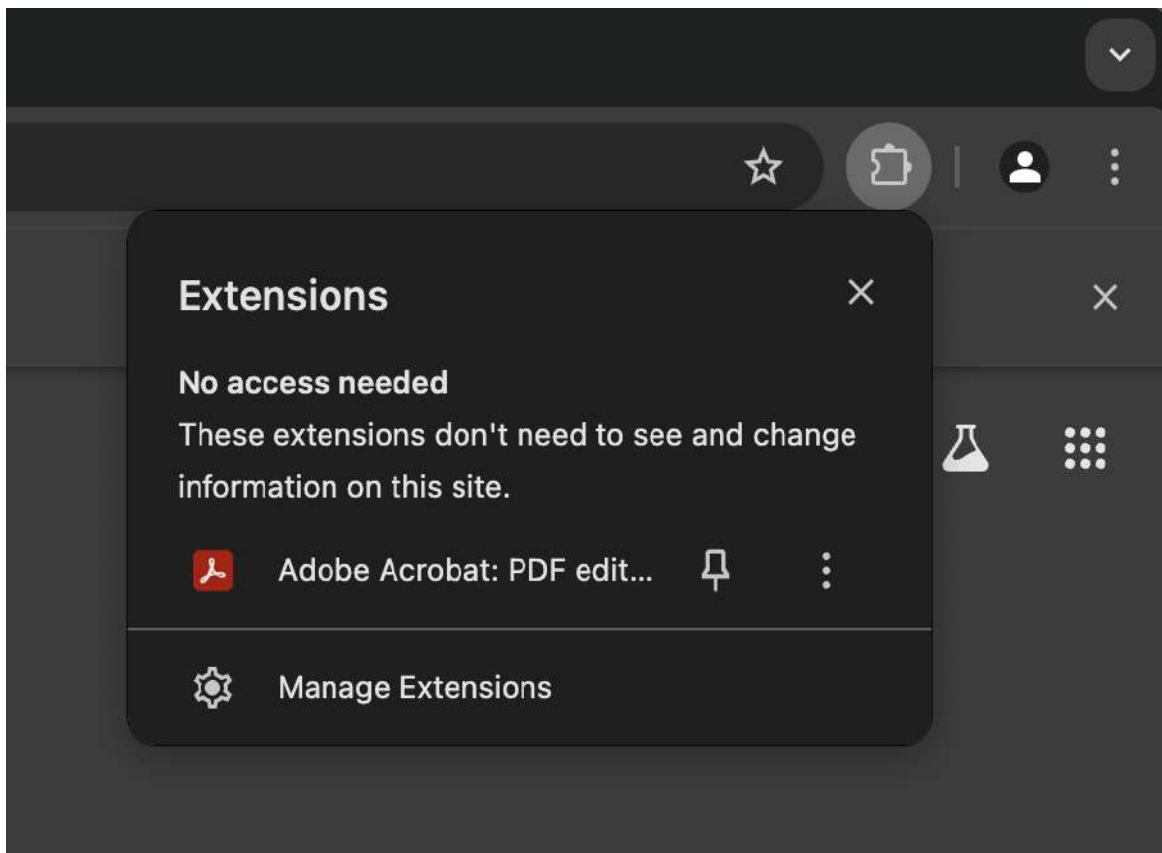
Kemudian, hasil identifikasi tersebut, dikroscek dengan dua perangkat analisis, yakni [Sapling AI](#) dan [Quillbot](#). Keduanya bisa digunakan gratis, tetapi untuk Sapling, ada opsi lain yang berbayar karena versi gratis hanya terbatas pada 2000 karakter. Akurasi Sapling berkisar pada 66-70%, sementara Quillbot hingga 94%.

Kita dapat mengakses Sapling melalui tautan <https://sapling.ai/ai-content-detector> atau memasang extensions-nya pada peramban.

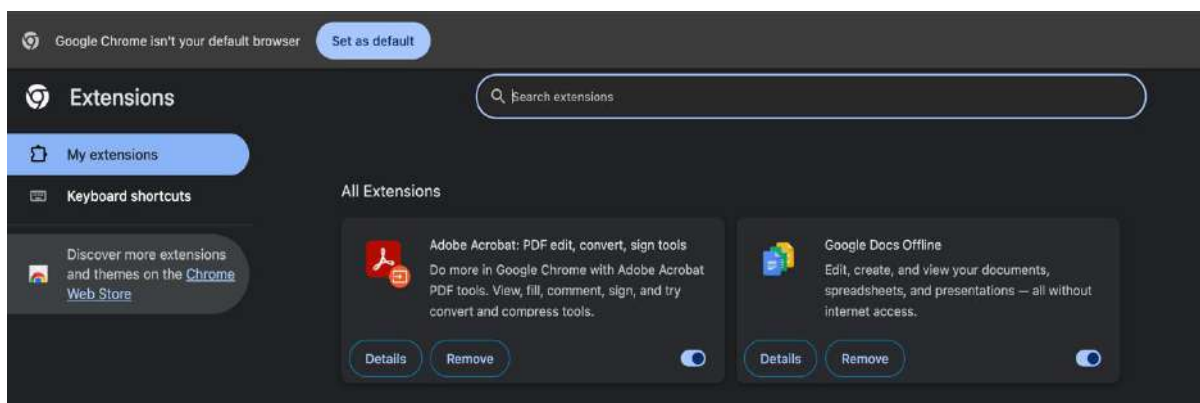
Untuk memasang extensions, Anda dapat mengetuk logo/icon kepingan puzzle di sisi kanan peramban.



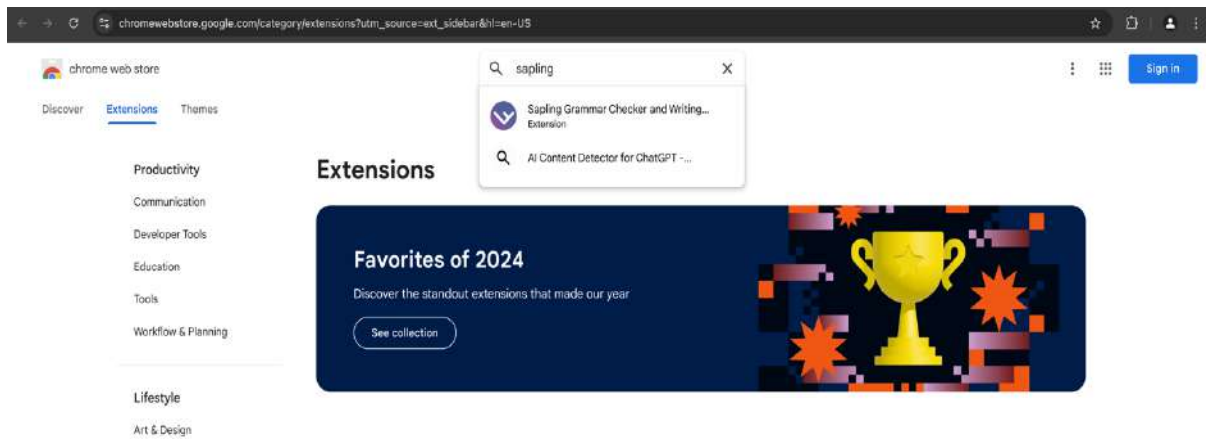
Setelah mengetuk logo tersebut, Anda dapat mengetuk opsi pengaturan atau manage extensions seperti tangkapan layar di bawah ini:



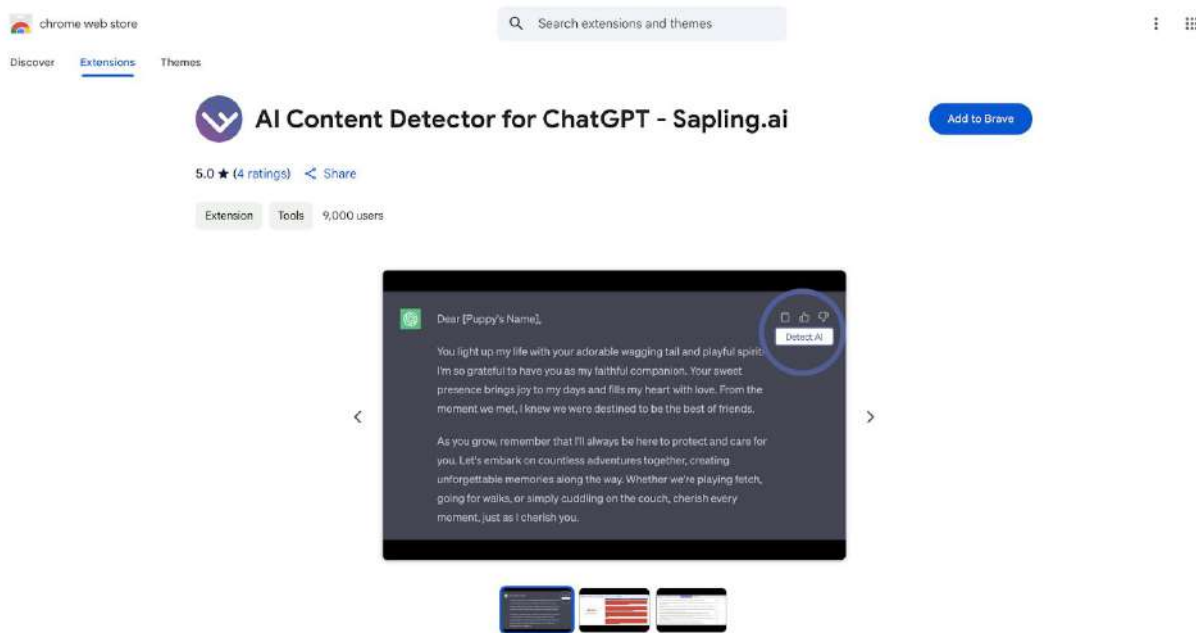
Langkah selanjutnya, Anda perlu mengakses tautan Chrome Web Store yang ada di kolom sisi kiri sebelum bisa mengidentifikasi extensions Sapling yang akan dipasang pada peramban.



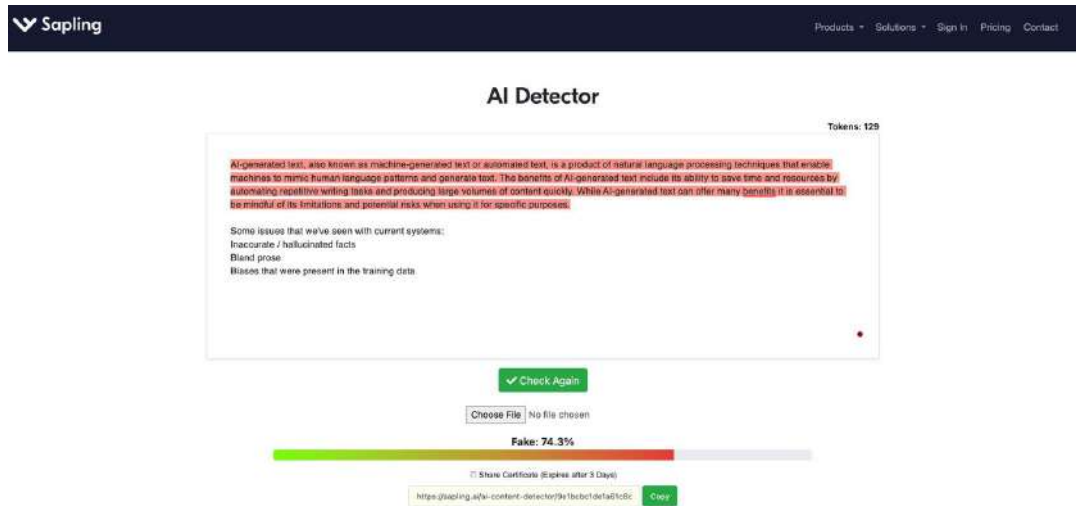
Setelah masuk ke Chrome Web Store, Anda perlu mengetikkan Sapling di kolom pencarian, setelah muncul extensions-nya baru Anda ketuk.



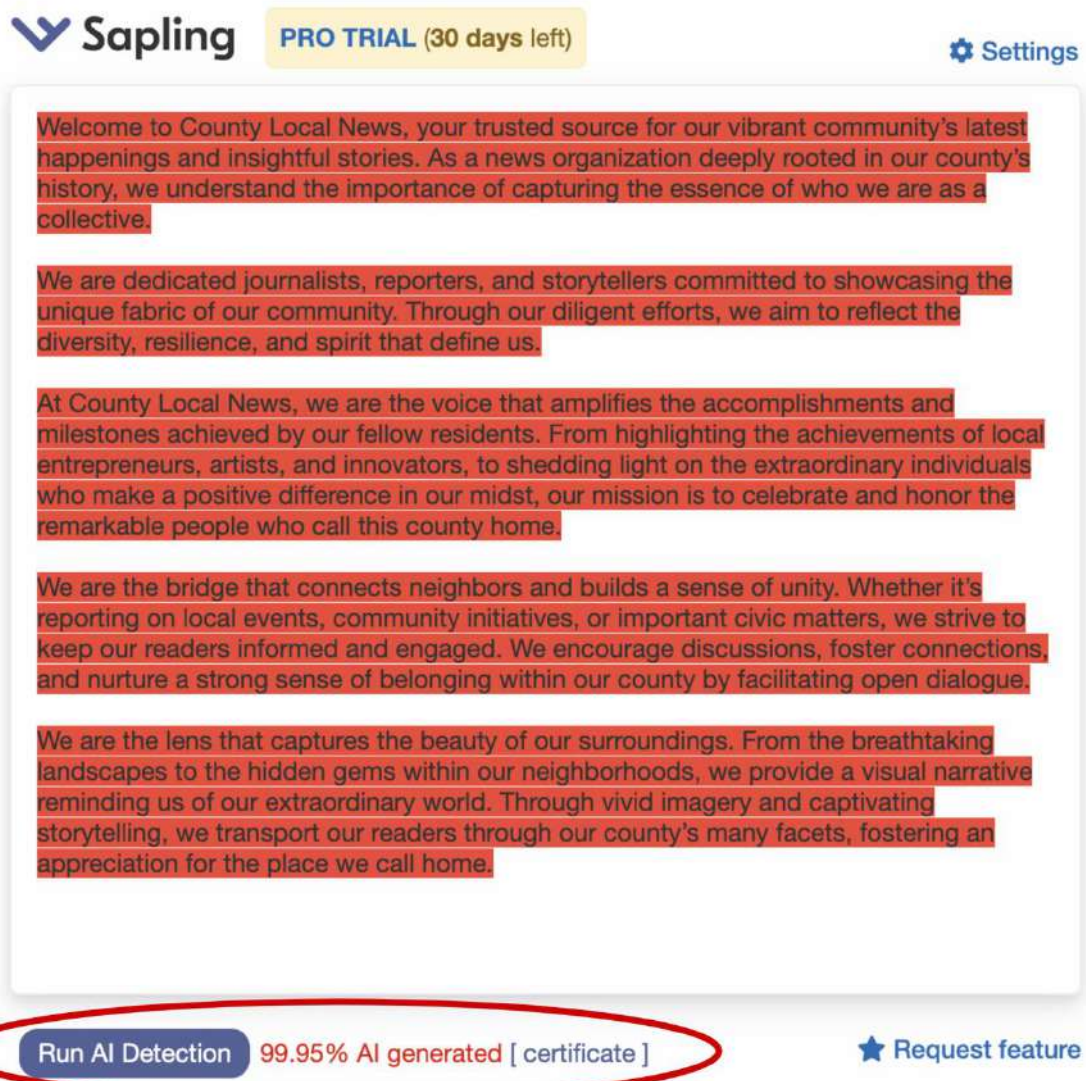
Pemasangan extensions Sapling baru bisa berjalan setelah Anda mendapatkan opsi “Add to Chrome”. Setelah terpasang, layanan Sapling akan meminta pendaftaran menggunakan alamat email.



Pemanfaatan fitur pengecekan teks Sapling ini bisa dilakukan dengan mengunggah teks atau file.



Hasil dari pemeriksaan atau deteksi teks memanfaatkan bantuan AI akan muncul dalam bentuk persentase di bagian bawah.



Namun dalam memanfaatkan fitur pengecekan teks berbasis AI, Anda tetap harus berhati-hati dan melakukan verifikasi ulang. Kasusnya terjadi pada contoh teks 2.

Tokens: 567

Konflik di Sigi, Sulawesi Tengah, terjadi pada November 2020. Insiden ini melibatkan serangan yang diduga dilakukan oleh kelompok teroris Mujahidin Indonesia Timur (MIT) yang berbasis di Poso. Berikut adalah beberapa detail penting mengenai konflik tersebut:

Serangan di Desa Lembantongoa:
 Pada 27 November 2020, terjadi serangan di Desa Lembantongoa, Kabupaten Sigi. Serangan tersebut menewaskan empat orang dan menyebabkan beberapa rumah dibakar.

Pelaku:
 Serangan ini diduga dilakukan oleh kelompok MIT, yang dipimpin oleh Ali Kalora. MIT adalah kelompok militan yang berafiliasi dengan ISIS dan telah lama terlibat dalam berbagai aksi kekerasan di Sulawesi Tengah.

Respon Pemerintah:
 Pemerintah Indonesia melalui TNI dan Polri segera melakukan operasi pengejaran terhadap pelaku. Operasi Tinombala, yang sudah berlangsung lama untuk memberantas MIT, ditingkatkan intensitasnya setelah serangan ini.

Dampak Terhadap Masyarakat:
 Serangan ini menciptakan rasa takut di kalangan masyarakat setempat. Beberapa warga terpaksa mengungsi karena khawatir akan adanya serangan lanjutan.

Latar Belakang Konflik:
 MIT telah aktif di wilayah Sulawesi Tengah selama bertahun-tahun. Kelompok ini terkenal karena keterlibatannya dalam serangkaian serangan teror, pembunuhan, dan bentrokan dengan pasukan keamanan Indonesia.

Konflik ini menunjukkan tantangan yang dihadapi Indonesia di daerah tersebut, namun masih banyak pekerjaan yang perlu dilakukan untuk mengatasi akar permasalahan dan mencegah kekerasan lebih lanjut.

✓ Check Again

Choose File No file chosen

Fake: 10.2%

Share Certificate (Expires after 3 Days)

Hasil pemeriksaan menyatakan tingkat pemanfaatan AI dalam rangkaian teks tersebut sangat sedikit atau sekitar 10,2% saja. Padahal contoh teks 2 diproduksi menggunakan Chat GPT. Hal ini terlihat secara kasat mata dari susunan konten yang dihasilkan, seperti paparan informasi yang berbentuk poin-poin dengan Kesimpulan di bagian akhirnya.

Layanan lainnya yang bisa dipergunakan untuk melakukan pendeteksian adalah QuillBot yang dapat diakses via tautan <https://quillbot.com/ai-content-detector>. Namun layanannya masih belum dapat mendeteksi teks bahasa Indonesia.

The screenshot shows the QuillBot AI Detector interface with the language set to Indonesian. The text being analyzed is a news article about a conflict in Sigi, Sulawesi Tengah, in November 2020. The interface includes a sidebar with various tools like Paraphraser, Grammar Checker, and Plagiarism Checker. The main content area displays the text with a 'Detect AI' button at the bottom right. A message on the right side states: 'We don't support Indonesian yet. Replace text with English, German, Spanish, or French.'

Lain halnya saat QuillBot dipergunakan untuk mendeteksi teks berbahasa Inggris.

The screenshot shows the QuillBot AI Detector interface with the language set to English. The text being analyzed is a paragraph about a community's commitment to showcasing its unique fabric. The interface displays a 100% AI detection score. A bar chart shows the breakdown: 74% AI-generated, 26% AI-generated & AI-refined, 0% Human-written & AI-refined, and 0% Human-written. A 'Try Paraphraser' button is visible. A caution message at the bottom states: 'Caution: Our AI Detector is advanced, but no detectors are 100% reliable, no matter what their accuracy scores claim. Never use AI detection alone to make decisions that could impact a person's career or academic standing.'

Berdasarkan dua layanan tersebut, kita dapat menarik kesimpulan:

1. Tidak semua *tools* AI mampu mendeteksi teks diproduksi dengan AI atau tidak secara akurat. Terutama dalam bahasa Indonesia. Karena, *tools* ini dikembangkan oleh peneliti dari luar negeri.
2. Layanan *tools* bisa meningkat dan membaik seiring “latihan” yang dijalaninya. Apabila belum dapat mendeteksi bahasa Indonesia secara

akurat, bisa jadi karena materi “latihan” lebih banyak menggunakan bahasa Inggris.

3. Tempatkan *tools* AI sebagai asisten, sehingga pengecekan secara manual juga tetap diperlukan.

Memanfaatkan *tools* AI untuk mengecek keaslian rangkaian kalimat apakah diproduksi menggunakan AI atau tidak, HANYALAH SALAH SATU CARA. Semakin banyak “latihan”, bisa jadi konten hasil pembangkitan AI akan lebih baik hasilnya.

Berikut cara lainnya yang dapat Anda lakukan:

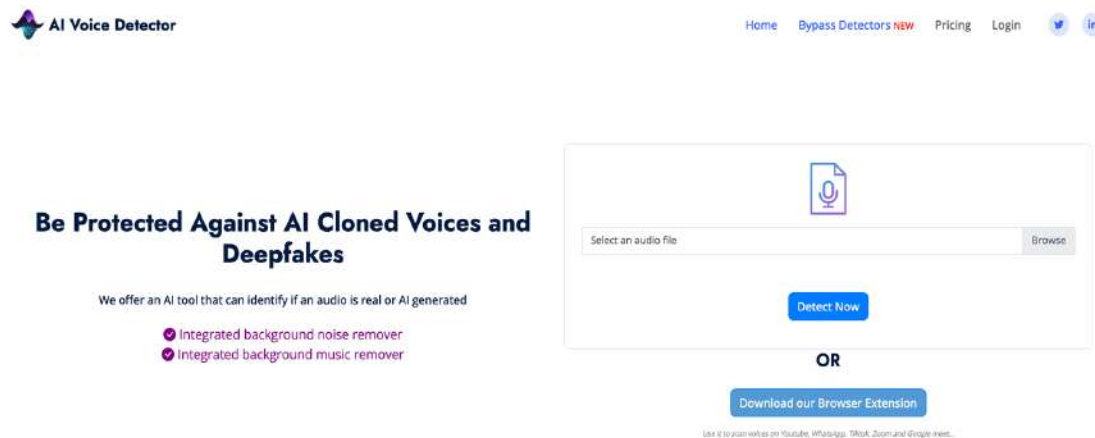
1. Apabila Anda mencurigai konten-konten informasi pada sebuah portal, coba lihat dengan teliti. Biasanya portal yang menayangkan teks hasil pembangkitan AI cenderung memiliki desain bawaan yang disediakan Wordpress atau Blogspot.
2. Periksa siapa penulisnya. Apakah penulisnya seseorang yang kredibel? Cek profil-nya di media sosial.
3. Apakah artikelnya menggunakan judul yang bombastis? Apakah kontennya berasal dari sumber terpercaya?
4. Periksa lebih dalam konten teksnya, apakah ada kronologinya, konteksnya, atau latar belakang peristiwa?
5. Cek komposisi S-P-O-K (Subyek-Predikat-Objek-Keterangan). Apakah ada kata yang berulang?
6. Cek apakah tulisannya monoton, tanpa alur, tanpa unsur kejutan, atau tidak ada emosinya.

2.5.2. Pemeriksaan Audio

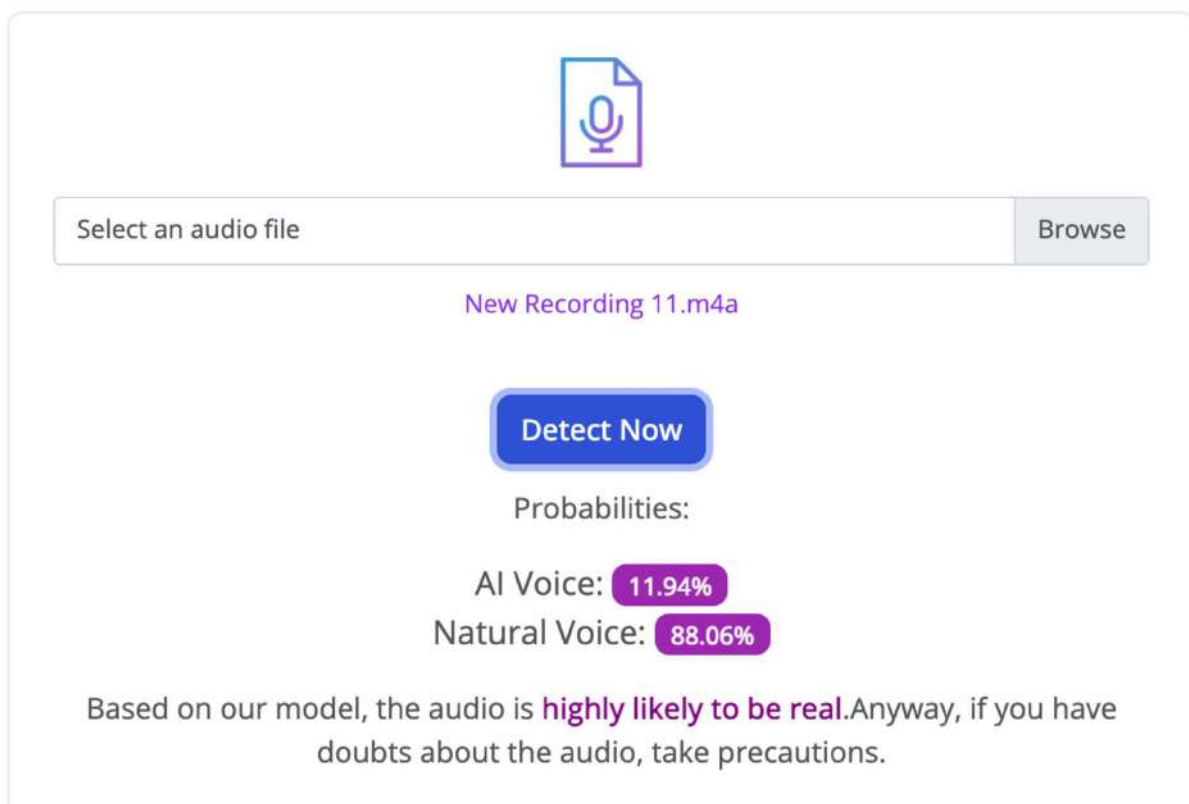
Seperti sebelumnya, kita akan memulainya dengan studi kasus. Kali ini konten berbasis audio atau suara. Peserta pelatihan diminta untuk mendengarkan suara [via tautan ini](#) dan diminta pendapatnya: apakah asli atau palsu, dan jelaskan alasannya.

Setelah diskusi, pelatih menjelaskan bahwa secara sekilas suara kedua orang yang berbincang-bincang itu terdengar mirip dengan Najwa Shihab dan Raffi Ahmad.

Untuk bisa melakukan pengecekan berbasis suara itu, salah satunya bisa dilakukan menggunakan tools AI Voice Detector.



Anda hanya perlu memasukkan file ke kolom yang tersedia dan kemudian dilanjutkan dengan menyetuk opsi “detect now”. Hasilnya:



Namun, sepertinya, AI detector tidak bisa mendeteksi dengan baik untuk audio ini karena data latihan dalam bahasa Indonesia yang belum

mencukupi dan tingkat kemiripan dengan suara asli yang cukup tinggi. Namun, rekaman suara ini juga sudah diperiksa kebenarannya oleh tim pemeriksa fakta, salah satunya dari Kompas.com yang hasilnya bisa diakses melalui [tautan ini](#).

Untuk kasus lain, seperti suara Surya Paloh dan Anies Baswedan, perangkat ini mampu mendeteksi secara akurat bahwa audio tersebut adalah buatan AI, seperti dapat dicek di [video ini](#).

Hingga modul ini ditulis, masih belum ada tools pemeriksaan suara yang dapat diakses cuma-cuma. Layanan seperti AI Voice Detector menerapkan biaya 13 USD per bulan.

Jika Anda mendapati konten berbasis suara saja dan patut diduga produksinya menggunakan bantuan AI, ada baiknya memerhatikan:

1. Apakah **kata yang digunakan sering digunakan**?
2. Apa **ciri khas dari pembicara** tersebut, apakah kekhasannya hilang?
3. AI tidak bisa meniru **intonasi**, jeda bicara, memancarkan emosi. (Tapi hati-hati, semakin canggih AI, makin canggih untuk meniru)
4. Detail **dialog, kata sapaan**: apakah sesuai dan seperti biasanya?
5. Apa ada **noise** di latar belakang?
6. Jika ragu, tanya langsung ke yang bersangkutan atau wawancara langsung.

2.5.3. Memeriksa Foto dan Video yang dibuat AI

Produksi konten berbasis visual menggunakan teknologi AI jamak ditemukan dalam beragam aplikasi. Untuk memulai materi pemeriksaan visual ini, dapat dilakukan dengan mengajak peserta melakukan tes secara kasat mata dengan menebak aneka wajah yang ditampilkan. Sebagian di antaranya diproduksi memanfaatkan teknologi AI. Cara ini menarik untuk dipakai agar peserta memahami sampai sejauh mana konten visual itu bisa diproduksi dengan AI.

Untuk memulainya, pelatih dapat mengakses permainan dari the *New York Times* melalui tautan [ini](#). Konten ini mengajak pengunjungnya menebak sejumlah foto, mana yang asli atau mana yang diproduksi AI.

Jika sebelumnya hanya foto wajah, kita akan melihat bagaimana AI dapat memproduksi konten visual yang lebih dari sekedar wajah seperti contoh-contoh di bawah ini. Kita dapat mengajak peserta untuk mengidentifikasi apa saja tanda-tanda foto di bawah ini diproduksi oleh AI.



Sumber: Amnesty International

Foto di atas menunjukkan karakteristik AI: terlalu mulus, *background* yang kabur dan tidak sesuai dengan foto *foreground*, posisi kalung terlihat aneh.



Sumber: EU News.

Foto di atas menunjukkan karakteristik AI: terlalu mulus, *background* yang kabur dan tidak sesuai dengan foto *foreground*, serta senjata laras panjang terlihat aneh.

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

Trump supporters target black voters with faked AI images

4 March 2024

Share Save

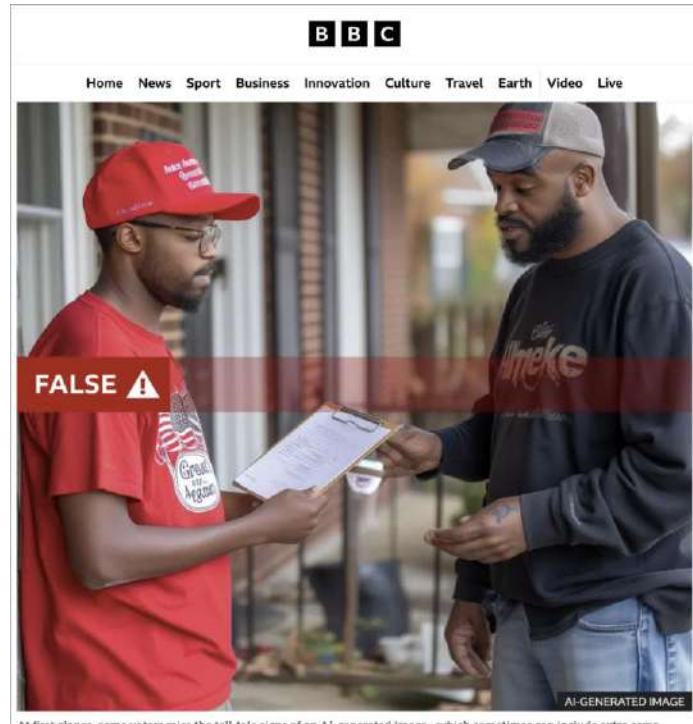
Marianna Spring
BBC Panorama and Americast



This image, created by a radio host and his team using AI, is one of dozens of fakes portraying black Trump supporters

Donald Trump supporters have been creating and sharing AI-generated fake images of black voters to encourage African Americans to vote Republican.

Trump berfoto bersama dengan orang kulit hitam. Jelas ini adalah foto buatan AI. Karena, menilik sejarahnya, Trump tidak mendukung gerakan-gerakan yang diinisiasi oleh orang kulit hitam dan orang kulit berwarna lainnya.



Coba lihat orang berbaju biru tampak memiliki tiga tangan. Ini menunjukkan halusinasi AI untuk memvisualisasikan gambar.

Bagaimana tahapan pengecekan selanjutnya?

Baik foto atau video memiliki proses pengecekan yang sama. Pertama, kita tentukan gambar atau *frame* yang akan dicek. Untuk video, gambar dapat diambil dari salah satu tangkapan layar karena sebenarnya video merupakan kumpulan dari *frame* atau gambar yang dipadatkan dalam durasi waktu sehingga tampak bergerak.

Kemudian, cek menggunakan Google Lens, Google Reverse Image, TinEye, Yandex, atau perangkat lainnya. Beberapa visual yang dimanipulasi menggunakan AI bersumber dari foto atau video yang sudah tayang di internet. Tapi, banyak juga yang memang konten sepenuhnya buatan AI dan

belum pernah terungghah. Cari sumber lain juga yang mendukung, misal dari situs berita, media sosial, atau situs lembaga lain.

Selain identifikasi manual, ada juga alat yang bisa membantu mengidentifikasi secara otomatis seperti <https://isitai.com/ai-image-detector/>. Namun layanan ini mensyaratkan penggunaanya untuk mendaftar dengan mencantumkan surat elektronik. Jika sudah mendaftar, penyedia layanan menyediakan opsi untuk menggunakan layanan ini langsung dari extension di peramban berbasis chromium seperti Google Chrome atau Brave.

Is It AI?
AI Detection Made Simple

Text Detector Image Detector Pricing Contact Us Log in

AI-Generated Image Detector

Please note that we have an updated Image Detection Model that is available exclusively for registered users. By registering, you will gain access to the most accurate and informative image detection results, enjoy an ad-free experience, and stay informed with the latest updates and features. [Register now for free](#) - [click here](#) to sign up and enhance your experience!

How It Works

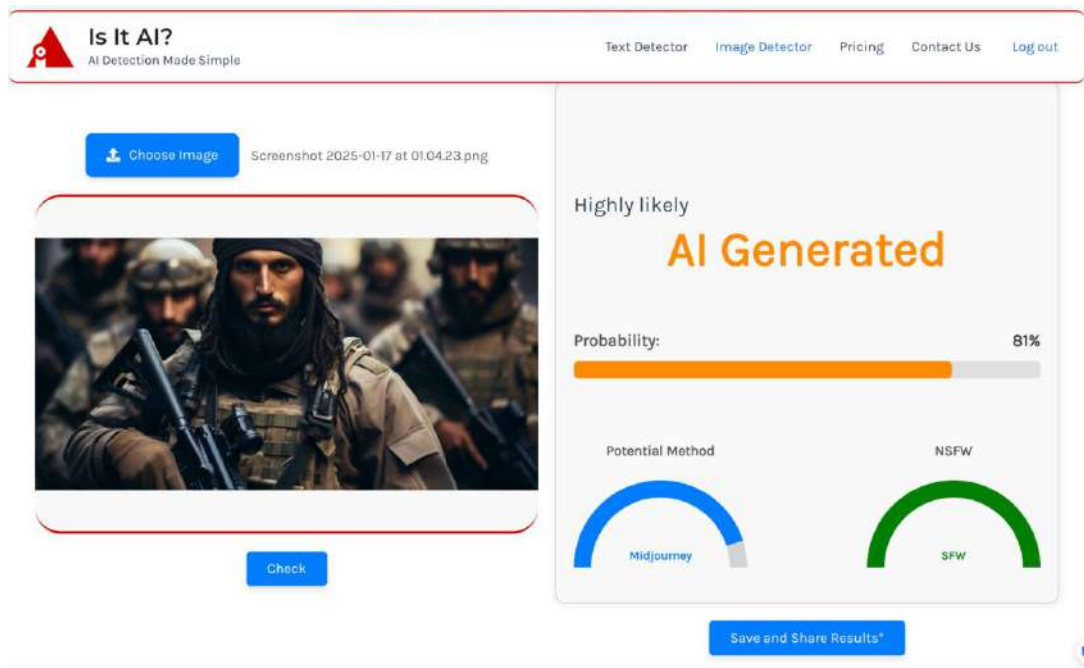
Our AI detection tool analyzes images to determine whether they were likely generated by a human or an AI algorithm. The tool works by using machine learning models to examine various features of the image, such as color patterns, shapes, and textures, and then compares them to patterns typically found in human-generated images or AI-generated images.

The machine learning models were trained using a large dataset of images that were labeled as either human or AI-generated. Through this training process, the models were able to learn to recognize patterns that are indicative of either human or AI-generated images.

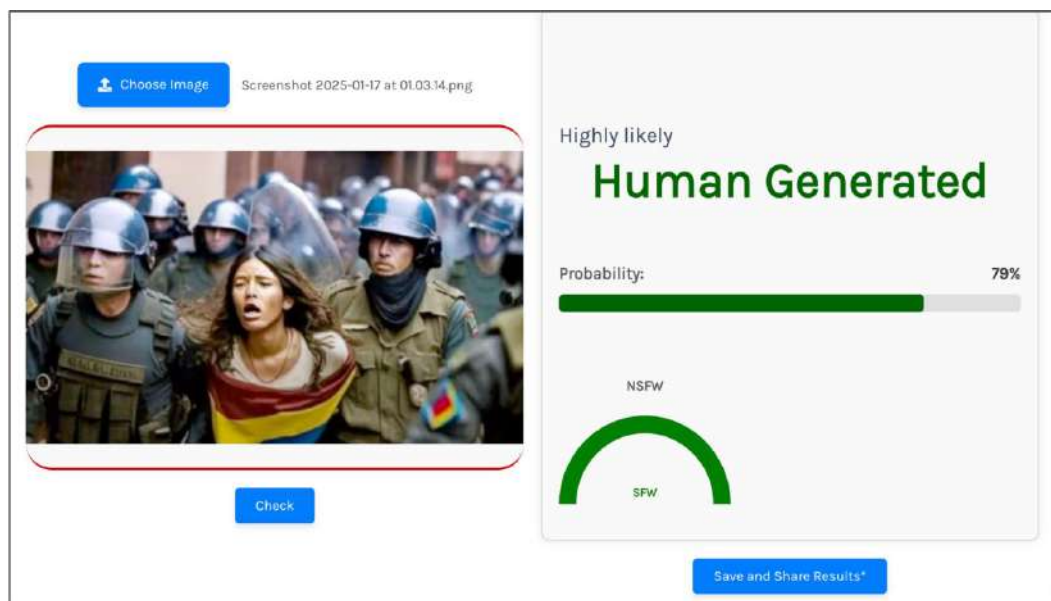
Choose File No file chosen

Check

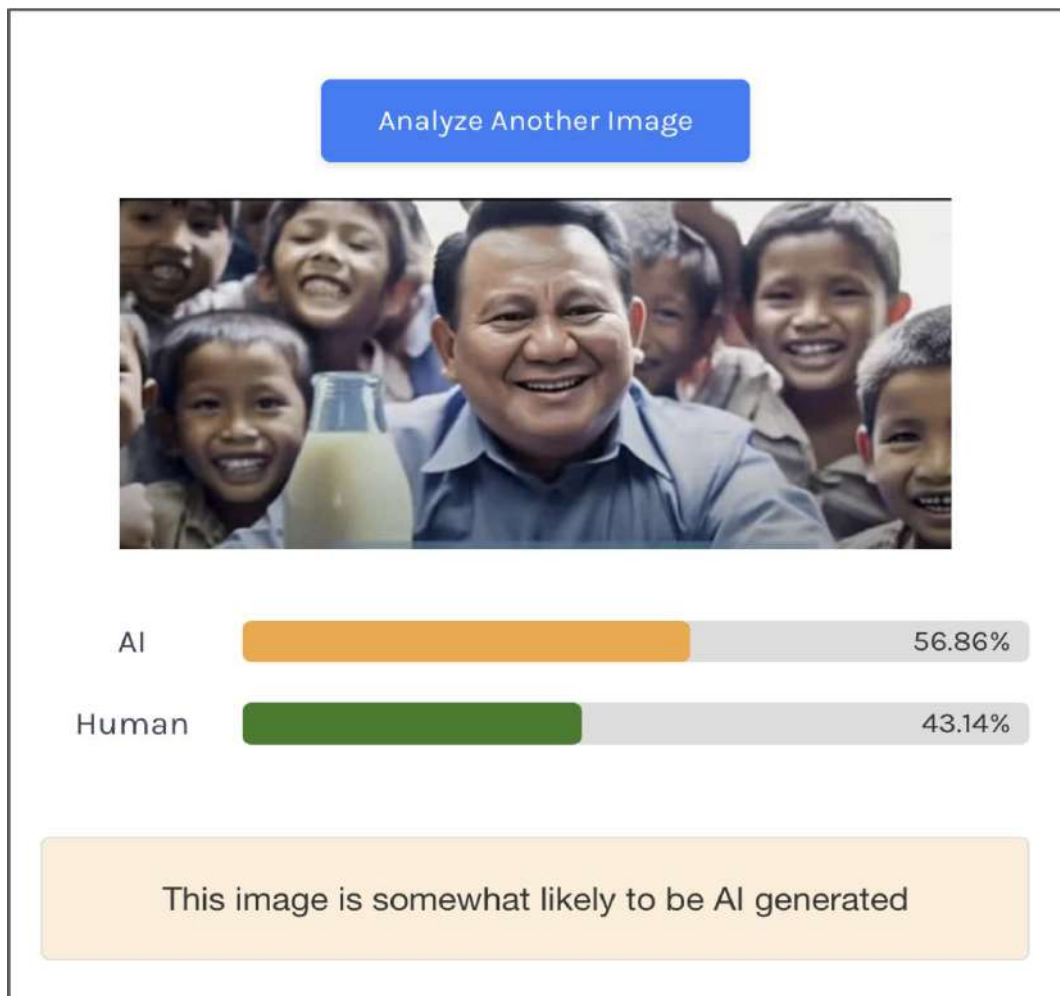
Setelah mendaftar, pengguna nantinya dapat mengunggah file foto ke kolom di sisi kanan sebelum meng-klik 'check. Kemudian, alat ini akan memunculkan hasil, apakah foto tersebut dibuat oleh manusia atau AI, seperti di bawah ini:



Dalam proses pemeriksaan yang menggunakan sumber terbuka, pemeriksa fakta perlu tetap mengedepankan sikap kritis. Verifikasi dan konfirmasi tetap jadi landasan dasar sebelum menyatakan sebuah informasi yang beredar itu mengandung disinformasi seluruhnya, sebagian, atau ada konteks yang keliru. Demikian juga halnya dengan hasil pemeriksaan menggunakan layanan berbasis AI. Contohnya dalam konteks pemeriksaan visual ini:



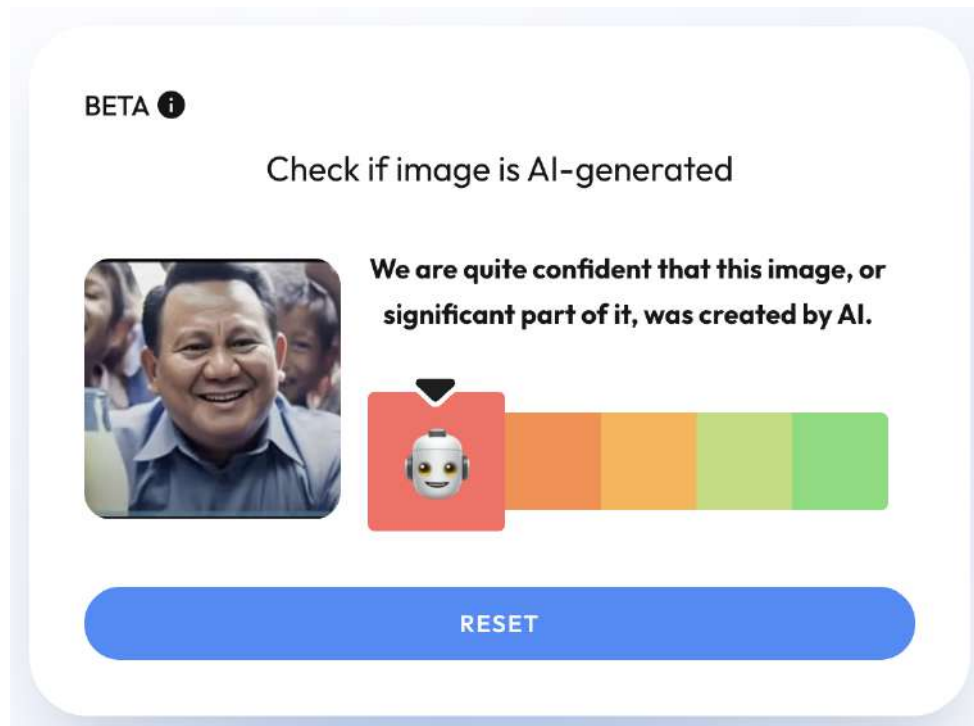
Atau seperti di bawah ini:



Alat ini gagal untuk mendeteksi bahwa keduanya adalah buatan AI, bukan manusia. Dalam visual Prabowo, layanan pemeriksaan gambar berbasis AI mengindikasikan gambar itu 56,86% diproduksi dengan AI dan 43,14% diproduksi oleh manusia. Hasil pemeriksaan seperti ini sangat membutuhkan verifikasi dan konfirmasi ulang lebih lanjut.

Layanan pemeriksaan berbasis AI lainnya bisa diakses via <https://wasit.com>. Dalam layanan ini pengguna dapat langsung menarik dan menyimpan gambar yang hendak diperiksa ke kolom pengecekan tanpa perlu mendaftar.

Hasil pemeriksaannya akan terlihat seperti ini:



Mengkombinasikan beberapa layanan pemeriksaan visual berbasis AI sangat baik dilakukan dalam upaya verifikasi sebuah gambar atau foto.

Perhatikan kesamaan dari masing-masing layanan pemeriksaan visual berbasis AI, setidaknya dari dua layanan di atas, sama-sama tidak mengkategorisasikan atau memisahkan hasil pemeriksaan secara hitam dan putih. Mereka membuat gradasi penilaian soal berapa besar kemungkinan sebuah visual diproduksi memanfaatkan AI.

Layanan lainnya yang cukup mudah dipergunakan adalah <https://fotoforensics.com/>. Namun saat ini, per Maret 2025, layanan tersebut tidak dapat diakses dari Indonesia. Alasan mereka, lebih dari 80% konten yang diunggah dari Indonesia melanggar ketentuan layanan portal. Termasuk di antaranya bukti transfer ATM, kartu identitas, hingga konten pornografi. Karena alasan tersebut, pengembang layanan melarang adanya unggahan dari Indonesia.

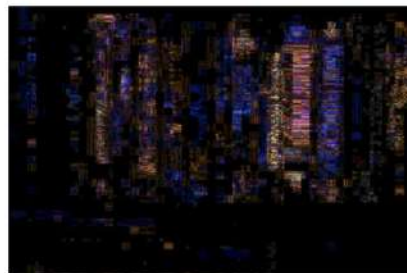
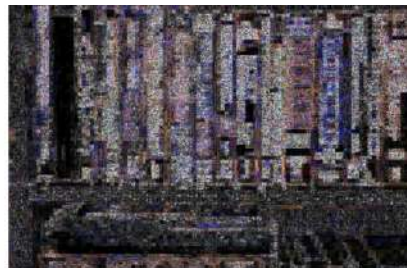
Layanan ini juga tidak dapat diakses lewat TOR (The Onion Router) atau jaringan yang memungkinkan pengguna menjelajahi internet dengan aman dan mengedepankan privasi karena menyembunyikan Alamat IP (internet protocol) dan aktivitas penjelajahan penggunaannya. Meski demikian,

pemeriksa fakta dapat menggunakan VPN dan memanipulasi server ke selain Indonesia dan Singapura, untuk mengakses layanan ini.

Informasi yang diberikan oleh Foto Forensics beragam, di antaranya *Error Level Analysis* (ELA), untuk mengetahui perbedaan level kontras, saturasi, *brightness*, tekstur, dan lainnya. Selain itu, ada juga metadata, yang memberikan informasi terkait kapan foto diambil, menggunakan jenis kamera apa dan beberapa juga bisa diketahui lokasi pengambilan gambarnya.

Untuk metode *Error Level Analysis* (ELA), jika kita mengunggah gambar, dia akan memberikan hasil analisisnya.

Untuk JPEG, seluruh gambar mestinya berada di level warna yang sama: hitam atau putih. Jika ada yang berbeda, kemungkinan itu adalah hasil modifikasi.



Sumber: FotoForensics.com

Perhatikan gambar di sisi kiri dan bandingkan dengan gambar yang sejajar di sisi kanannya. Pada gambar paling atas nampak hasil pemeriksaan ELA memperlihatkan dimensi warna yang serupa.

Bandingkan dengan gambar paling kiri bawah yang dimodifikasi memanfaatkan 'penempelan' gambar dinousarus sehingga di hasil pemeriksaan pada bagian kanannya nampak ada dimensi warna serupa sebagai identifikasi adanya modifikasi gambar.

Modifikasi gambar itu juga terlihat pada hasil pemeriksaan di bawah ini. Perhatikan ada warna berbeda pada bagian dasinya. Kemungkinan besar gambar itu sudah dimodifikasi. Karena jika tidak ada modifikasi, maka kedua gambar harus menampilkan warna hitam atau putih saja.



Contoh pada gambar berikutnya, memperlihatkan adanya modifikasi:



2.5.4. Menginvestigasi Teks AI dan Pemilik Situs Palsu Menggunakan Akun Iklan Digital

Jika kita mendapati sebuah situs dan curiga bahwa dia menggunakan konten AI, tapi kemudian setelah ditelusuri lewat beragam cara seperti di atas ternyata masih gagal, maka cara yang dapat kita tempuh adalah mengecek iklan digital dalam situs tersebut.

Studi kasus yang sudah berhasil menggunakan cara ini adalah investigasi ProPublica dan [situs cek fakta LeadStories](#) terhadap situs *Conservative Beaver* (CB). Pada November 2021, situs ini menyebarkan konten palsu yang menyebutkan penangkapan CEO Pfizer karena penipuan. Konten ini tersebar luas di kalangan kelompok anti-vaksin. Pfizer menuntut lewat pengadilan agar penyedia hosting dan domain DreamHost untuk membuka identitas pemilik situs *Conservative Beaver* (CB), dengan tujuan agar Pfizer bisa menuntut pemilik CB atas pencemaran nama baik. Setelah dicek, ini bukan kali pertama CB mempublikasikan konten palsu. Konten lainnya

We're trying to make news that tells people the truth on issues others want to hide or distort. Those in positions of authority and those that work in the mainstream media need to stop lying. Until then, you have **Toronto Today**.

Founded by Mark Slapinski.

For questions about our editorial standards, or to request a correction please email TorontoToday@Protonmail.com and someone will respond within 48 hours. Unlike other outlets, we take editorial standards seriously.

Dulunya *Toronto Today* menggunakan nama *The Red Panther*, tapi kemudian berubah pada pertengahan 2020. Situs ini juga memfabrikasi konten palsu. ID yang sama digunakan oleh situs Toronto99.com seperti tampak pada tangkapan layar di bawah ini.

```
<html lang="en-US" style="transform: none;">
  <head>
    <script src="https://web.archive.org/web/20211223082818/https://partner.googleadservices.com/pagead/managed/js/adsense/m202112060101/show_ads_impl.js" id="google_shimpl"></script>
    <script type="text/javascript" async src="https://web.archive.org/web/20211209131816/https://www.google-analytics.com/analytics.js"></script>
```

Setelah itu, penelusuran kembali ke situs CB. Ternyata, salah satu penulis konten situs tersebut menggunakan satu akun yang terhubung dengan alamat email Slapinski.

Slapinski terbukti mengelola situs konten palsu yang berhubungan dengan isu-isu di Toronto, Kanada.

Siapa Mark Slapinski? Hati-hati, Slapinski melakukan personal branding seolah-olah dirinya pro-vaksin. Padahal dia menyebarkan konten palsu propaganda anti-vaksin juga. Dari kasus ini kita belajar bahwa penelusuran penyebar konten palsu bisa dilakukan melalui investigasi iklan digital.



Bagaimana cara untuk mengetahui apakah satu akun Google AdSense atau mitra iklan digital juga dipakai oleh situs lainnya? Cara paling mudah adalah dengan memasukkan tambahan *extension* ads.txt setelah alamat situs. Misalnya: <https://www.kompas.com/ads.txt> dan hasilnya:

```

← → ↻ 🏠 🌐 kompas.com/ads.txt

ownerdomain=kgmedia.id
google.com,pub-7784034061253020,DIRECT,f08c47fec0942fa0
google.com,pub-5525656313349147,DIRECT,f08c47fec0942fa0
google.com,pub-7486139053367666,DIRECT,f08c47fec0942fa0
google.com,pub-9012468469771973,DIRECT,f08c47fec0942fa0
#endgoogle

#StartR2B2
r2b2.cz, 243, DIRECT
r2b2.io, 243, DIRECT
#endgooglerubiconproject.com, 11352, RESELLER, 0bfd66d529a55807
contextweb.com, 557671, RESELLER, 89ff185a4c4e857c
etarget.cz, 322, DIRECT
IDEO #DISPLAY,f5ab79cb980f11d1
#StartR2B2-ads.txt-v2.5.0
r2b2.cz,243,DIRECT
r2b2.io,243,DIRECT
rubiconproject.com,11352,RESELLER,0bfd66d529a55807
contextweb.com,557671,RESELLER,89ff185a4c4e857c
etarget.cz,322,RESELLER
etarget.sk,14478,RESELLER
adform.com,811,RESELLER
adform.com,1099,RESELLER
criteo.com,B-060876,RESELLER,9fac4a4a87c2a44f
themediagrid.com,VU352P,DIRECT,35d5010d7709b49d
smartadserver.com,2910,RESELLER
smartadserver.com,3924,RESELLER
contextweb.com,560288,RESELLER,89ff185a4c4e857c
pubmatic.com,156439,RESELLER
pubmatic.com,154037,RESELLER
pubmatic.com,156030,RESELLER,5d62403b186f2ace
pubmatic.com,156030,RESELLER,5d62403b186f2ace

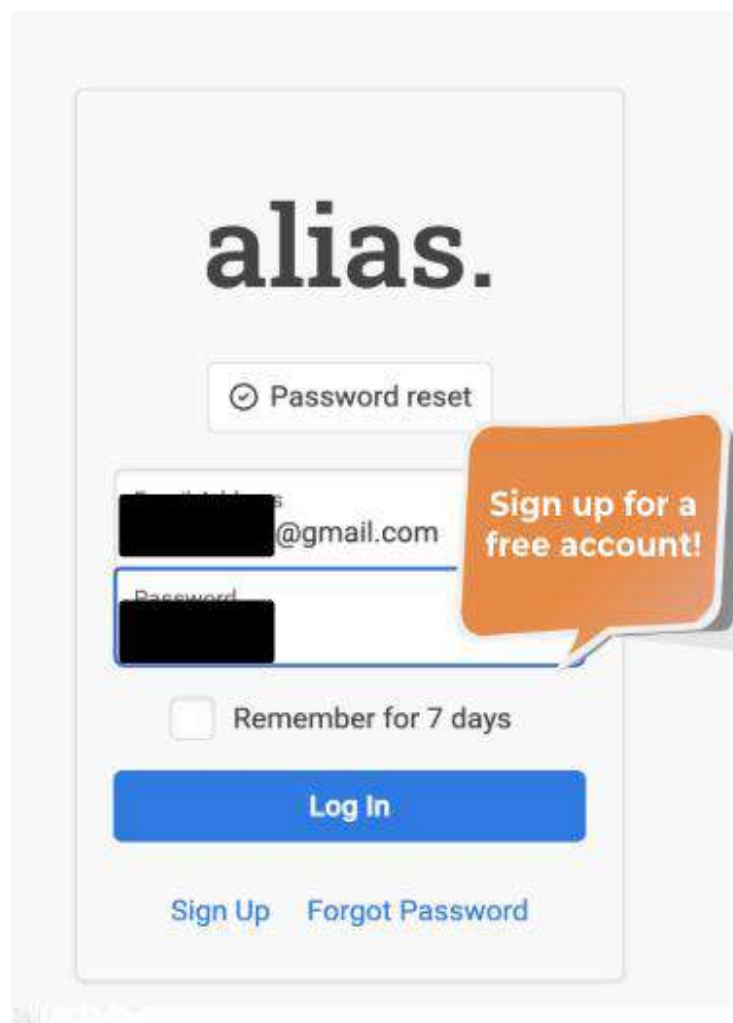
```

Dari tampilan itu kita lihat ada *user ID* yang digunakan *Kompas.com* untuk beriklan lewat Google AdSense, yakni pub-7784034061253020, pub-5525656313349147, pub-7486139053367666, dan pub-9012468469771973.

Selanjutnya kita bisa cek, situs apa saja yang menggunakan ID tersebut. Pengecekan ini dapat dilakukan melalui layanan <https://well-known.dev>.

Tapi, sebelumnya, kita mau mengecek data iklan digital yang digunakan oleh *Kompas.com*. Dari situs tersebut kita juga dapat mengetahui *ID* yang digunakannya untuk memasang iklan.

Untuk mengakses, kita perlu mendaftarkan akun terlebih dahulu melalui Alias.



alias.

Password reset

Remember for 7 days

[Sign Up](#) [Forgot Password](#)

Sign up for a free account!

Setelah masuk menggunakan akun, tulis Kompas.com dalam kotak pencarian.

The screenshot shows a search engine interface with the search term 'kompas.com' entered in the search bar. Below the search bar, there are three search results listed in a table format. The table has columns for Rank, Domain, Resource, Status, Scanned, and Simhash.

Rank	Domain	Resource	Status	Scanned	Simhash
4,533	kompas.com	robots.txt	Ok	2024-02-16	29659cc4e1f3
4,533	kompas.com	app-ads.txt	Ok	2024-02-16	979b9f95b56b
4,533	kompas.com	ads.txt	Ok	2024-02-16	c0c23885538c

Nantinya akan muncul data seperti di bawah ini. Kita bisa tahu siapa pemilik domain Kompas, yakni Kompas Gramedia Media. Kalau diklik, akan memunculkan nama media dalam jaringan Kompas. Untuk kasus situs palsu, seringkali domain tidak tercantum.

Variable	Value
OWNERDOMAIN	kgmedia.id
OWNERDOMAIN	kgmedia.id
MANAGERDOMAIN	adpushup.com
MANAGERDOMAIN	anymanager.io
INVENTORYPARTNERDOMAIN	9mediaonline.com

Mari fokus ke ads.txt. Ada dua akun yang digunakan Kompas, *direct* dan *reseller*. *Direct* artinya Kompas.com punya akun yang terdaftar di jaringan mitra pengiklan secara langsung. Mitra tersebut di antaranya *Google*, *r2b2.cz*, *etarget.cz*, dan lainnya

Ad System	Seller ID	Name	Domain
adbro.me	db52c60d-7ece-414a-a36c-05d3be8e1d68	PT. KREASI INTISARI NUSANTARA	kompasgramedia.com
adform.com	37	Zoznam s.r.o.	media.roznam.sk
adform.com	557	Wirtualna Polska Media S.A.	wp.pl
adsparc.com	768	MobilityWare, LLC	mobilityware.com
adtelligent.com	315908	Streamlynn Pte LTD	luponmedia.com
adwmg.com	100094	24h.com.vn	24h.com.vn
amplify.com	amp00485	iVideoSmart Pte. Ltd.	showheroes.com
appnexus.com	10726	Excellence Advertising Corp.	losandes.com.ar
appnexus.com	12998	The Jerusalem Post Ltd	jpost.com
appnexus.com	3457	Wirtualna Polska Media S.A.	holding.wp.pl
atlas5.co	4229	Sports Technologies Private Limited(PFA)	fancode.com
connectad.io	20	Wirtualna Polska Media S.A.	wpartner.pl
critico.com	B-071800	diDNA, INC.	didna.io
ergadx.com	3662	kompas.com	kompas.com/
ergadx.com	3758	yieldmartech.com	yieldmartech.com
eskiml.com	esa-019157	KG Media	kompas.com
etarget.cz	13655	Niko Valach	adka-48.playzooone.com

Sementara itu akun *reseller* adalah akun yang dikelola oleh pihak ketiga, bukan oleh media atau situs itu sendiri. Jadi, ini bisa kita abaikan dan fokus ke *direct*.

Direct Sellers (394)		random generated number of user ID	Perusahaan	
Publisher Direct Sellers (86)				
Mitra pengiklan	Ad System	Seller ID	Name	Domain
	adbro.me	db52c609-7ece-414a-e36c-05d3be6e1068 (22)	PT. KREASI INTISARI NUSANTARA	kompasgramedia.com
	adform.com	37 (2,386)	Zoznam s.r.o	media.zoznam.sk
	adform.com	557 (7,022)	Wirtualna Polska Media S.A.	wp.pl
	adsparc.com	768 (1,495)	MobilityWare, LLC	mobilityware.com
	adtelegant.com	315908 (2,247)	Streamiyn Pte LTD	luponmedia.com
	adwmg.com	100094 (1,894)	24h.com.vn	24h.com.vn
	amplify.com	amp00485 (113)	IVideoSmart Pte. Ltd.	showheroes.com
	appnexus.com	10726 (8,868)	Excellence Advertising Corp.	losandes.com.ar
	appnexus.com	12998 (7,054)	The Jerusalem Post Ltd	jpost.com
	appnexus.com	3457 (7,021)	Wirtualna Polska Media S.A.	holding.wp.pl
	atlas5.co	4229 (66)	Sportia Technologies Private Limited(PFA)	fancode.com
	connectad.io	20 (6,878)	Wirtualna Polska Media S.A.	wpartnerpl
	critico.com	B-071800 (136)	diDNA, INC.	didna.io
	ergadx.com	3682	kompas.com	kompas.com/
	ergadx.com	3758 (7)	yieldmartech.com	yieldmartech.com
	eskimi.com	eas-019157	KG Media	kompas.com
	etarget.cz	13555 (271)	Niko Vslach	adka-46 playzooone.com

Mari kita cek mitra pengiklan Google yang dipasang oleh *Kompas.com*. Angka di dalam tanda () menunjukkan jumlah situs yang berbagi akun yang sama di Google AdSense dengan *Kompas.com*. Kalau kita klik di bagian itu akan menunjukkan data domain yang menggunakan ID tersebut untuk memasang iklan Google AdSense.

google.com	pub-1237260803267758 (1,486)	Geniee International Pte. Ltd	geniee.co.jp
google.com	pub-5525656313349147 (26)	PT. Kreasi Intisari Nusantara	-
google.com	pub-7486139053367666 (24)	PT. Kreasi Intisari Nusantara	-
google.com	pub-7784034061253020 (26)	PT. Kreasi Intisari Nusantara	kgmedia.id
google.com	pub-9012468469771973 (24)	PT. Kreasi Intisari Nusantara	kgmedia.id

Dari data domain kita tahu bahwa *Kompas.com* berbagi ID Google AdSense dengan *Kontan*, *Kompasiana*, *Sonora*, dan lainnya. Teknik serupa bisa kita gunakan untuk mendeteksi apakah sebuah situs juga memiliki ID Google AdSense yang sama dengan situs lainnya.

ads_direct:"google.com|pub-7784034061253020"

Select Columns +

Results 1 to 20 of 26

Rank	Domain	Resource	Status	Scanned	Simhash
3,100	kompas.com	ads.txt	Ok	2024-04-14	44a2a983538c
3,209	tribunnews.com	ads.txt	Failed	2023-10-10	41879282538c
8,040	bolasport.com	ads.txt	Ok	2024-04-15	c8a392854388
9,921	kompas.tv	ads.txt	Ok	2024-04-13	44a28945538c
18,909	sonora.id	ads.txt	Ok	2024-04-14	02ca888757cd
20,279	grid.id	ads.txt	Ok	2024-04-12	00a3b380470c
24,425	kontan.co.id	ads.txt	Ok	2024-04-15	80e3b883578c
28,211	kompasiana.com	ads.txt	Ok	2024-04-13	048aaa8357cc
29,716	kgnow.com	ads.txt	Ok	2024-04-17	44df8084cf18
32,906	gridoto.com	ads.txt	Ok	2024-04-12	c8a38ac453cd
36,911	kompas.id	ads.txt	Ok	2024-04-15	9463c984cbdd
54,254	motorplus-online.com	ads.txt	Ok	2024-04-12	4383a081538c
71,435	juara.net	ads.txt	Ok	2024-04-15	48a39a85578c
97,234	parapuan.co	ads.txt	Ok	2024-04-14	89a39ac5578c
129,407	tribunnewswiki.com	ads.txt	Failed	2023-08-12	41879287538c
224,995	tribunjualbeli.com	ads.txt	Failed	2022-12-08	1187928753cc
610,819	bolanas.com	ads.txt	Ok	2024-04-15	4883ba87558c
699,585	gridtechno.com	ads.txt	Ok	2024-04-16	02a393c737d2
-	jip.co.id	ads.txt	Ok	2024-04-11	c8a38ac453cd
-	kompasianival.com	ads.txt	Ok	2024-04-12	4287b0d67fdd

Disclaimer: layanan Well Known Dev akan terus dimutakhirkan. Tangkapan layar di atas adalah data Google ID milik Kompas pada tahun 2024 yang mungkin berbeda apabila kita mengakses situs layanan tersebut pada waktu yang berbeda.



**ALIANSI
JURNALIS
INDEPENDEN**
Alliance of Independent Journalist

BAB III.

AI DALAM PENELITIAN AKADEMIK DAN INDUSTRI MEDIA

BAB III AI DALAM PENELITIAN AKADEMIK DAN INDUSTRI MEDIA

Tujuan bab ini adalah untuk memperkenalkan beragam penggunaan tools AI di dunia akademik dan industri media, serta meningkatkan kewaspadaan terhadap problematika yang muncul dalam penggunaannya.

Pertanyaan pemantik:

1. Apa saja tools AI yang populer dan membantu kerja akademik khususnya riset dan publikasi artikel ilmiah?
2. Apa saja tools AI yang populer dan membantu dalam kerja jurnalistik dan industri media secara umum?
3. Bagaimana permasalahan teknis dalam penggunaan tools AI bagi dunia akademik dan industri media?

Metode penyampaian:

- Ceramah
- Praktik
- Diskusi

3.1. Penggunaan AI dalam Penelitian Akademik

Dalam satu dasawarsa terakhir, pengkajian soal peran dan dampak AI terhadap dunia akademik di dunia, termasuk Indonesia, terbelah menjadi dua. Pertama dalam konteks positif bahwa AI berkontribusi bagi akselerasi kerja-kerja akademik, terutama riset, pengajaran dan publikasi. Kedua, AI – dalam konteks negatif– bisa memicu aksi plagiarisme dan pelanggaran integritas akademik lainnya. Bab ini akan menguraikan aspek pertama dengan kewaspadaan atas munculnya aspek kedua. Dalam kerangka ini, akademisi dapat menempatkan AI secara proporsional, yaitu menempatkan AI sebagai partner kerja.

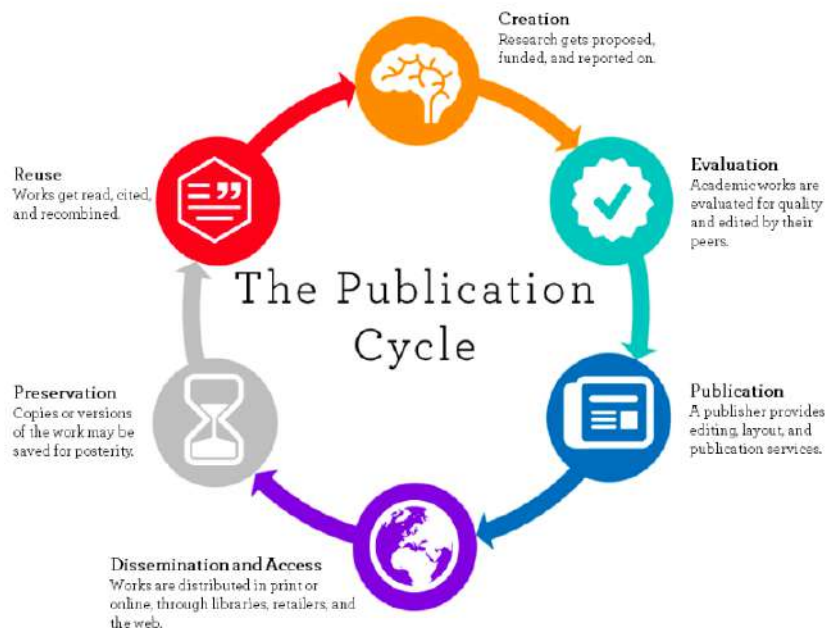
Ada tiga pembahasan dalam bab ini. Pertama, tahapan penelitian dalam dunia akademik dan peran AI. Kedua, peran AI dalam penulisan ilmiah hasil penelitian. Ketiga, beberapa isu yang perlu menjadi perhatian terkait keduanya, secara teknis dan etis.

3.1.1. Pelaksanaan Riset Akademik

Apakah dalam kerja riset atau publikasi kita selama ini sudah menggunakan AI? Jika ini ditanyakan ke dosen dan mahasiswa, hampir pasti jawabannya ya. Dari survei sederhana saat training of trainer AI bagi akademisi di Bogor, Jawa Barat akhir Februari 2025, di kertas kecil para peserta menulis sedikitnya lima tools AI yang pernah dipakai. Artinya, AI sudah akrab dengan mereka. Beberapa tools AI yang populer adalah: Zotero, Grammarly, Google Translate, Microsoft Copilot, Turnitin.

AI pada generasi awal ditandai dengan munculnya layanan search engine Google, mesin pencari artikel ilmiah yang hingga hari ini masih dianggap paling populer. Aplikasi AI kemudian mengalami revolusi, dari mesin pencari, lalu memiliki kemampuan mengkoreksi, menerjemahkan hingga memiliki kemampuan menulis seperti manusia.

Kerja penelitian hingga publikasi dalam dunia akademik merupakan suatu lingkaran kerja akademik melingkar seperti dapat dicermati pada gambar ini:



Sumber: <https://libguides.asu.edu/scholcomm/publishing>

Mengapa akademisi dan juga praktisi media melakukan penelitian? Ada beberapa alasan mendasar, yang pada gilirannya itu akan berpengaruh terhadap pelibatan AI. Pertama, untuk mencapai suatu kerja akademik yang berdampak kepada kehidupan sosial, tidak terbatas pada laporan administrasi. Kedua, bagian dari produksi untuk kekayaan intelektual,

termasuk paten bagi negara Indonesia. Ketiga, sebagai bahan baku publikasi ilmiah (baik pada jurnal di tingkat universitas, nasional, dan internasional). Keempat, upaya menghasilkan model/prototipe/teknologi tepat guna bagi transformasi sosial. Kelima, sebagai bahan penguatan dan pengayaan materi ajar/buku ajar/buku referensi dosen saat mengajar di kelas. Keenam, bagian dari kerja sosial untuk pemberdayaan/pengabdian masyarakat yang berbasis riset. Lebih jauh penelitian yang dilakukan kampus atau dosen memiliki keterkaitan dengan kiprah perguruan tinggi Indonesia dalam forum nasional dan internasional, melalui model kerjasama penelitian antar perguruan tinggi dan industri yang membangun reputasi. Terakhir, riset akademik akan menjadi sumber pendapatan alternatif perguruan tinggi negeri atau swasta di luar pendapatan klasik dari pembayaran SPP mahasiswa (*income generating sources*).

Merujuk metode penelitian yang dirumuskan Creswell (2010), ada lima tahapan utama dalam riset akademik. Hampir di semua tahap ini ada peran AI. Pertama, perumusan gagasan atau topik yang akan diteliti yang bisa dilakukan secara induktif (penelusuran situasi empirik) dan deduktif (kajian laporan studi-studi akademik terdahulu). Perumusan gagasan ini berujung pada pembuatan proposal yang melibatkan AI dalam review hingga formatnya. Kedua, pelaksanaan riset lapangan berupa pengumpulan data, yang diawali koordinasi tim riset untuk penyamaan persepsi, dll. Pengumpulan data itu melibatkan peran manusia dan teknologi digital seperti Googleform. Rekrutmen peneliti juga kerap kali melibatkan AI. Ketiga, tahapan analisis atas data yang terkumpul dari lapangan. Analisis data memakai pendekatan kualitatif, kuantitatif atau campuran, saat ini juga melibatkan beragam aplikasi AI seperti NVIVO. Keempat, penyampaian laporan hasil riset dalam bentuk oral/presentasi hingga laporan deskriptif—termasuk pemakaian dana. Teknologi AI membantu dosen/peneliti dalam memdesain laporan naratif, laporan keuangan (excel) hingga pembuatan PPT untuk presentasi. Kelima, penulisan artikel ilmiah yang menjadi luaran/kewajiban ke publik, yang dikirimkan ke jurnal nasional dan internasional bereputasi, baik dalam bahasa Indonesia atau bahasa Inggris.

Dalam keseluruhan kerja riset di atas, dosen atau akademikus pada umumnya selalu bersikap terbuka dan merujuk pada beragam database untuk menemukan kebaruan dari risetnya nanti. Di samping itu, dosen akan selalu menentukan topik riset yang selaras dengan peta jalan akademik yang ia minati sehingga memudahkannya dalam mencapai karir akademik, sejak dari asisten ahli hingga level guru besar.

Merujuk pada berbagai literatur, dalam proses awal kerja riset, pencarian informasi (baik primer atau sekunder) sangat memperhatikan dimensi

state of the art, kebaruan, yang dalam prakteknya dibantu beragam tools AI. Demikian halnya dalam proses perumusan masalah yang mengadopsi pola pikir pencarian problem atau *gap* (adanya kesenjangan antara situasi empirik dan akademik antara yang seharusnya dengan kenyataan). Pencarian dimensi kesenjangan (*gap*) ini harus dilakukan melalui studi literatur di pustaka digital dan atau observasi langsung ke lapangan.

Sebuah proposal riset yang baik, dan pada gilirannya dikerjakan dengan bantuan AI, akan selalu terdiri dari aspek-aspek substansi dan alur kerja seperti di bawah ini:

1. Judul Penelitian dan Abstrak
2. Pendahuluan (Latar belakang, Rumusan masalah, Tujuan dan Manfaat penelitian)
3. Kajian Pustaka (Peta konsep yang pernah dipakai)
4. Metode Penelitian
5. Daftar Pustaka
6. Lampiran (Jadwal, Sarana-prasarana, Anggaran penelitian)

Dalam proses riset, tahapan studi pustaka menjadi krusial. Dalam dua dekade terakhir proses ini kerap melibatkan AI. Bantuan AI dapat menjangkau bagaimana deskripsi yang analitikal atas kajian-kajian terdahulu atas topik yang dipilih, yaitu pada kajian konsep tertentu yang dikemas lebih sederhana, memusat pada satu konteks/varianbel/isu. Tools AI juga membantu perumusan kerangka konsep tertentu (*framework*), asumsi atas mazhab suatu konsep, pola pikir analitis. AI lebih jauh membantu merumuskan teori atau konsep yang relevan, merumuskan bentuk pertanyaan mana yang akan dijawab dari riset. Dengan kata lain, AI akan memberi petunjuk membuat formulasi rumusan masalah riset.

Selain studi pustaka, penentuan metode riset juga dapat melibatkan tools AI. Kerja pelibatan ini meliputi pilihan metode yang tepat, tahapannya secara terperinci, bahkan bisa dihubungkan dengan kebutuhan pendanaan.

Deskripsi bagian metode dalam proposal dan laporan penelitian mudah dikerjakan dengan AI, terutama untuk menghindari deskripsi dari aspek yang tidak perlu. Misalnya, metode penelitian tidak perlu lagi definisi tentang metode, apakah metode yang digunakan *up to date* (tidak *out of date*). Apabila ada sampling, tools AI mampu menjelaskan teknik samplingnya. AI juga membantu menjelaskan bagaimana peneliti melakukan analisis data hingga bagan alur kerja untuk penelitian multistadial.

Pada prinsipnya, AI membantu dalam proses kerja riset sejak data input (proses *adjustment*, *data processing* —proses assessment terkait interpretasi dan prediksi, kegagalan), hingga data outcome. Dari Google, ada sejumlah aplikasi AI yang bisa berperan penting, mulai dari search engine Google, Google scholar, Google form, hingga Google translate. Terbaru Google meluncurkan aplikasi AI-nya, Gemini. Beberapa tools AI lainnya juga semakin populer pasca kehadiran ChatGPT, seperti Microsoft copilot, Perplexity AI, Research Rabbit, dll.

Merujuk pada hasil survei yang dilakukan Litmaps, kontribusi AI dalam kerja akademik telah memberikan dampak pada sisi efisiensi waktu (*time efficiency*), terutama untuk kajian pustaka. AI juga memperkuat kolaborasi manusia-mesin dan antar-mesin, misalnya dalam mengatasi kendala bahasa asing ke bahasa Indonesia. AI juga bisa memperbaiki tingkat akurasi data dan penulisannya. Ada juga bantuan sitasi yang lebih reliable serta pendalaman atas suatu isu atau insights. AI juga bisa membantu *cross-disciplinary connections* antarberagam bidang ilmu. Lebih jauh soal ini dapat dicermati pada <https://www.litmaps.com/learn/best-ai-research-tools>.

Dalam artikel berjudul *Using Artificial Intelligence in Academic Writing and Research: An Essential Productivity Tool* (Khalifa dan Albadawy, 2024) disebutkan ada enam sektor penting dimana AI berkontribusi terhadap kerja akademik. Pertama, membantu generalisasi ide riset dan publikasi hasil riset, termasuk desain proposalnya. Kedua, memperbaiki konten dan struktur tulisan/laporan akademis. Ketiga, mendukung proses kerja pencarian pustaka dan melakukan sintesis atas berbagai literatur. Keempat, memperkuat manajemen data hasil riset dan pengelolaan analisisnya. Kelima, membantu dalam proses koreksi, edit, review dan publikasi hasil riset, terutama ke jurnal ilmiah. Keenam, membantu proses komunikasi antara pihak yang terlibat seperti peneliti, enumerator, informan, pengelola jurnal, penerima manfaat, dan pemberita dana riset, serta tata kelola etik-nya.

Khalifa dan Albadawy menyatakan, masing-masing tools AI memiliki kelebihan dan kekurangan. Misalnya, Zotero dan Mendeley sangat berperan dalam manajemen kajian pustaka, namun tidak dapat membantu dalam proses kerja penulisan artikel dan deteksi plagiarisme. Chat GPT membantu dalam asistensi penulisan artikel, tetapi tidak ada fasilitas analisis data. NVivo sangat berkontribusi dalam studi literatur dan analisis data, tetapi lemah dalam bantuan penulisan. Dengan kondisi seperti itu, kedua penulis merekomendasikan peneliti mengintegrasikan seluruh tools AI, tidak fokus kepada tools AI tertentu. Peneliti harus selalu memahami bahwa tools AI

terus bertumbuh sehingga selalu melakukan *skill update* dari segi teknis dan etis.

Publikasi Hasil Riset

Di lini masa media sosial orang Indonesia, termasuk dari para akademisi, bertebaran tawaran pelatihan atau bantuan teknis dalam kerja publikasi ilmiah di tengah maraknya bermunculan aplikasi AI. Dalam konteks ini, diperlukan sikap kritis, waspada dan sikap kembali kepada motivasi dan kehendak ilmiah dalam kerja menulis artikel untuk publikasi, terutama jika datanya hasil dari sebuah riset.

Motivasi publikasi dari sebuah artikel ilmiah bisa beragam. Hal itu pada gilirannya akan menentukan sejauh mana pelibatan tools AI serta pilihan aplikasi AI yang layak dipakai. Kehadiran beragam aplikasi akal imitasi dalam konteks publikasi hasil riset, khususnya melalui jurnal ilmiah, sangat terkait dengan *commodification in academic knowledge distribution* (Michael Nentwich, 2021), dan ini memicu pertanyaan dasar soal *who own knowledge* (Petrescu, 2024). Ringkasnya, tujuan menerbitkan laporan riset di jurnal adalah realisasi dari beragam motivasi: *culture of sharing-rising global knowledge; academic carier (Western model); money/academic commodification*.

Menulis artikel pada jurnal nasional dan internasional adalah juga upaya berbagi hasil riset untuk mengurangi 'ketimpangan informasi dan karya akademik' antara 'Barat' dan 'Timur', Ia juga sekaligus berperan dalam membentuk citra penulisnya, reputasi peneliti dari hasil risetnya, personal branding, suatu pencapaian/rekognisi (global academic presence), dan manajemen reputasi akademik. Lebih jauh, publikasi hasil riset juga merupakan bentuk 'silaturahmi' akademik internasional, memperkuat basis komunitas pada minat studi serupa, peningkatan karir dan otoritas akademik seperti Lektor, Lektor Kepala dan Guru Besar. Pada akhirnya, sebuah tulisan akademik yang terbit di level internasional dan berbasis riset menambah jumlah penghargaan, yang akan memberi benefit finansial dan sosial. itu juga menguatkan diseminasi hasil riset sebagai public good yang merujuk pada cycle *disseminate, preserve, reuse*.

Disamping dari hasil riset terbaru, suatu publikasi dapat berasal dari kajian riset lama yang diolah kembali, atau riset berjenjang sejak dari level program studi, universitas hingga riset yang diperoleh dari kolaborasi internasional. Data publikasi juga dapat berasal dari beragam ekosistem dalam data raya digital sebagai berikut:

1. Pengamatan atau riset tidak terstruktur (observasi, kajian literatur, analisis dokumen, dll. yang diolah menjadi laporan riset).
2. Pengembangan naskah paper di jurnal nasional, artikel dalam buku atau paper/makalah dalam seminar/konferensi, laporan/naskah publikasi dari skripsi/ tesis/disertasi, atau tulisan akademik lain dari karya pribadi atau kolaborasi.

Ada banyak pilihan dalam publikasi hasil riset. Antara lain:

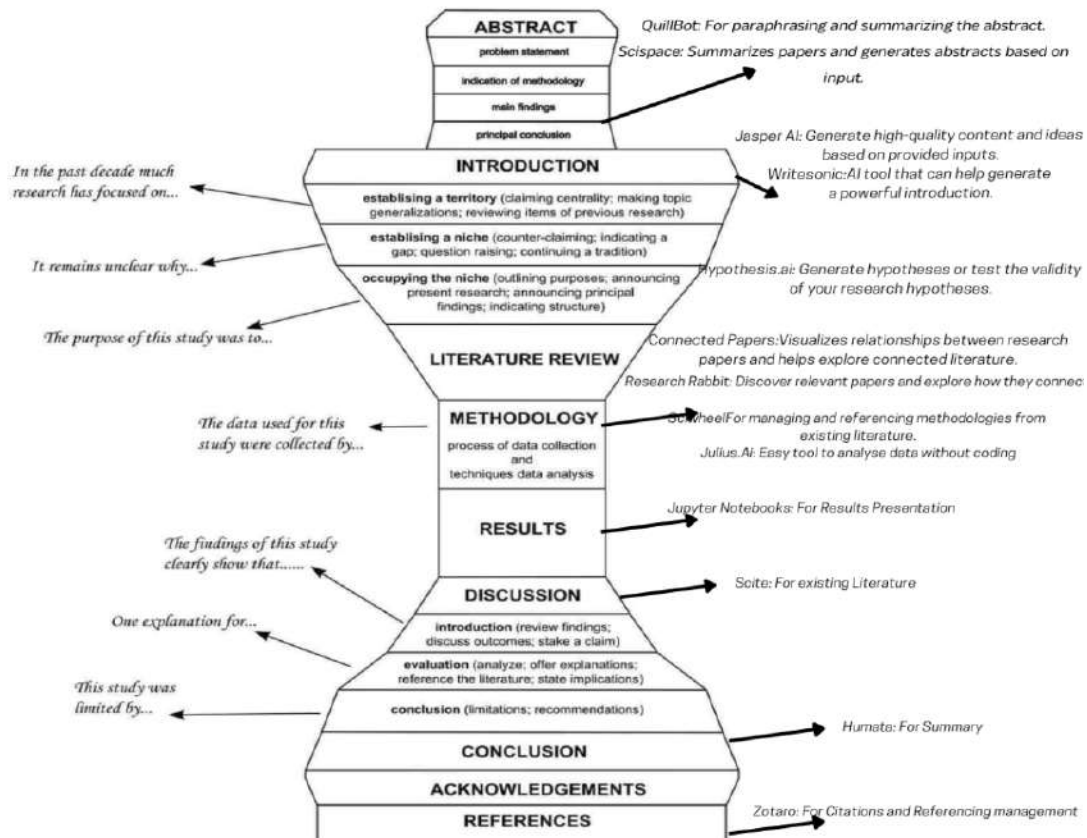
1. Jurnal internasional *terindeks* (Berapapun jumlah penulisnya, yang terdiri dari penulis utama, penulis anggota).
2. Buku dalam bahasa internasional pada penerbit *terindeks* (Berapapun jumlah penulisnya, yang terdiri dari penulis utama, penulis anggota).
3. Artikel dalam buku berbahasa internasional pada penerbit *terindeks* (Penulis utama, penulis anggota)
4. Artikel yang dimuat pada prosiding *konferensi internasional terindeks Scopus* (Penulis utama, penulis anggota)

Dalam kaitannya dengan peran AI dalam riset dan publikasi akademik, ada banyak aplikasi yang mendekati 100% kemampuan manusia dalam hal berikut: *literature search and information retrieval; data analysis; summarizing the content; bibliography and citation management; create abstracts, images, videos, and manuscripts; image quality control; content formatting; language translation and grammar checking; target journal selection; peer review and statistical quality assessment; similarity check to prevent plagiarism; detection of data and image fabrication; detection of paper mills, etc.*

Litmaps membuat survei terkait popularitas tools AI untuk kerja akademik. Ada beberapa tools AI yang jamak dipergunakan di dunia akademik dalam analisis data berbasis open source, antara lain, SPSS, NVivo, Google AutoML. Dalam hal pencarian literatur, beberapa tools AI ini cukup populer: Semantic Scholar, Litmaps, Google Scholar, Scopus. Adapun dalam hal *editing, tone suggestions, paraphrasing dan summarization*, beberapa tools ini akrab di telinga dan tangan dosen: Grammarly, Paperpal, dan Quillbot.

Gambar berikut ini menggambarkan bagaimana AI tools membantu akademisi membuat kerangka hingga substansi tulisan ilmiah:

Ai Tools for every Step of Research



Sumber: <https://thephdcoaches.com/ai-tools-for-every-step-of-research-a-comprehensive-guide/>

Berkenaan penggunaan AI untuk publikasi ilmiah, ada banyak potensi risiko yang muncul. Dua di antaranya adalah fenomena naskah palsu (*paper mills*) dan retraksi. Penggunaan AI yang serampangan dapat mengarah pada produksi paper mills, praktik di mana naskah ilmiah diproduksi secara massal, dan kemudian dijual kepada peneliti yang ingin meningkatkan jumlah publikasi dengan cepat (Ali & Djalilian, 2023). Praktik ini sangat merusak integritas ilmiah dan sulit dideteksi, terutama karena AI dapat menghasilkan teks yang tampak orisinal.

Untuk menghadapi ancaman dari adanya naskah semacam ini, beberapa penerbit telah memakai alat deteksi khusus yang didukung oleh AI, seperti PapermillAlarm dan ZeroGPT. Alat ini dirancang untuk mendeteksi naskah yang dihasilkan secara otomatis dan mengidentifikasi tanda-tanda

kecurangan, seperti manipulasi data atau gambar. Namun, alat-alat ini masih memiliki keterbatasan dan dapat menghasilkan kesalahan positif atau negatif. Deteksi oleh manusia tetap perlu untuk memastikan akurasi. Oleh karena itu penting mengembangkan pedoman penulisan akademik oleh penerbit jurnal yang lebih rinci dan spesifik mengenai penggunaan AI dalam kerja penelitian dan publikasi.

Seiring dengan meningkatnya penggunaan AI dalam penelitian, jumlah retraksi artikel ilmiah juga meningkat. Retraksi adalah proses di mana artikel ditarik kembali setelah diterbitkan karena ditemukan pelanggaran etika atau kesalahan teknis. Pada beberapa tahun terakhir banyak artikel yang ditarik karena isu plagiarisme, duplikasi publikasi, dan manipulasi data. Semua ini diperburuk oleh massifnya penggunaan AI.

Masalah lanjutan dari fenomena ini adalah bagaimana menentukan sebuah kesalahan itu disebabkan oleh manusia atau AI. Untuk memitigasi kasus-kasus plagiarisme, para pengelola penerbitan dan akademisi dapat merujuk pedoman COPE (<https://publicationethics.org/>) yang menekankan transparansi proses retraksi, termasuk mengungkapkan jika AI terlibat di dalam suatu artikel. Pedoman retraksi dari COPE telah mencakup alasan-alasan untuk retraksi, seperti manipulasi gambar, penggunaan data tanpa izin, dan masalah hukum. Pedoman ini mengatur bahwa penulis dan editor harus memperhatikan dan memberlakukan ketentuan seperti di bawah ini:

The authors are urged to provide evidence/declaration that the findings are reliable, free from an error (miscalculation or experimental error), or as a result of fabrication (eg, of data) or falsification (image manipulation). The authors declare findings have not previously been published elsewhere as a disclosure to the editor, or having permission to republish, or justification (ie, cases of redundant publication); The author(s) avoid a failure to disclose a major competing interest (a.k.a. conflict of interest) that, in the view of the editor, would have unduly affected interpretations of the work or recommendations.

3.2. Penggunaan AI dalam Penelitian di Industri Media

3.2.1 Bagaimana jurnalis dan ruang redaksi menggunakan AI?

AI sudah jamak digunakan dalam industri media, mulai dalam proses pengumpulan informasi dan data (*news gathering*), produksi berita (*news production*), dan diseminasi konten (*news distribution*). Hal ini merujuk

pada [survei](#) terhadap 105 media di 46 negara pada April hingga Juli 2023 oleh London School of Economics and Political Science (LSE) (Beckett, 2023). Alasan penggunaannya adalah untuk meningkatkan efisiensi dan produktivitas para jurnalis agar bisa lebih menggunakan waktunya untuk menghasilkan karya inovatif dan kreatif lainnya.

Dalam tahapan pengumpulan informasi dan data, layanan AI seringkali digunakan untuk mengubah format data, yang semula Optical Character Recognition (OCR) menjadi data yang mudah diolah misal dalam format Excel, CSV, txt dan lainnya. Misalnya, jurnalis seringkali mendapatkan data dalam format JPG yang kemudian disimpan dalam bentuk PDF. Perangkat AI dapat membantu mengubah teks dalam gambar menjadi data yang bisa dibaca oleh mesin, dalam bentuk Excel dan lainnya. Selain itu, layanan AI juga digunakan untuk proses transkrip wawancara atau siaran langsung. Manfaat AI lainnya adalah mendapatkan ringkasan dari sebuah sumber bacaan dalam proses riset, mendeteksi tren, dan mendapatkan temuan baru sebuah berita saat melakukan riset.

Dalam proses produksi, AI juga digunakan untuk beragam hal. BBC, misalnya, menggunakan *tagging* untuk mengkategorisasikan berita agar mudah dicari dan diambil oleh mesin pencarian (*search engine*). Selain itu, ada pula ringkasan berita (*summary*), yang memudahkan audiens untuk memahami intisari berita dalam beberapa kalimat atau satu paragraf. Media yang menggunakan fungsi ini di antaranya *BBC*, *Reuters*, *South China Morning Post*. *Robot journalism* juga digunakan oleh beberapa media luar dan Indonesia, seperti *Los Angeles Times* untuk melaporkan gempa bumi, *The Associated Press* untuk menulis berita *baseball*, *The Washington Post* untuk memberitakan sepak bola, dan TV One yang memiliki presenter AI. Penggunaan AI untuk mengecek fakta dilakukan beberapa media, seperti *AFP* dan *Liputan 6*. Untuk analisis dan visualisasi data, *BBC* dan *the New York Times* juga ikut menggunakannya. Penggunaan lainnya adalah untuk mengecek apakah penulisannya sudah sesuai dengan panduan masing-masing media, seperti yang dilakukan oleh *AFP* dan *Irish Reminder*.

Pada proses distribusi konten, banyak media sudah menggunakan bantuan AI. *The Times of London* membuat produk bernama JAMES yang digunakan untuk menganalisis perilaku konsumen dan memberikan konten yang

sesuai dengan perilaku dan ketertarikan pembaca. Hal yang sama juga dilakukan *BBC*. Sejumlah media juga menggunakan perangkat seperti *Echobox* dan *SocialFlow* untuk mengatur penayangan artikel atau berita. Aplikasi lainnya, yang membantu jurnalis untuk mengecek tren pemberitaan dan percakapan di media sosial (*AI-driven SEO tools*), adalah *Ubersuggest*, *NewsWhip Spike*, dan *Google Trend*. Untuk membuat ringkasan sosial media, *Bloomberg* membuat sendiri alat berbasis AI yang disebut dengan *BloombergGPT*. Layanan AI untuk distribusi konten juga digunakan media dalam bentuk *chatbot* dan iklan digital yang menyasar audiens dengan perilaku tertentu.

Bagaimana *BBC* beradaptasi dengan AI? Di dalam ruang redaksi *BBC* sudah dikembangkan beragam perangkat berbasis AI, di antaranya:

- **Live transcription machine.** Mesin ini dikembangkan sendiri oleh tim *software engineer* *BBC* untuk secara langsung mentranskrip secara langsung konferensi pers dan kemudian secara otomatis memotong klip, bisa dalam bentuk audio atau video, untuk disebar ke media sosial.
- **Machine to pooling up live page stories.** *BBC* juga mengembangkan mesin untuk memantau siaran langsung pada situs daring (digital) *BBC* di 42 tayangan bahasa (*BBC World Service*). Mesin ini digunakan para editor untuk mengecek dan mengambil berita yang menarik dari belahan dunia lainnya.
- **Graphic generator.** Perangkat AI ini digunakan untuk membuat ulang grafik dari versi digital yang tayang di situs, menjadi versi media sosial.
- **Summarise points.** *BBC* juga memiliki perangkat *in-house* yang digunakan untuk membuat ringkasan berita yang diunggah ke dalam *Content Management System*-nya.

Dalam keseharian, AI juga digunakan dalam proses pembuatan berita *hard news*, pengecekan fakta, dan liputan in-depth dan investigatif.

1. Dalam pembuatan berita *hard news*, AI digunakan:

- Untuk mengecek apa yang sedang tren dan populer dengan menggunakan *Google Trend*, *NewsWhip Spike*, dan *Ubersuggest*.

- Untuk mencari apa yang diminati oleh audiens dan belum banyak ditulis oleh media, dengan menggunakan NewsWhip Spike.
2. Dalam proses pengecekan fakta, AI digunakan misalnya untuk:
- **Scraping mis/disinformation content.** Mendeteksi pernyataan untuk cek fakta, mengidentifikasi klaim yang dibuat melalui pidato, wawancara, dan bahan audio lainnya yang dilakukan oleh Newtral menggunakan Claim Hunter.
 - **Debunking process.** Newtral juga memiliki perangkat otomatis untuk mengecek fakta menggunakan NLP dan *machine learning*. Ada pula Duke Reporter Lab melalui alat yang diberi nama FactStream. Ini untuk mengecek klaim palsu pada pidato, debat, atau kegiatan publik dengan membandingkannya dengan fakta yang sudah diperiksa sebelumnya.
 - **Chatbots.** Liputan6.com dan Rappler menggunakan *chatbot* untuk diseminasi produk cek fakta kepada audiennya.
 - **Tracking politicians' statements on some topics during the election.** *The New York Times* membuat alat pelacak jejak ucapan yang dilontarkan Presiden Amerika Serikat Donald Trump dan mengeceknya apakah benar atau tidak. Di Ghana, alat serupa juga dibuat untuk mengecek ucapan politisi, melalui knowyourleader.ai.
3. Dalam pembuatan liputan in-depth dan investigasi, AI dipakai untuk:
- **Proses membersihkan data**
- Dalam proses ini, perangkat AI membantu jurnalis untuk membersihkan data dan mengubah format data menjadi lebih mudah dibaca oleh mesin. Contohnya adalah dalam proses analisis, yakni mengubah teks dalam gambar menjadi dataset. Tangkapan layar di bawah ini menunjukkan proses *data cleaning*. Mulanya dokumen yang dimiliki adalah Surat Keputusan Hasil Pileg anggota DPRD Sumatera Utara tahun 2019 dari situs Bawaslu dan berbentuk file PDF. Di dalamnya ada tabel perolehan suara tiap partai. Untuk melakukan analisis lebih jauh terkait partai mana yang dominan di provinsi tersebut, kita membutuhkan data tabel tersebut dalam

bentuk CSV atau Excel. Nantinya data ini juga dibutuhkan untuk visualisasi. Yang kita butuhkan untuk itu adalah tangkapan layar tabel dari dokumen PDF. ChatGPT membantu mengonversi teks dalam gambar tersebut dan mengekstrasikannya ke dalam format yang kita butuhkan. Hal ini sangat memangkas waktu, alih-alih harus memasukkan data ke dalam tabel secara manual.

This document appears to display the seat allocation results for a political party election in North Sumatra (Sumatera Utara) for Electoral District 2. Here's a breakdown of its structure:

- Header Information:**
 - Electoral District: Sumatera Utara 2
 - Province: Sumatera Utara (North Sumatra)
 - Seat Allocation: 7 seats
- Table Contents:**
 - Columns:**
 - No Urut: Order number of the party
 - Nama Partai: Name of the political party

Would you like this information converted into a table format, or do you need a specific analysis?

From column Nama partai, Suara sah, and Jumlah perolehan kursi, make a table

No Urut	Nama Partai	Suara Sah	Jumlah Perolehan Kursi
1	Partai Kacangkutan Bangsa	19154	0
2	Partai Gerakan Indonesia Raya	67502	1
3	Partai Demokrasi Indonesia Perjuangan	76106	2
4	Partai Golongan Karya	75381	1

Here is the table with the columns for Party Name, Valid Votes (Suara Sah), and Total Seats Acquired (Jumlah Perolehan Kursi) based on the data you provided. Let me know if you need further analysis or adjustments.

Contoh lainnya adalah menyatukan puluhan data JSON hasil Pemilu Sri Lanka yang digunakan untuk analisis dan visualisasi. Untuk ini, ChatGPT diminta membuat satu skrip bahasa pemrograman Python yang berfungsi untuk *merge* data tersebut.

Convert this to a table

To convert this election data to a table, I will consolidate key columns based on the provided polling divisions and parties. Here's the structured table format using sample data from Trincomalee and Digamadulla polling divisions:

Electoral District	Polling Division	Party Name	Valid Votes	Total Seats Acquired
Trincomalee	Seruwela	All Ceylon T. Congress	84	N/A

can you write me a script in Python to combine json?

Certainly! Below is a Python script that reads multiple JSON files, extracts data, and combines it into a single JSON structure, which you can then save as a new file.

Python Script to Combine JSON Files

```
python
import json
import glob

def combine_json_files(input_folder, output_file):
    # Initialize an empty list to store all data
    combined_data = {"data": []}

    # Get a list of JSON files in the input folder
    json_files = glob.glob(f"{input_folder}/*.json")

    for file_path in json_files:
        with open(file_path, "r") as file:
            data = json.load(file)

            # Adjust this part based on the structure of your JSON files.
            # Here, assuming each file contains similar "by_party" structure
            # with "id_name", "id_name", and "by_party" data
            division_data = {}
            "id_name": data.get("id_name"),
            "id_name": data.get("id_name"),
            "by_party": data.get("by_party"), []
            }

            combined_data["data"].append(division_data)

    # Save the combined data to a new JSON file
    with open(output_file, "w") as output_file:
        json.dump(combined_data, output_file, indent=4)

print(f"Combined JSON saved to {output_file}")

# Usage example
combine_json_files(input_folders="path/to/your/json/files", output_file="combined.json")
```

Contoh lainnya adalah membersihkan awan pada citra satelit. Gambar di bawah adalah citra satelit sungai di Yangon, Myanmar, yang hilang dan terputus seiring berubahnya sungai tersebut menjadi daratan dari tahun ke tahun. Dalam proses pembersihan, AI membantu menghilangkan awan-awan yang muncul saat citra satelit dihapus. Caranya, pakai bahasa pemrograman melalui Google Earth Engine.



- **Proses analisis**

AI juga membantu dalam proses analisis yang tidak mungkin dilakukan secara manual. Pada artikel di bawah ini, BBC melakukan analisis aktivitas kapal perang Cina di pangkalan militer Angkatan Laut Kamboja, Ream.

Jurnalis mengalami kesulitan untuk masuk ke dalam pangkalan tersebut karena terbatasnya akses yang diberikan oleh pemerintah Kamboja kepada pihak luar. Satu-satunya cara langsung atau manual untuk melihat aktivitas yang ada di dalam pangkalan tersebut adalah dengan menaiki bukit yang ada di sekitar pangkalan dan mengambil gambar menggunakan kamera dengan lensa lebar.

Dengan keterbatasan tersebut, perangkat AI sangat membantu reportasenya. Alih-alih turun ke lapangan dengan akses terbatas, citra satelit dapat secara jelas menangkap perubahan dan perkembangan pembangunan pangkalan dari tahun ke tahun. AI juga membantu mengidentifikasi adanya kapal perang Cina yang bersandar di pelabuhan dalam kurun waktu beberapa bulan.

Apa arti dari temuan lapangan menggunakan AI ini? Aktivitas militer Cina di pangkalan militer milik Kamboja ini dapat mengguncang stabilitas politik dan keamanan di Laut China Selatan, serta memicu ketegangan dengan Amerika Serikat. Hasil temuan soal aktivitas militer Cina ini sudah dikonfirmasi oleh peneliti politik dan keamanan serta pengamat militer.



Contoh lain dari pemanfaatan AI adalah mengecek perubahan lahan dari waktu ke waktu. Para jurnalis yang tergabung ke dalam tim From Above (proyek JournalismAI dari LSE), yakni wartawan dari *Bloomberg*, *LaNacion* dan *CLIP*- bekerja sama dengan Knight Lab di Northwestern University mengembangkan skrip Python yang bisa mendeteksi perubahan tutupan lahan di suatu daerah. Perangkat ini dapat dikembangkan untuk mencari beragam bahan atau topik untuk liputan, misalnya, perubahan iklim di suatu daerah, perubahan

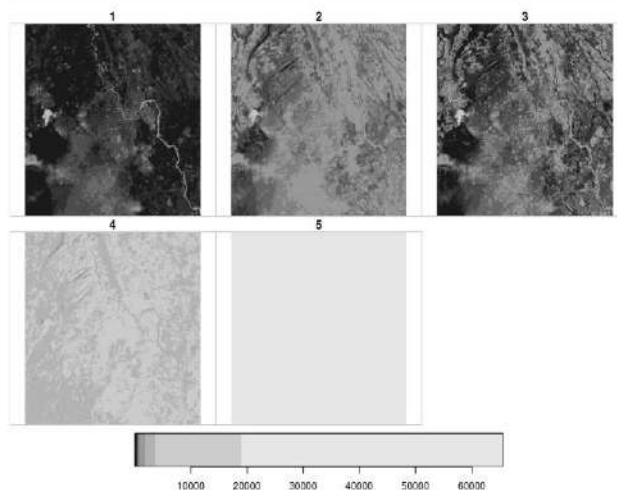
pergerakan hewan langka, perubahan penggunaan lahan dari hutan ke perkebunan, dan lainnya.

Reading the data in

Then we read in and explore the satellite data matching our Area of Interest, previously downloaded from services such as Planet's NICFI or Sentinel data. Encoded in a satellite image, there is reflectance information encoded in blue, green, red and near infra red spectrums of an image such as the ones from the Planet program. Load the satellite image, in this case Planet's analytical tif file with four bands: G,R,B and Near Infrared (NIR)

Understanding the layers of raster images

```
satellite_data <- read_stars("input/colombia2_analytic.tif", proxy = T, resample = "cubic_spline")
plot(satellite_data)
```



Sumber: Tangkapan layar https://datacritica.github.io/FromAboveAI_guide/

- **Proses visualisasi data**

Proses visualisasi data juga bisa dilakukan oleh Gen-AI dengan memasukkan *prompt* dan dataset yang diinginkan. Aplikasi yang bisa membantu proses ini adalah Co-pilot dan JuliusAI. Visualisasi menggunakan AI ini masih jarang dilakukan ruang redaksi media.

Implementasi AI di Ruang Redaksi Media di Indonesia dan Tantangannya

Penggunaan AI tercatat mengalami peningkatan yang signifikan, termasuk di kalangan anggota Asosiasi Media Siber Indonesia (AMSI). Teknologi ini diadopsi dan dimanfaatkan dalam berbagai aspek, mulai dari penyuntingan, penandaan otomatis (*automatic tagging*), pengisi suara (*voice-over*), hingga pembuatan avatar.

Dalam [focus group discussion \(FGD\) yang diselenggarakan AJI Indonesia](#) pada 17 September 2024, juga ditemukan sejumlah pola pemanfaatan AI di organisasi berita di Indonesia, baik di media nasional maupun lokal. Umumnya pemanfaatannya berkisar pada pencarian data serta informasi awal, diikuti oleh pencarian atau penyusunan ide liputan, penyuntingan bahan dan membantu proses analisis data, hingga personalisasi konten.

Tangkapan layar di bawah adalah bentuk penggunaan AI oleh media lokal Zonautara.com untuk melacak janji politik yang dilontarkan oleh calon anggota legislatif yang berkompetisi pada Pilkada 2024 lalu.



Dengan melihat praktik pemanfaatan AI yang sudah dilakukan oleh ruang redaksi, apa saja tantangannya?

- **Teknis.** AI terus berkembang dengan banyak inovasi baru. Jurnalis mengalami kesulitan untuk terus beradaptasi dengan hal yang baru dalam waktu yang sangat pendek.
- **Etik.** Bagaimana jurnalis bisa secara bijak menggunakan AI dan menghindari bias algoritma yang ada di dalamnya? Ini juga masih menjadi tantangan tersendiri.
- **Budaya.** Masih ada resistensi dari kelompok tertentu di mana AI dianggap sebagai ancaman karena akan menggantikan peran jurnalis, alih-alih membantu kerja mereka.
- **Manajerial.** Sulitnya mengimplementasikan AI karena banyaknya tim manajemen atau pimpinan yang harus memberikan izin untuk

penggunaannya. Di satu sisi, ada pula juga tuntutan dari atas yang mengharuskan jurnalis menggunakan AI pada situasi yang mungkin sebenarnya tidak perlu.

Dengan situasi seperti ini, apa yang perlu dilakukan ke depan? Menurut Becket (2023), perlu adanya kolaborasi, penelitian, dan pelatihan dari kalangan akademik dan praktisi media untuk mengembangkan perangkat AI yang membantu proses pembuatan karya jurnalistik dan riset untuk keilmuan.

3.2.2 Analisis dan visualisasi data menggunakan Gen-AI

Untuk kebutuhan analisis dan visualisasi sederhana, bisa dilakukan dengan meminta Gen-AI (menggunakan *prompt*) untuk membersihkan, mencari pola, dan memvisualisasikan dataset,

Bagaimana cara membuat *prompting* yang baik?

- **Specify role.** Posisikan kita sebagai analisis data atau peneliti.
- **Read.** Minta AI untuk mengenali data dan format, variable, value.
- **Detailed tasks.** Apa yang ingin dilakukan?
- **Audience.** Tentukan siapa yang menjadi audiens-nya.
- **Context.** Biasanya AI sudah bisa langsung mengidentifikasi kolom. Akan tetapi lebih baik bisa menambahkan konteks data dan sumbernya dari mana.
- **Format.** Pastikan bentuk *output*-nya berupa tabel, CSV, atau yang lain.
- **Ingat prinsip analisis dan visualisasi.** Gen-AI hanya membantu kita untuk melakukan kerja dengan lebih efisien. Yang paling penting adalah bagaimana kita memiliki pola pikir yang kritis dan paham ke arah mana dataset ini akan kita gali.

Perangkat Gen-AI seperti ChatGPT, Copilot dan Julius AI bisa digunakan untuk mengolah dataset, mulai dari membersihkan, menganalisis, hingga visualisasi. Ada pula dua perangkat lainnya untuk membantu riset, yakni Gemini dan NotebookLM. Berikut ringkasan kemampuan perangkat-perangkat tersebut.

Tabel 3.

Aktivitas atau karakteristik	ChatGPT	Copilot	JuliusAI	Gemini	NotebookLM
Meriset atau mencari informasi	v	v	v	v	v
Membersihkan data (termasuk fungsi OCR untuk mengambil data dalam bentuk gambar)	v	v	v	v	x
Menganalisis data	v	v	v	x	x
Memvisualisasikan data	v	v	v	x	x
Menyediakan skrip Python/R	v	x (hanya saat diminta)	v	x	x
Bisa mengunggah dataset (Excel), dokumen (PDF, Doc, TXT), gambar (JPG dan PNG)	v	v (Semua bisa kecuali JPG atau PNG)	v	v (Semua bisa kecuali Excel dan CSV)	v (Hanya bisa dalam bentuk PDF dan .doc atau Google Doc dan mengambil tabel di dalamnya)
Bisa mengunggah audio dan memintanya untuk mentranskrip atau menganalisis	v	x	v	x	v

Hasil tangkapan layar di bawah adalah contoh bagaimana ChatGPT merespons *prompt* untuk menganalisis data. Data berikut terkait dengan gaji pekerja di sektor *data science* di seluruh dunia di berbagai level pengalaman dan geografis.

DataScience Salaries 2024 Unable to display visualization

Read this and categorise job title into broader group, make a new column of it.

The dataset contains various columns related to salaries, job titles, and employment details. To categorize the "job_title" into broader groups and add a new column for it, I'll create a mapping for job titles to broader categories (e.g., "Data Scientist," "ML Engineer," etc., grouped into "Data Science" or "Machine Learning").

Let me proceed. [-]

Data Science Salaries With Job Categories				
	work_year	experience_level	employment_type	job_title
1	2021	Ml	FT	Data Scien
2	2021	Ml	FT	BI Data An
3	2020	Ml	FT	Data Scien
4	2021	Ml	FT	ML Engine
5	2022	SE	↓ ↑	Lead Mact Learning F

Ask anything

+ Search ...

Look for only data in 2024, and find the top 3 companies paying highest salaries in each experience level

Top 3 Companies Paying Highest Salaries By Experience Level I...				
	company_location	company_size	experience_level	salary_in_usd
1	MX	M	EN	774000
2	US	M	EN	300000
3	US	M	EN	300000
4	US	M	EX	448000
5	US	M	EX	438000
6	US	M	EX	408500

I have provided a list of the top 3 companies paying the highest salaries in 2024 for each experience level. Let me know if you'd like to explore or analyze this data further! [-]

Hasil tangkapan layar di bawah adalah contoh bagaimana Gemini merespons *prompt* untuk riset soal konflik di Sigi. Gemini, buatan Google, memang tidak bisa memberikan layanan untuk mengolah data, tetapi untuk ini Google memiliki layanan Google Spreadsheet --meski harus dilakukan manual dan tidak otomatis seperti perangkat AI lain.

Gemini
2.0 Flash

Doba Gemini Advanced

Konflik di Sigi

- Kabupaten Sigi, Sulawesi Tengah, Indonesia, telah mengalami beberapa konflik yang kompleks dan beragam. Berikut adalah beberapa poin utama mengenai konflik di Sigi:

 - Serangan Sigi 2020:**

 - Pada 27 November 2020, sebuah keluarga dibunuh oleh orang tak dikenal di Desa Lembantongoa, Kecamatan Pakolo, Kabupaten Sigi.
 - Pelaku kemudian diketahui adalah kelompok Mujahidin Indonesia Timur (MIT) pimpinan Ali Kalora.
 - Serangan ini memicu kecaman luas dan upaya pengejaran oleh aparat keamanan.
 - Konflik Antar Desa:**

 - Kabupaten Sigi sering mengalami konflik antar desa yang dipicu oleh berbagai faktor, seperti sengketa lahan, batas wilayah, dan masalah-masalah sosial lainnya.
 - Konflik ini sering kali melibatkan kekerasan dan dapat berdampak serius pada kehidupan masyarakat setempat.
 - Penyelesaian konflik antar desa seringkali menggunakan cara kearifan lokal.

Minta Gemini

Gemini dapat membuat kesalahan, jadi periksa kembali hasilnya

Copilot adalah salah satu layanan Gen-AI yang bisa membaca dataset, memungkinkan pengguna untuk mengunggah data dalam berbagai format. Copilot, sama seperti dengan JuliusAI, bisa ‘menawarkan’ hasil analisis untuk membaca pola dari dataset. Tapi, untuk fungsi ini, seperti layaknya tahapan riset, lebih baik pengguna membersihkan datanya terlebih dulu sebelum memulai proses analisis.

Copilot

Yes, I can read and analyze the data from the file you uploaded. Here's a summary of the dataset:

Basic Information

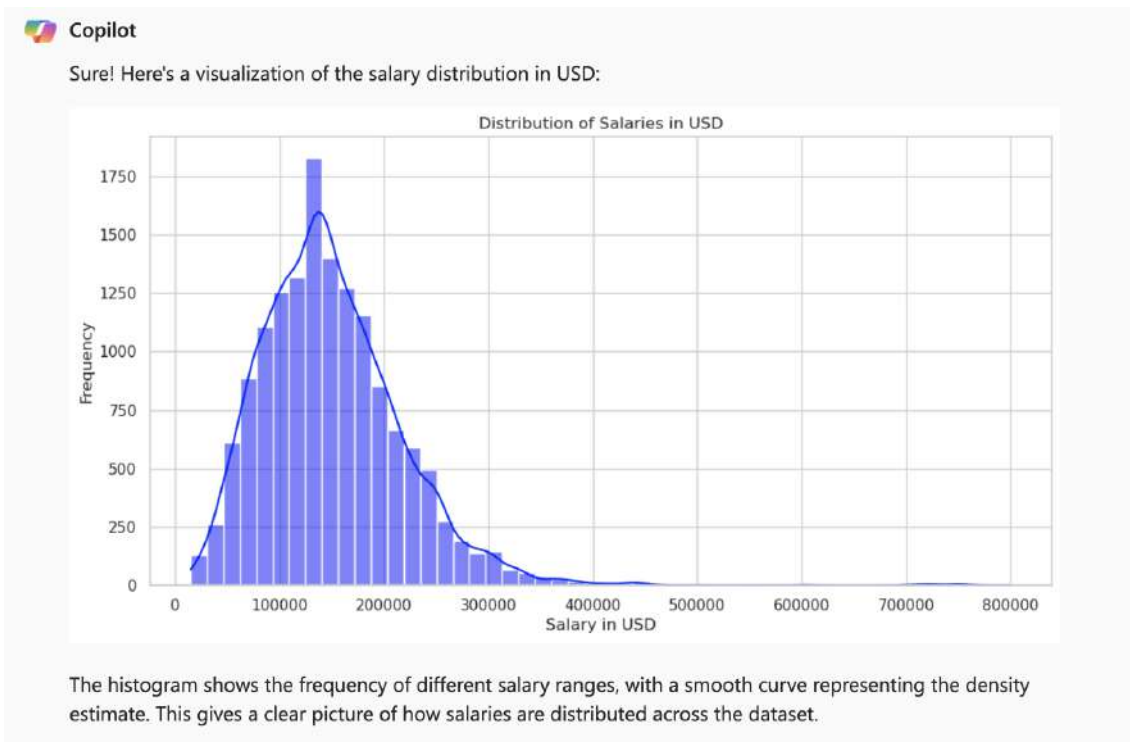
- Total Entries: 14,838
- Columns: 11 (work_year, experience_level, employment_type, job_title, salary, salary_currency, salary_in_usd, employee_residence, remote_ratio, company_location, company_size)

First Few Rows

work_year	experience_level	employment_type	job_title	salary	salary_currency	salary_in_usd	employee_residence	remote_ratio	company_location	company_size
2021	MI	FT	Data Scientist	304000	CLP	40038	CL	100	CL	L
2021	MI	FT	BI Data Analyst	110000	HUF	36259	HU	50	US	L
2020	MI	FT	Data Scientist	110000	HUF	35735	HU	50	HU	L

View prompts

Copilot juga bisa memberikan visualisasi dari data yang kita analisis, seperti terlihat dalam tabel di bawah ini.



Tangkapan layar di bawah ini adalah bentuk layanan dari JuliusAI, yang sampai saat ini merupakan perangkat paling bagus dibandingkan empat lainnya untuk menganalisis dataset. JuliusAI bisa menawarkan beragam hasil analisis. Tapi perlu tetap kita cek akurasi. Kita sebagai pengguna harus menempatkan diri sebagai “peneliti” yang memahami konteks dari topik riset.

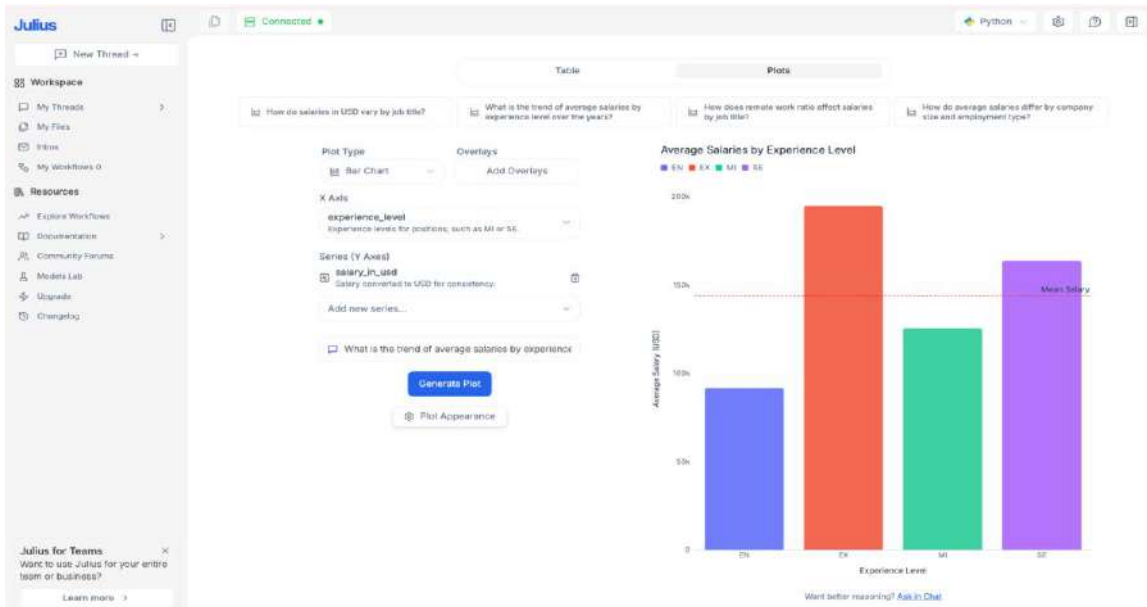
Table Plots

How do salaries in USD vary by job title? What is the trend of average salaries by experience level... How does remote work ratio affect salaries by job title? How do average salaries differ by company size and...

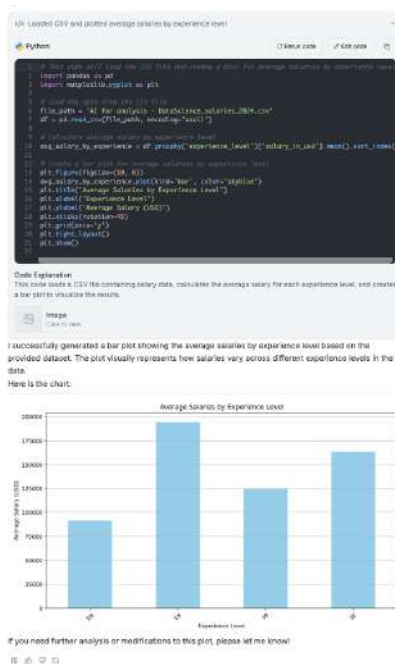
	work_year	experience_level	employment_type	job_title	salary	salary_currency	salary_in_usd	employee_res
0	2021	MI	FT	Data Scientist	30400000	CLP	40038	CL
1	2021	MI	FT	BI Data Analyst	11000000	HUF	36259	HU
2	2020	MI	FT	Data Scientist	11000000	HUF	35735	HU
3	2021	MI	FT	ML Engineer	8500000	JPY	77364	JP
4	2022	SE	FT	Lead Machine Learning Engineer	7500000	INR	95386	IN
5	2021	MI	FT	ML Engineer	7000000	JPY	63711	JP
6	2021	SE	FT	Data Science Manager	7000000	INR	94685	IN
7	2022	EN	FT	Data Scientist	6600000	HUF	17684	HU
8	2022	EX	FT	Head of Machine Learning	6000000	INR	78309	IN
9	2022	EN	FT	Research Engineer	5500000	JPY	41809	JP
10	2023	MI	FT	Head of Data Science	5000000	INR	60805	IN

JuliusAI juga bisa memberikan layanan visualisasi data. Namun sebaiknya kita juga memahami prinsip visualisasi data, misal, *colour visibility* atau

warna apa yang sesuai dan mudah dipahami orang dengan buta warna serta elemen apa saja yang harus ada di dalam sebuah grafik (judul, x dan y axis, unit pengukuran, sumber, keterangan, dan lainnya).



Tidak semua perangkat atau layanan Gen-AI memberikan script Python atau R dalam respons mereka, sebagai bentuk pertanggungjawaban dan transparansi kepada pengguna. ChatGPT dan JuliusAI termasuk yang unggul untuk hal ini.



```

Analysis
python

import matplotlib.pyplot as plt

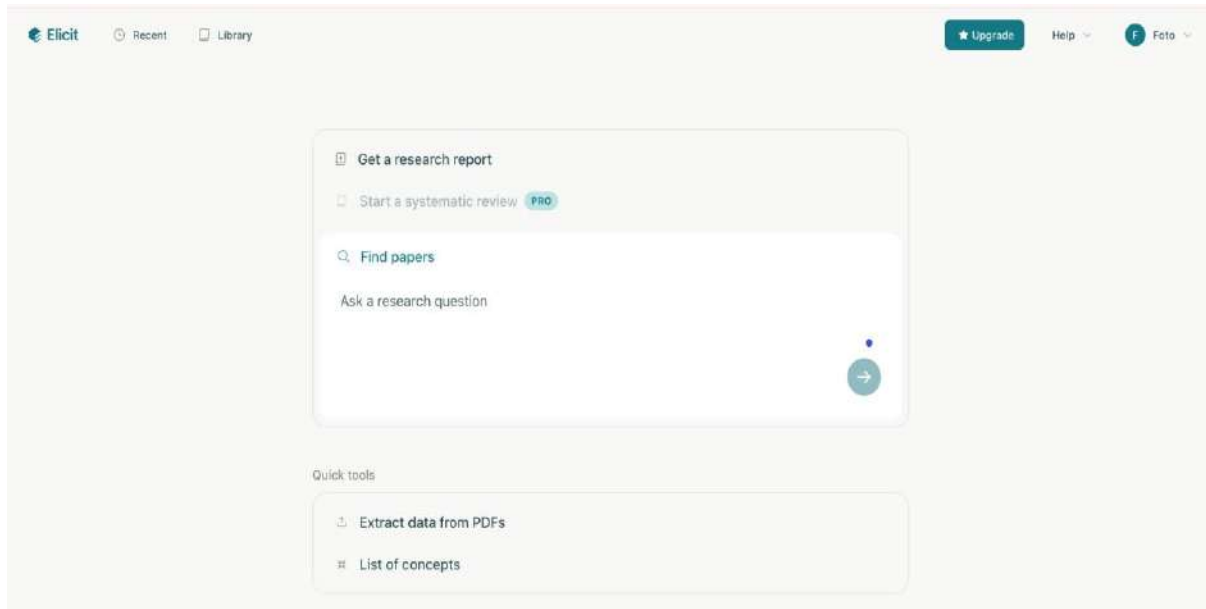
# Calculate the average salary in USD by experience level
avg_salary_by_experience = df.groupby("experience_level")["salary_usd"].mean()

# Create the bar chart
plt.figure(figsize=(8, 5))
avg_salary_by_experience.plot(kind="bar")

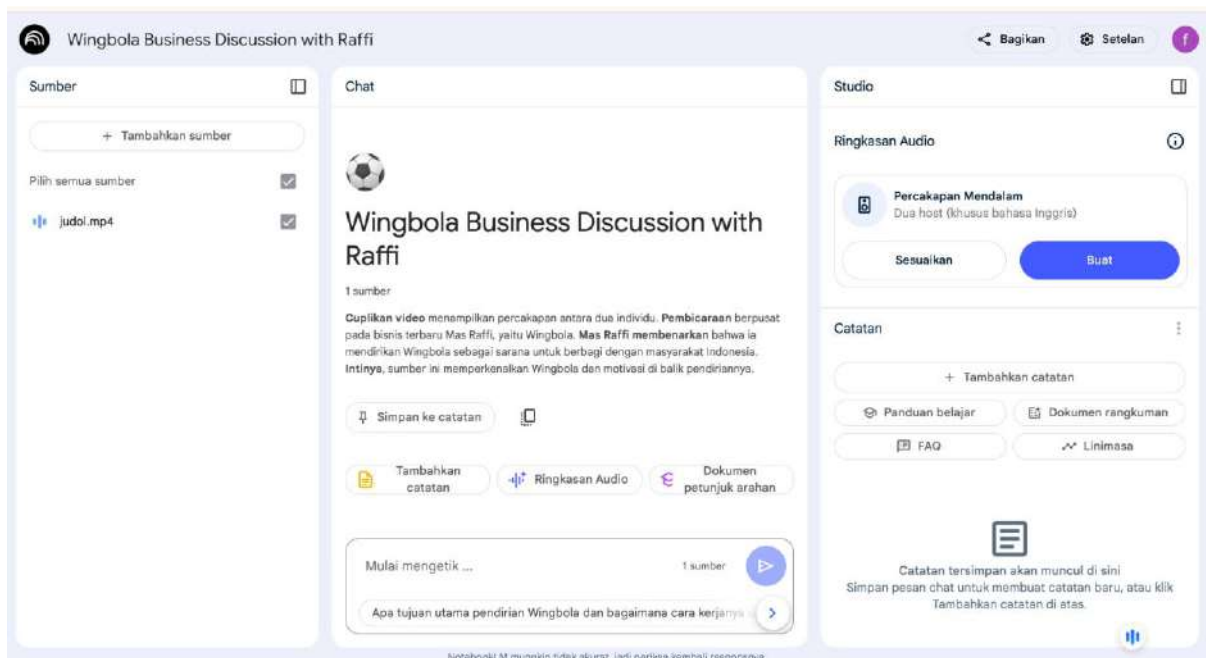
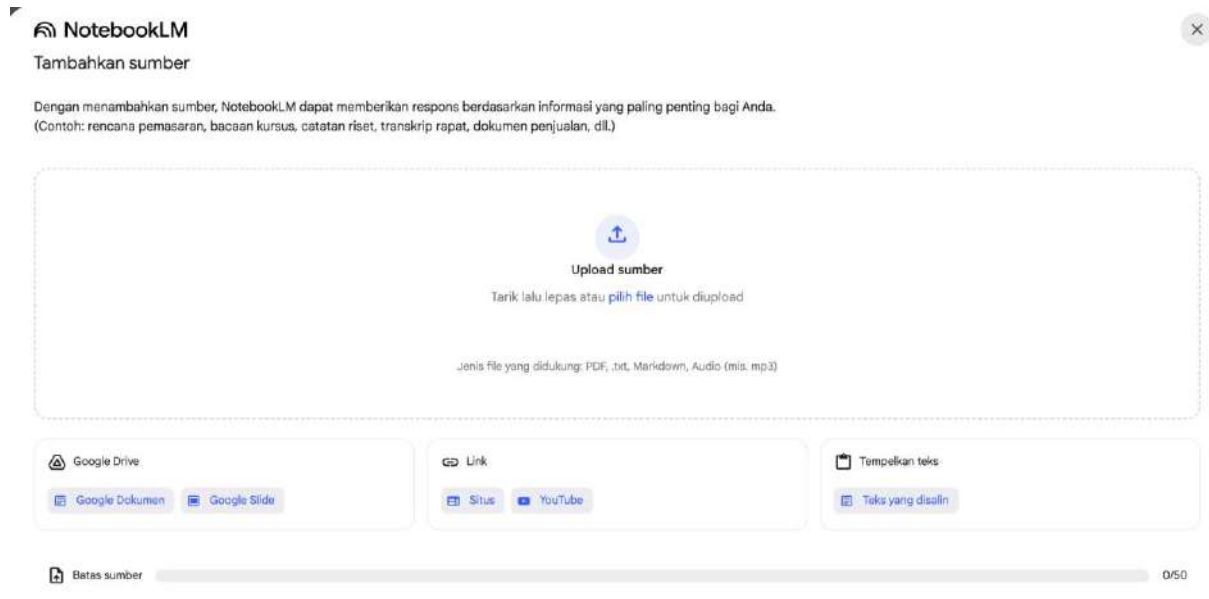
# Formatting the chart
plt.xlabel("Experience Level")
plt.ylabel("Average Salary (USD)")
plt.title("Average Salary by Experience Level")
plt.xticks(rotation=0)
plt.grid(axis="y", linestyle="—", alpha=0.7)

# Show the chart
plt.show()
    
```

Perangkat lain yang dapat membantu proses riset adalah Elicit, yaitu untuk mendapatkan ringkasan dari jurnal atau artikel.



Ada pula Notebook LM. Perangkat ini mengizinkan kita untuk mengunggah audio, mentranskrip, bahkan mengubahnya ke dalam bentuk seakan-akan percakapan antara dua orang yang membahas isu tersebut. Notebook LM juga sangat membantu pengguna untuk mengambil intisari dari dokumen yang diunggah. Namun kita tidak bisa memasukkan data dalam format Excel atau CSV untuk dianalisis. Di bagian kanan bawah, Notebook LM mampu memberikan rekomendasi hasil *output* yang kita inginkan dari sumber yang kita unggah. Misal, lini masa, rangkuman dokumen, panduan belajar, atau *Frequently Asked Question* (FAQ).



Di akhir sesi, kita dapat mengajak peserta untuk melakukan latihan *prompting* menggunakan dataset [dummy](#) soal gaji pekerja di sektor Data Science yang didapat dari Kaggle.

Berikut panduan untuk sesi praktik:

1. Unduh data gaji pekerja di sektor Data Science.
2. Buka satu akses perangkat dan bebaskan untuk memilih, apakah ChatGPT, JuliusAI, Copilot, atau NotebookLM.

3. Buat *prompt* untuk analisis gaji pekerja di sektor Data Science. Prompt yang digunakan bebas.
 - Buat satu kolom tambahan. Kategorisasikan pekerjaan berdasarkan: Scientist, Engineer, Analyst, Manager, Lead.
 - Cari pekerjaan dengan gaji paling tinggi selama 2024 yang bisa dilakukan dengan remote (full) dan cari tahu di mana saja mereka tinggal?
 - Berapa banyak yang berada di posisi level senior?
 - Bidang apa saja yang mereka geluti (berdasarkan kategorisasi yang sudah dilakukan sebelumnya)?
 - Dari seluruh entries, cari pekerjaan dengan gaji tertinggi untuk setiap negara tempat tinggal pekerja.
 - Cari perusahaan yang menggaji karyawan paling tinggi di tiap level (experience level) hanya untuk data tahun 2024.
4. Proses analisis ini harus dilakukan mandiri oleh masing-masing peserta.
5. Hasil analisis disimpan dalam bentuk CSV.
6. Setelah analisis, mari kita diskusi bersama soal akurasi masing-masing perangkat.



**ALIANSI
JURNALIS
INDEPENDEN**
Alliance of Independent Journalist

BAB IV.

KEAMANAN DIGITAL DI ERA ARTIFICIAL INTELLIGENCE

BAB IV. KEAMANAN DIGITAL DI ERA ARTIFICIAL INTELLIGENCE

Tujuan: Peserta diharapkan memahami pentingnya keamanan digital serta mempraktikkan langkah-langkah mitigasi bahaya saat beraktivitas menggunakan internet. Terlebih saat memanfaatkan teknologi AI.

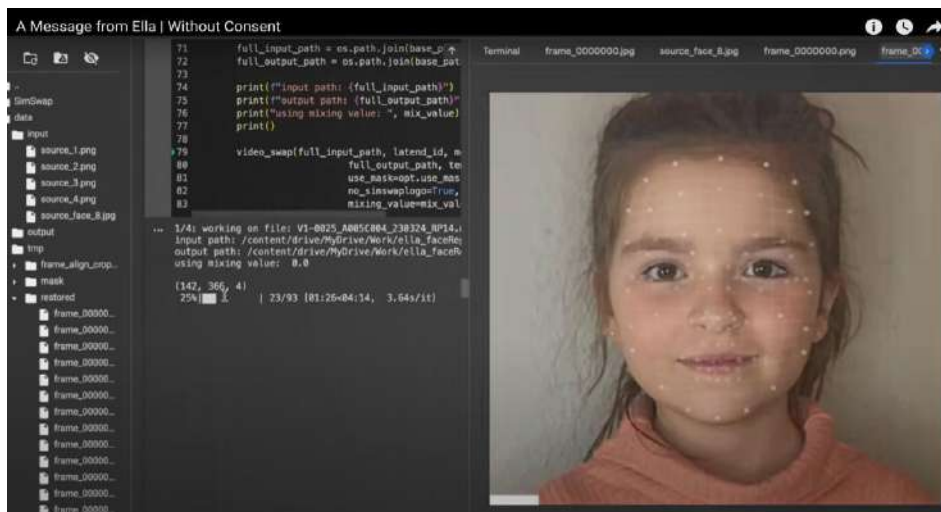
Pertanyaan pemantik:

1. Apakah selama berinternet, kita aman?
2. Apakah selama berinternet, kita menjadi konsumen atau produk dari sebuah platform?
3. Apakah kita pernah membaca secara detil syarat dan ketentuan pada sebuah platform sebelum menggunakannya?
4. Siapa dan bagaimana mereka memanfaatkan data kita sebagai pengguna?
5. Apakah ada jaminan keamanan bahwa data dan prompt yang kita gunakan pada layanan AI tidak akan digunakan oleh penyedia AI?

Metode penyampaian:

- Ceramah
- Praktik
- Diskusi

Sebelum masuk dalam modul, ada baiknya kita menyimak dulu video pendek yang tersedia pada tautan ini: [A Message from Ella](#).



Setelah menonton video pendek tersebut, pelatih dapat membuka sesi diskusi untuk mengetahui pendapat peserta. Mulai dari refleksi mereka soal pesan dari video atau kerentanan apa saja yang muncul akibat perkembangan teknologi AI.

Perkembangan teknologi dan informasi yang begitu pesat membawa perubahan signifikan dalam berbagai aspek kehidupan manusia. Kondisi ini memberikan beragam kemudahan untuk kita beraktivitas, berinteraksi sosial, mempermudah proses kerja, mengekspresikan diri, hingga mencari hiburan.

Berbarengan dengan itu, ada juga beragam tantangan, termasuk di dalamnya kejahatan digital seperti penipuan daring, pencurian data, perisakan daring, hingga kekerasan daring atau fisik. Untuk menghadapi tantangan tersebut, penting bagi pengguna internet memiliki pengetahuan dasar soal keamanan digital.

Keamanan digital ini merupakan disiplin multidimensi guna melindungi aset digital, data, serta sistem informasi dari akses tidak dikenal, penyerangan, pengungkapan, atau penghancuran yang tidak sah. Secara sederhana, keamanan digital adalah upaya memahami dan memitigasi segala jenis serangan yang memanfaatkan teknologi digital, baik langsung maupun tidak langsung.

Keamanan digital ini terkait dengan dua jenis keamanan lainnya, yaitu keamanan fisik dan keamanan psikososial. Ini yang biasa disebut dengan konsep keamanan holistik atau keamanan menyeluruh. Modul ini hanya akan membahas keamanan digital, karena serangan jenis ini bisa berdampak pada keamanan fisik dan keamanan psikososial.

Cakupan keamanan digital spektrumnya luas, tidak terbatas, mulai dari langkah-langkah teknis, prosedural, hingga strategis. Secara teknis, ada tiga hal yang saling terkait dalam langkah pengamanan digital, yaitu teknologi, kebijakan, dan manusia.

Panduan ini akan lebih fokus pada aspek manusia. Sebab, seringkali perilaku di dunia sehari-hari dan dunia digital yang justru menjadi titik masuk terjadinya serangan digital.

4.1. Prinsip Keamanan Digital

Tidak ada jaminan 100 persen aman.

Dalam interaksi digital, tidak pernah ada jaminan 100 persen aman. Ilustrasi sederhana, aplikasi PeduliLindungi yang digunakan pemerintah saat pandemi COVID-19 sudah berganti menjadi aplikasi SATUSEHAT. Terkait pergantian aplikasi tersebut, publik atau penggunanya tidak mendapatkan pertanyaan untuk konfirmasi pemanfaatan data pada aplikasi yang berbeda. Selain itu, jika kita memeriksa informasi keamanan data, disebutkan developer atau pengembangnya tidak menyediakan informasi perihal penghapusan data pengguna.

Keamanan berbanding terbalik dengan kenyamanan.

Teknologi hadir untuk menawarkan beragam kemudahan bagi penggunanya. Dalam konteks keamanan digital, beragam kemudahan itu malah bisa jadi celah masuknya ancaman. Setiap kita membuka aplikasi yang membutuhkan akses masuk seperti penulisan akun dan password, maka ada layanan yang menawarkan fitur pengingat masuk ke akun tersebut tanpa Anda repot-repot menulis lagi nama akun dan password berikutnya. Seandainya Anda mengakses layanan tersebut dari komputer kantor atau laptop yang ditinggalkan terbuka di meja kerja, bisa jadi ada pihak lain yang dapat mengakses layanan yang pernah Anda buka tanpa harus repot mengetahui nama akun dan password-nya.

Keamanan digital berhubungan erat dengan perilaku.

Praktik keamanan digital tidak melulu berkaitan dengan penggunaan teknologi atau infrastruktur. Salah satu yang kerap diabaikan adalah perilaku saat berinternet. Saat Anda memiliki banyak akun media sosial dan kesulitan mengingat password, maka Anda membuat password yang sama untuk semua akun. Risiko terjadinya kebocoran data pada platform tidak pernah bisa kita ketahui pasti. Membedakan dan mengganti password akun setiap enam bulan merupakan cara aman dan sangat mudah dilakukan.

Personal dan kontekstual.

Setiap orang memiliki standar berbeda-beda terkait keamanan digital. Alasannya, kepentingan setiap orang tidak sama saat memanfaatkan internet atau teknologi digital. Seorang jurnalis investigasi yang melakukan peliputan ke wilayah rawan, biasa mematikan GPS karena itu akan

membuatnya dapat ditandai lokasinya. Namun bagi seorang konsumen transportasi daring, mematikan lokasi bakal membuatnya kesulitan mengakses layanan.

Mencegah lebih baik daripada memulihkan.

Setiap penyedia layanan media sosial memiliki fitur pemulihan akun apabila penggunaannya mengalami peretasan. Namun tidak ada platform yang memberikan jaminan apakah korban peretasan dapat Kembali menguasai akunnya dalam durasi waktu tertentu. Nasib pemilik akun yang kena retas sepenuhnya berada di tangan platform, meski bukan tidak mungkin penggunaannya meminta bantuan pihak ketiga yang terpercaya. Berkaca dari fakta tersebut, sebaiknya pemilik akun atau pengguna media sosial selalu memitigasi dan mengurangi risiko terjadinya peretasan.

Kekerasan digital bisa jadi pintu masuk kekerasan fisik dan psikososial.

Kehadiran media sosial membuat semua orang dapat membagikan informasi apa saja kepada siapa saja dan kapan saja. Namun banyak pihak yang tidak menyadari bahwa kebiasaan membagi informasi, terutama terkait kehidupan pribadi, dapat menjadi celah masuknya ancaman digital. Termasuk di dalamnya dengan penggunaan teknologi AI. Ingat kembali video pendek tentang Ella.

Ancaman itu mulai dari pemanfaatan foto atau video pribadi untuk kepentingan impersonasi atau peniruan sebagai langkah awal melakukan penipuan daring. Apabila ini terjadi, warganet yang merasa tertipu dapat membongkar informasi pribadi, termasuk alamat rumah dan hubungan sosial orang yang ditiru, oleh penipu. Korban penipuan selanjutnya dapat mengunjungi dan melakukan tindakan merugikan terhadap orang yang ditiru informasinya.

Dalam melakukan mitigasi keamanan digital, kita perlu mengetahui karakter serangan digital. Berikut adalah karakter dari serangan digital:

- Pelakunya bisa melakukan serangan dari mana saja.
- Modus serangannya beragam.
- Serangan bisa terjadi kapan saja, tidak mengenal batas waktu.
- Dampak serangan sulit diukur.
- Bentuk serangan sangat beragam.
- Semakin tidak terlihat serangannya, bisa jadi makin berbahaya.

Secara umum, serangan digital terbagi menjadi dua jenis:

- Serangan teknis: membutuhkan kemampuan teknis dan kerap kali tidak disadari.
- Serangan psikologis atau non-teknis: tidak membutuhkan kemampuan teknis untuk menyasar mental korbannya.

4.2. Bentuk-bentuk dari serangan teknis:

Ada sejumlah serangan yang masuk dalam kategori ini. Bentuknya bisa berupa malware, spyware, phishing, spear phishing, peretasan, Ddos Attack dan penyadapan.

4.2.1. Malware

Malware (malicious software) adalah istilah untuk perangkat lunak khusus yang dibuat dengan tujuan 'mengganggu' sistem komputer milik orang lain. Serangan malware dapat terjadi pada perangkat digital seperti CPU, laptop, handphone, dan tablet.

Selain menyerang atau merusak file, perangkat lunak tersebut juga dapat menduplikasi diri hingga merusak sistem kerja hard disc dan perangkat lunak, mengambil data, hingga merusak sistem operasi pada perangkat digital sasaran.

Malware bisa berupa perangkat lunak atau kode yang bekerja dengan persetujuan atau tanpa persetujuan pengguna perangkat digital. Malware yang sangat merusak juga dapat mematikan antivirus yang terpasang pada sistem komputer.

Ada beberapa contoh bentuk malware, antara lain trojan, worm, dan virus. Cara kerjanya berbeda-beda. Ada yang mengumpulkan informasi dari perangkat digital sasaran, mengakses dokumen tanpa izin, menduplikasi data, atau menyerang jaringan internet sasaran.

4.2.2. Spyware

Seperti namanya yang menggunakan 'spy', perangkat lunak ini bekerja untuk memata-matai. Secara umum, perangkat lunak ini dibuat untuk mengumpulkan data dengan memata-matai perangkat digital. Data ini nantinya akan dikirimkan ke pihak yang menanamkannya tanpa sepengetahuan target serangan.

Data yang bisa diambil beragam, mulai dari kata sandi, PIN, nomor identitas yang tersematkan dalam salah satu atau lebih aplikasi, memantau kebiasaan target serangan saat berinternet, hingga pergerakan target serangan lewat GPS pada perangkat.

Perangkat lunak ini bekerja dengan cara ‘menempel’ pada perangkat lunak lain yang diunduh atau dipasang oleh korban. Seperti malware, proses penyusupan perangkat lunak ini juga bisa melalui situs tertentu atau surat elektronik yang diakses korban.

4.2.3. Phishing

Merupakan tindakan rekayasa sosial yang untuk menipu orang lain di dunia digital. Penipuan ini kerap hadir melalui penyebaran pesan (surat elektronik, aplikasi percakapan, unggahan media sosial) guna menciptakan kondisi darurat, keingintahuan, hingga ketakutan pada korbannya. Penyerang bakal memainkan kondisi psikologis korban agar mengungkapkan informasi sensitif, mengetuk tautan tertentu, atau membuka lampiran yang berisi malware.

4.2.4. Spear phishing

Jenis serangan ini merupakan versi lain dari teknik penipuan phishing yang lebih kompleks dan terstruktur. Penyerang biasanya sudah menarget sasaran atau perusahaan tertentu. Mereka akan menyesuaikan pesan manipulatif berdasarkan karakter, posisi pekerjaan, atau kontak milik korban agar serangannya tidak terdeteksi dan mencolok.

4.2.5. Peretasan

Serangan ini bisa terjadi pada individu atau lembaga. Pada individu, penyerang berupaya menguasai akun media sosial atau identitas digital seseorang untuk keperluan pemerasan atau rekayasa sosial seperti penipuan mengatasnamakan korban. Sementara serangan pada lembaga, biasanya terjadi pada laman-laman resmi milik institusi dengan tujuan beragam, mulai dari mendapatkan uang hingga menjatuhkan kredibilitas atau reputasi lembaga.

4.2.6. DDoS Attack

DDoS merupakan singkatan dari distributed denial-of-service. Serangan DDoS merupakan jenis serangan yang memanfaatkan pengiriman paket permintaan data yang sangat besar pada suatu sistem pada saat bersamaan hingga mengakibatkan sistemnya kewalahan dan tidak dapat diakses. Pada level individu, jenis serangan ini juga dapat terjadi dengan cara membanjiri

komentar pada salah satu akun media sosial dalam waktu bersamaan sehingga terjadi anomali data, yang berdampak pada sulitnya akun tersebut untuk diakses.

4.2.7. Penyadapan

Upaya pemantauan aktivitas target secara ilegal dan tidak diketahui korban.

4.3. Bentuk-bentuk Serangan non-Teknis

4.3.1. Doxxing

Upaya mengungkapkan data-data pribadi target serangan dengan tujuan merusak nama baik atau menjatuhkan kredibilitas.

4.3.2. Ujaran Kebencian

Adalah segala jenis komunikasi dalam ucapan, tulisan, atau perilaku di internet yang menyerang atau menggunakan bahasa yang merendahkan, diskriminatif, atau yang menimbulkan rasa kebencian atau permusuhan yang mengacu pada seseorang atau kelompok berdasarkan atas suku, agama, ras, dan antar golongan.

4.3.3. Persekusi daring

Pelaporan massal pada sebuah akun sehingga hilang atau ditangguhkan oleh platform.

4.3.4. Impersonasi

Pembuatan akun tiruan target serangan yang mengunggah hal-hal bertentangan dengan kampanye atau sikap target serangan.

4.3.5. Kriminalisasi

Upaya pemidanaan kepada warganet dengan menggunakan pasal-pasal karet di Undang-Undang Informasi dan Transaksi Elektronik atau peraturan lainnya berdasarkan unggahan di internet.

4.4. Mengapa bisa terjadi serangan digital

Serangan digital dapat terjadi karena saat ini akses internet yang tidak terbatas. Ada banyak alasan yang jadi motif penyerangan. Secara umum motif pelaku melakukan serangan antara lain karena ketidaknyamanan atas unggahan atau komentar seseorang, ada motif mendapatkan keuntungan, hingga keinginan untuk menjatuhkan reputasi dan kredibilitas seseorang.

Sebagai pengguna aneka layanan di internet, kita juga bisa memanfaatkan fasilitas pemeriksaan soal kemungkinan terjadinya kebocoran data lewat tautan [periksadata](https://periksadata.com).

Layanan ini memanfaatkan data dari layanan serupa yang bisa dicek pada tautan ini [HaveiBeenPwned](https://haveibeenpwned.com) agar publik dapat memeriksa secara berkala, apakah menjadi korban kebocoran data atau tidak?







Layanan Periksa Data ini dikembangkan oleh individu pegiat keamanan siber, praktisi hukum, serta pegiat perlindungan data juga memberikan informasi perihal langkah-langkah yang dapat Anda tempuh paska mendapati informasi kebocoran data. Silahkan akses tautan [periksadata](https://periksadata.com) yang tangkapan layarnya seperti di bawah ini:

Silahkan masukkan alamat surat elektronik yang paling sering Anda gunakan untuk beragam keperluan, seperti mengakses layanan atau media sosial. Hasilnya dapat terlihat setelah Anda menyetuk opsi “PERIKSA SEKARANG” di bagian bawah kotak berwarna merah.

Jika alamat email yang Anda masukkan pernah bocor (tentu saja Anda tidak perlu terlalu panik), maka akan tampil tulisan sebagai berikut:

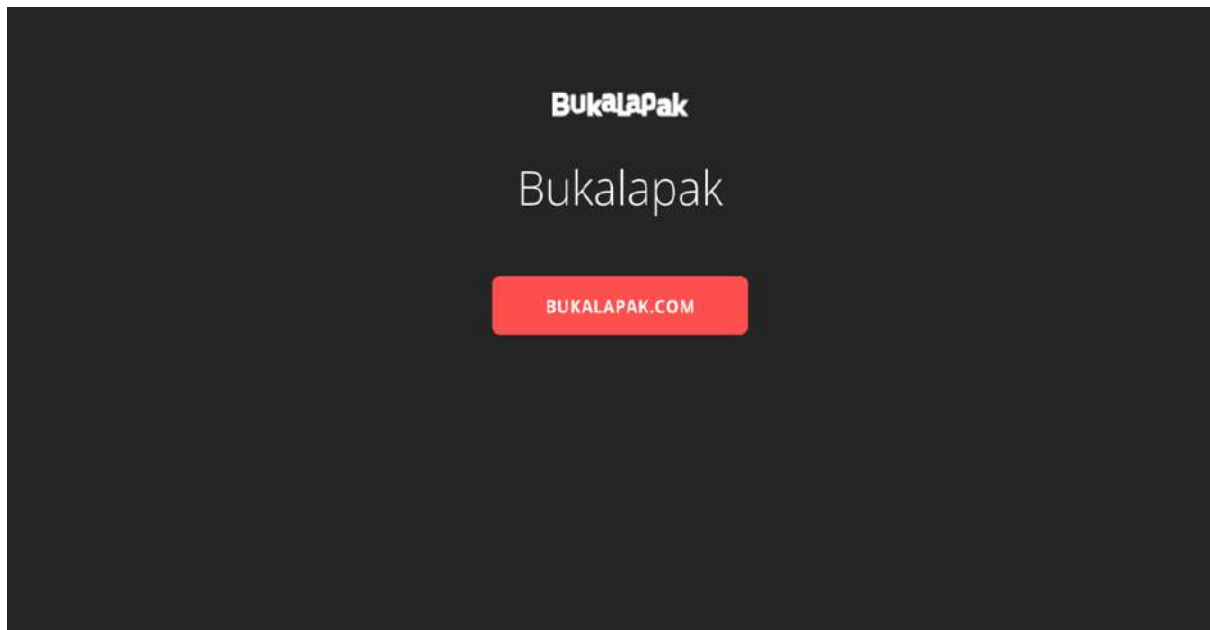
“(alamat surat elektronik yang tadi dimasukkan) telah menjadi korban ...(jumlah kejadian) peristiwa kebocoran data”.

Untuk mengetahui kebocorannya di mana saja, Anda bisa menggulirkan tetikus atau layar ke bawah hingga terlihat informasi seperti di bawah ini:

 <p>Bukalapak Tanggal kejadian 23 Oktober 2017 Data yang bocor Email, Alamat IP, Nama Lengkap dll Total keseluruhan data yang bocor 13,369,666 Selengkapnya »</p>	 <p>Canva Tanggal kejadian 24 Mei 2019 Data yang bocor Email, Lokasi geografis, Nama Lengkap dll Total keseluruhan data yang bocor 137,272,116 Selengkapnya »</p>
 <p>Tokopedia Tanggal kejadian 17 April 2020 Data yang bocor Tanggal lahir, Email, Jenis kelamin dll Total keseluruhan data yang bocor 71,443,698 Selengkapnya »</p>	 <p>ShopBack Tanggal kejadian 17 September 2020 Data yang bocor Email, Lokasi geografis, Nama Lengkap dll Total keseluruhan data yang bocor 20,529,819 Selengkapnya »</p>
 <p>Gravatar Tanggal kejadian 03 Oktober 2020 Data yang bocor Email, Nama Lengkap, Username dll Total keseluruhan data yang bocor 113,990,759 Selengkapnya »</p>	 <p>Naz API Tanggal kejadian 20 September 2023 Data yang bocor Email, Password, dll Total keseluruhan data yang bocor 70,840,771 Selengkapnya »</p>

Silahkan Anda catat satu persatu layanan yang terkoneksi dengan alamat surat elektronik yang tadi dimasukkan. Sekali lagi, tidak perlu panik. Dengan melakukan pencatatan, Anda sudah selangkah menuju mitigasi. Ingat, kebocoran itu tidak hanya menimpa Anda tapi juga jutaan pengguna lainnya.

Untuk mengetahui lebih lanjut informasi terkait kebocoran tersebut, Anda bisa mengetuk “Selengkapnya” pada setiap layanan yang muncul di layar yang salah satu contohnya seperti di bawah ini:



PENJELASAN SINGKAT

Pada 23 Oktober 2017, Bukalapak mengalami kejadian kebocoran data. Total keseluruhan data pengguna yang bocor adalah 13,369,666 data. Sekumpulan data yang bocor tersebut kemudian ditambahkan pada 18 April 2019.

DATA YANG BOCOR



UPDATE TERAKHIR

18 April 2019

Perhatikan informasi terkait kapan kejadian kebocoran itu terjadi serta data apa saja yang bocor. Dalam tangkapan layar terlihat kebocoran pada salah satu platform belanja daring meliputi alamat surat elektronik, alamat *internet protocol* (IP), nama lengkap, password, hingga nama pengguna pada layanan tersebut.

Gulirkan tetikus atau layar ke bagian bawah hingga mendapatkan tampilan seperti di bawah ini:

JIKA DATA KAMU BOCOR

Ini yang harus kamu lakukan jika kamu telah menjadi korban kebocoran data.



Segera ganti password yang kamu gunakan. Agar lebih aman, gunakan kombinasi huruf, angka dan symbol di password yang kamu gunakan.

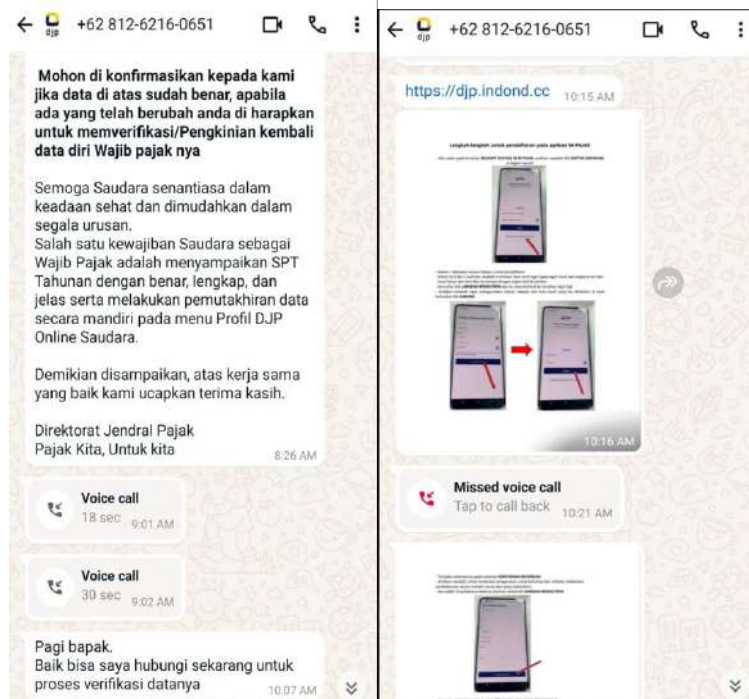


Aktifkan verifikasi 2 langkah sekarang agar akun milik kamu menjadi lebih aman. Disarankan untuk menggunakan Authenticator App daripada sms.



Jika kamu merasa kesulitan untuk mengingat banyak password, kamu bisa menggunakan password manager untuk menyimpan banyak password.

Tindakan mengecek dan memastikan apakah ada kebocoran data yang terkait dengan data kita merupakan langkah untuk mitigasi, mencegah terjadinya kerugian yang lebih besar. Misalnya saja ada kebocoran data terkait pajak yang kemudian dimanfaatkan untuk melakukan penipuan terhadap wajib pajak seperti pada tampilan layar yang didapat dari media sosial di bawah ini:

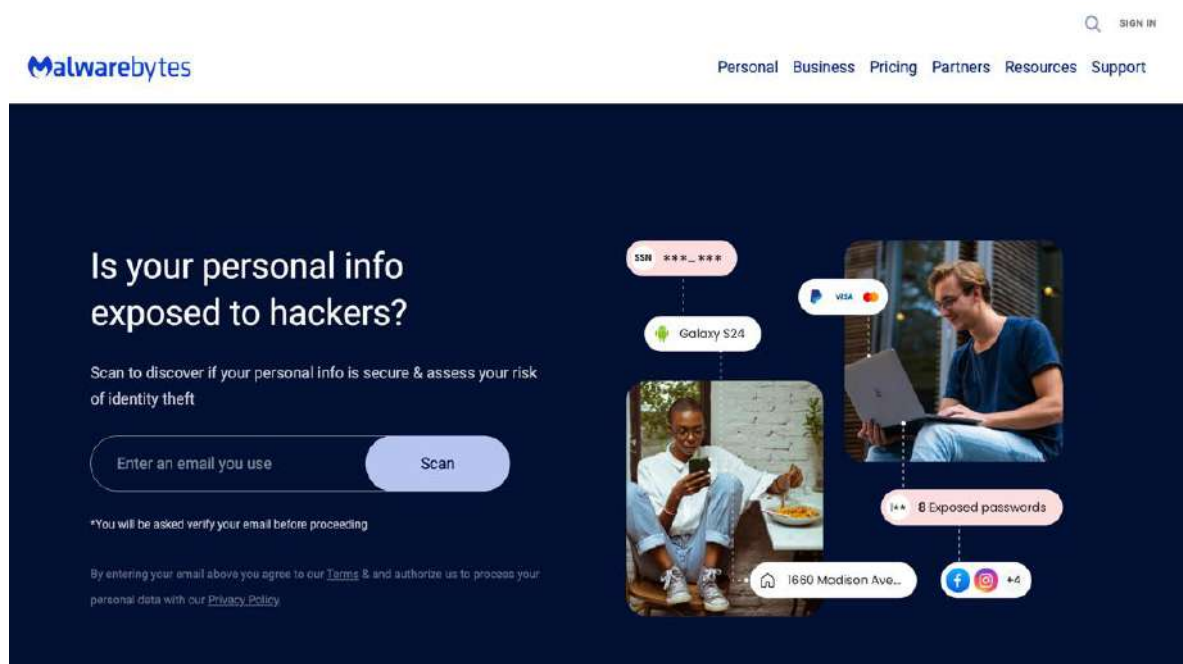


Pada tangkapan layar kiri percakapan dipotong karena pada bagian atasnya menampilkan data pribadi yang terdiri dari nama lengkap, alamat, alamat surat elektronik, nomor kontak, nomor pokok wajib pajak, nama perusahaan, hingga nomor induk berusaha, dan nomor pajak perusahaan.

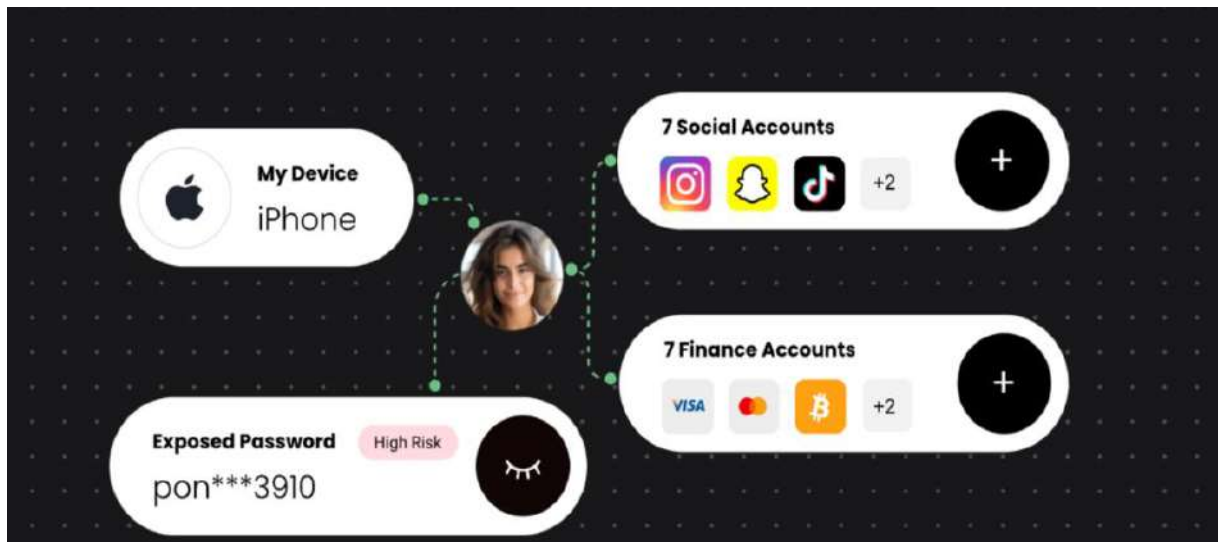
Penipu berupaya memperdaya wajib pajak untuk menyetujui tautan yang mereka sediakan, namun sebenarnya tautan itu mengandung malware.

Prinsip mitigasi seperti selalu menjaga dan memastikan sebaran data di internet dapat membantu agar kita tidak menjadi sasaran serangan digital. Salah satu cara lain untuk mengecek sejauh mana kebocoran data kita, bisa dengan mengakses layanan pemeriksaan kebocoran data dari [Malwarebytes](#) —perusahaan keamanan siber asal Amerika Serikat yang fokus mengembangkan piranti lunak bagi pengguna internet, telepon pintar dari malware dan ancaman digital lainnya.

Untuk mengakses layanan [Malwarebytes](#), Anda harus memasukkan alamat surat elektronik yang dapat Anda akses. Karena mereka akan mengirimkan kode otentifikasi ke alamat surat elektronik guna memastikan Anda adalah alamat pemilik surat elektronik tersebut. Tampilan mukanya akan terlihat seperti di bawah ini:



Setelah memasukkan alamat surat elektronik ke dalam kolom, tekan Scan di bagian kanannya. Setelah itu Anda perlu membuka alamat surat elektronik dan memasukkan enam angka yang mereka kirimkan. Nantinya, Anda akan melihat tampilan alamat surat elektronik itu terkoneksi pada asset-aset digital hingga nomor telepon dan password (jika memang bocor), seperti di bawah ini:



Sama seperti hasil pemeriksaan Periksa Data di bagian awal, Anda tidak perlu panik. Anda sebaiknya segera memastikan apakah seluruh layanan media sosial itu masih dipakai atau tidak. Jika tidak lagi dipakai, segera tutup akunnya. Atau ganti password-nya jika memang sudah pernah bocor. Periksa juga aset digital lain dan perkuat keamanannya.

Untuk mitigasi keamanan yang lebih detil, Anda juga dapat memanfaatkan layanan yang dikembangkan SAFEnet (Southeast Asia Freedom of Expression Network)— organisasi nirlaba yang memperjuangkan hak-hak digital termasuk hak mengakses internet, kebebasan berekspresi, dan hak atas rasa aman di ranah digital—pada tautan [PAKEM DIRI](#).



Layanan ini dapat digunakan publik secara cuma-cuma untuk menilai seberapa tinggi risiko keamanan digitalnya. Ada empat penilaian di aplikasi itu yang tampilannya seperti ini:

Petunjuk Pengisian

Panduan Menilai Keamanan Digital Mandiri

1. Silakan memilih salah satu bagian yang ingin Anda nilai. Anda bisa memilih salah satu atau semua bagian yang ingin Anda nilai.
2. Setelah memilih Anda akan berada di laman pemeriksaan.
3. Periksalah pengaturan keamanan pada perangkat laptop dan ponsel yang Anda gunakan sehari-hari. Jika Anda lakukan, pilih "Ya". Jika tidak Anda lakukan, pilih "Tidak".



Perangkat



Identitas



Komunikasi



Ponsel

Pada setiap opsi penilaian mandiri ini, Anda akan memilih antara jawaban YA dan TIDAK sesuai dengan praktik keseharian Anda. Sebaiknya, setiap pilihan TIDAK perlu dicatat pernyataannya sehingga Anda mengetahui perilaku apa yang sebaiknya diperbaiki guna mengurangi risiko keamanan digital Anda.

Pada setiap bagian akhir pengisian, akan muncul penilaian seperti di bawah ini:

Pemeriksaan Keamanan Perangkat

Periksalah pengaturan keamanan pada perangkat laptop dan ponsel yang Anda gunakan sehari-hari.

- | | |
|--|--|
| Memisahkan laptop untuk bekerja dan pribadi * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Memisahkan ponsel untuk bekerja dan pribadi * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Menggunakan sistem operasi (OS) orisinal, bukan bajakan * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Menggunakan kata sandi untuk membuka perangkat * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Mengaktifkan firewall * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Melakukan enkripsi media penyimpanan * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Mematikan fungsi lokasi pada laptop * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Mematikan fungsi lokasi pada ponsel kecuali diperlukan * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Melakukan pencadangan (back up) secara berkala, setidaknya sebulan sekali * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Membersihkan berkas dan aplikasi yang sudah tidak digunakan secara berkala * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Menggunakan antivirus dan pembersih (cleaner) * | <input type="radio"/> Ya <input type="radio"/> Tidak |
| Memperbarui (update) sistem operasi dan aplikasi jika ada pembaruan * | <input type="radio"/> Ya <input type="radio"/> Tidak |

Periksa



Setiap penilaian yang keluar akan disertai informasi tingkat risikonya. Cara untuk mengurangi risiko tersebut adalah dengan mengubah perilaku Anda agar penilaiannya jadi warna hijau, yang itu artinya tingkat risiko Anda rendah. Misalnya, jika sebelumnya Anda belum memisahkan akun pekerjaan dengan akun pribadi, maka ke depannya Anda perlu memisahkannya.

Salah satu masalah dalam upaya mitigasi risiko keamanan digital adalah ketidakmampuan pengguna internet mengidentifikasi aset-aset digitalnya. Sebagai ilustrasi, banyak aplikasi yang mewajibkan kita sebagai pengguna untuk menggunakan alamat surat elektronik. Namun seiring berjalannya waktu kita seringkali lupa alamat surat elektronik mana yang kita gunakan untuk keperluan aplikasi 1, aplikasi 2, dan aplikasi lainnya.

Untuk membantu proses identifikasi aset digital, Anda bisa mengakses dokumen pada tautan [manajemen aset digital](#) dan kemudian menduplikasinya untuk kebutuhan luring. Kenapa luring? Karena di dalam formulir aset digital ini nantinya akan ada kolom yang berisi kata sandi atau *password*.

	A	B	C	D	E	F	G	H
1	MANAJEMEN ASET DIGITAL							
2	Jenis	Layanan	Peruntukan	ID	Sandi	Terkait dengan	Authenticator-2FA	Catatan
3	Email 1 (contoh)	Gmail	Kerja	ajiindonesia@gmail.com	#Maju.JayaAbadi1994!	Handphone nomor 08112233445, akun aji yahoo, akun traveloka, Twitter @jemetabadi	2FA + Google Authenticator	
4	Email 2							
5	Medsos 1 (contoh)	Twitter	Pribadi	jemetabadi	JayaAbadi_1994!	akun ajiindonesia@gmail.com, HP 08112233445	2FA + Google Authenticator	
6	Medsos 2							
7	Aplikasi 1 (contoh)	Traveloka	Pribadi	ajiindonesia@gmail.com	MapayJalanSatapakNgajugjugKaiHijilLembur	akun ajiindonesia@gmail.com, HP 08112233445	2FA	
8								

Penggunaan formulir ini akan sangat membantu Anda mengidentifikasi aset digital apa saja yang anda miliki. Pada kolom A (jenis) dapat diisi dengan jenis layanan, mulai dari surat elektronik, aplikasi, hingga media sosial yang Anda miliki atau gunakan.

Cara mengisinya dimulai dari kolom JENIS yang kemudian secara detail dilanjutkan pada kolom B (LAYANAN), kolom C (PERUNTUKKAN) dari aset digital itu, apakah untuk kebutuhan pekerjaan/pribadi/belanja/permainan daring/keuangan, dan lainnya. Pada kolom D (ID), Anda bisa mengisi secara lengkap seperti alamat detail surat elektronik, nama akun pada media sosial dan aplikasi.

Pada kolom E (SANDI), Anda akan mengisi setiap *password* atau kata kunci yang dipergunakan. Dengan mengisi kolom E, Anda akan mengetahui apakah satu kata kunci digunakan untuk kebutuhan media sosial atau aplikasi lainnya. Guna memitigasi kebocoran, sebaiknya Anda memiliki kata sandi berbeda dari setiap media sosial atau aplikasi.

Pencantuman kata sandi ini penting agar Anda dapat memiliki pegangan saat ada peretasan dan orang yang mengambil alih akun mengganti kata sandi Anda. Biasanya layanan di internet akan meminta Anda untuk memasukkan kata sandi terdahulu sebagai penanda bahwa memang benar Anda pemilik akun yang sah.

Pengisian kolom F (TERKAIT DENGAN) juga tidak kalah penting. Seperti saat melakukan percobaan dengan mengisi surat elektronik di PERIKSA DATA atau MALWAREBYTES, bisa diketahui koneksi dari satu alamat surat elektronik ke berbagai layanan. Jika kedua layanan itu dapat mengidentifikasi jaringan dari surat elektronik Anda, ada peluang sangat besar peretas juga dapat melakukannya dan berupaya mengambil alih akun Anda yang lain jika salah satu akun sudah diretas.

Jika Anda bingung mengisi kolom F ini, Anda tinggal membuka telepon pintar dan mengecek ada aplikasi atau media sosial apa saja di telepon tersebut. Maka seluruh aplikasi dan media sosial tersebut dipastikan terkait dengan nomor telepon atau alamat surat elektronik yang Anda gunakan di telepon tersebut.

Sementara untuk kolom G (Authenticator/2FA) diisi apabila aplikasi atau media sosial Anda sudah dilapisi otentifikasi dua faktor. Ada beberapa aplikasi di internet yang bisa Anda pilih, seperti [Authy](#) atau [2FAS](#) yang memanfaatkan sumber terbuka atau *open source*.

Terkait dengan pembuatan kata sandi, Anda dapat memanfaatkan layanan dari [PasswordMonster](#), layanan pemeriksaan kekuatan *password*/kata kunci yang dikembangkan My1Login, perusahaan penyedia layanan keamanan siber asal Inggris yang terikat pada aturan General Data Protection Regulation di Uni Eropa.

Sebelum menggunakan layanan ini, Anda perlu memahami hasil yang muncul terkait dengan kapasitas dan kemampuan komputer pada saat Anda menggunakannya. Karena ada satu prinsip keamanan digital yang tidak boleh Anda lupakan: aman hari ini, tapi besok belum tentu. Jadi mitigasi dengan mengganti kata kunci secara berkala mutlak perlu dilakukan.

PasswordMonster Info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Stronger passwords use different types of characters Show password:

Type a password

No Password

0 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
0 second

Anda bisa memasukkan kata kunci atau sandi yang kerap Anda gunakan. Anda juga perlu menerapkan rasa skeptis, jangan-jangan layanan ini merekam kata sandi Anda. Jika Anda adalah orang yang tidak mudah percaya jika layanan ini tidak menyimpan data Anda, maka Anda bisa menggunakan pola serupa dengan kata sandi Anda saat mengisinya.

Misal kata sandi Anda adalah: “qwerty123456789” maka Anda bisa mengisikannya dengan pola sama, berupa 14 karakter seperti “makan610273845”. Layanan ini akan mengeluarkan informasi, berapa waktu yang peretas perlukan untuk membongkar kata sandi Anda, seperti tangkapan layar di bawah ini:

PasswordMonster

info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Stronger passwords use different types of characters

Show password:

.....|

Very Weak

17 characters containing:

Lower case

Upper case

Numbers

Symbols

Time to crack your password:

1.24 seconds

Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains a common password, a sequence of characters and a dictionary word.

Anda juga bisa mengecek apa kata sandinya dengan mencentang kotak di sisi kanan bertuliskan "Show password",

PasswordMonster

info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Stronger passwords use different types of characters

Show password:

qwerty12345678910

Very Weak

17 characters containing:

Lower case

Upper case

Numbers

Symbols

Time to crack your password:

1.24 seconds

Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains a common password, a sequence of characters and a dictionary word.

Anda bisa mengetahui berapa lama waktu yang diperlukan peretas untuk membobol kata sandi Anda. Kata sandi seperti contoh di atas sangatlah tidak aman karena peretas hanya memerlukan waktu kurang dari dua detik untuk meretasnya.

Untuk memitigasi peretasan melalui kata sandi, sebaiknya Anda menggunakan frasa sebagai pengganti kata sandi yang dikombinasikan dengan angka, huruf, simbol, karakter, hingga penggunaan huruf KAPITAL dan huruf kecil. Namun tentu frasa sandi yang baik adalah yang mampu ANDA INGAT. Misalnya: "Makannasikuning_pakeT3L0R#9". Hasilnya akan sangat berbeda seperti di bawah ini:

The screenshot shows the PasswordMonster website interface. At the top, it says "PasswordMonster" and "info@passwordmonster.com". The main heading is "How Secure is Your Password?". Below this, there is a section titled "Take the Password Test" with a tip: "Stronger passwords use different types of characters" and a "Show password:" checkbox. The password "Makannasikuning_pakeT3L0R#9" is entered in a green box, and the result is "Very Strong". Below the password box, it lists "27 characters containing: Lower case, Upper case, Numbers, Symbols". At the bottom, it states "Time to crack your password: 4 billion trillion years" and a review: "Review: Fantastic, using that password makes you as secure as Fort Knox."

Prinsip pembuatan kata sandi yang kuat adalah:

- Anda dapat mengingatnya.
- Tidak menggunakan kata sandi yang sama.
- Menggunakan kombinasi huruf, angka, simbol, hingga karakter seperti spasi (jika bisa).
- Paling sedikit memuat 15 karakter (satu huruf/simbol/karakter) dihitung satu karakter.
- Menggunakan frasa (bisa lirik lagu, peribahasa dalam bahasa daerah, dan lainnya dengan menerapkan prinsip di bagian atas).

Keamanan Komunikasi

Serangan digital lain yang perlu dimitigasi adalah *phishing* yang dilakukan dengan cara mengirimkan pesan lewat aplikasi percakapan, surat elektronik, hingga telepon. Seperti penjelasan di atas, phishing adalah cara

memanipulasi korban agar segera melakukan tindakan yang ujungnya dapat memberikan akses pada aset digital seperti nomor telepon, akun surat elektronik, hingga data perbankan.

Modus yang paling umum adalah dengan menguji korbannya dengan informasi yang terlalu menggembirakan atau mengkhawatirkan. Misal, korban mendapatkan hadiah atau informasi musibah yang menimpa keluarga atau rekannya. Penipu dapat menggunakan penipuan lewat suara, telepon (istilahnya *vhishing*) atau melalui pesan terselubung yang di dalamnya ada malware. Cara-cara ini termasuk dalam rekayasa sosial.

Untuk berlatih mengidentifikasi pesan terselubung yang kemungkinan berisi malware, Anda dapat memanfaatkan layanan dari [Shira](#). Ini produk dari Horizontal, lembaga nirlaba asal Amerika Serikat yang mendedikasikan layanan untuk keamanan dan privasi.



Home About

Welcome to Shira

Learn to identify and defeat phishing attempts

English

Start quiz




Layanan ini memang berbahasa Inggris namun ada fitur yang menarik di dalamnya. Penggunaanya bisa berlatih mengidentifikasi jenis phishing pada beragam aplikasi. Untuk mulai menggunakannya, Anda bisa membuat alamat surat elektronik atau memanfaatkan opsi pembuatan alamat surat elektronik otomatis.

Add a name and email address

We ask for a name and email address to make the phishing quiz feel more realistic. This information will not be saved, sent to our servers, or shared with anyone else.

To be extra-safe, you can use a fake name and email address, or generate random ones.

 Make a random name and email address

 Make a random name and email address



Next >

Setelah mengisi alamat surat elektronik, Anda bisa melanjutkan dengan mengetuk opsi “next” di sisi kanan bawah.

Which apps do you use?

Select at least 1



Gmail



Whatsapp



SMS



Messenger



Dating App

Tangkapan layar ini memperlihatkan beragam opsi percakapan yang Anda pilih untuk latihan mengidentifikasi phishing. Opsi ini yang jadi kelebihan dari layanan Shira.

Anda juga dapat memilih latar belakang Anda. Pemilihan ini nantinya berkaitan dengan isi pesan yang bakal Anda dapatkan saat latihan. Anda diberi opsi memilih tiga item. Tampilan layarnya akan seperti di bawah ini:

What areas are relevant to you?

Select up to 3 items



Human rights



Journalism and media



Academia



Marketing



Healthcare



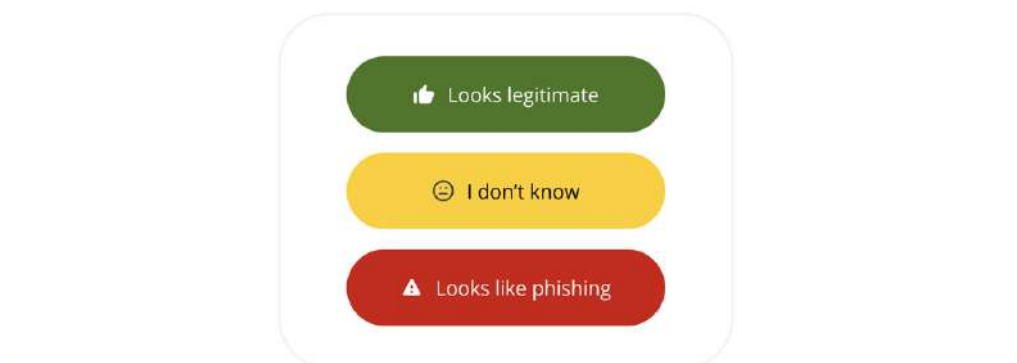
General

Setelah memilih latar belakang yang dirasa cocok, Anda akan mendapatkan petunjuk bagaimana latihan pada aplikasi ini. Pada setiap soal, Anda akan mendapatkan tiga pilihan, masing-masing, “looks legitimate” yang artinya bukan phishing, “I don’t know” jika Anda tidak dapat menentukan jawaban, serta “Looks like phishing” jika memang jawaban Anda atas soal yang muncul adalah phishing.

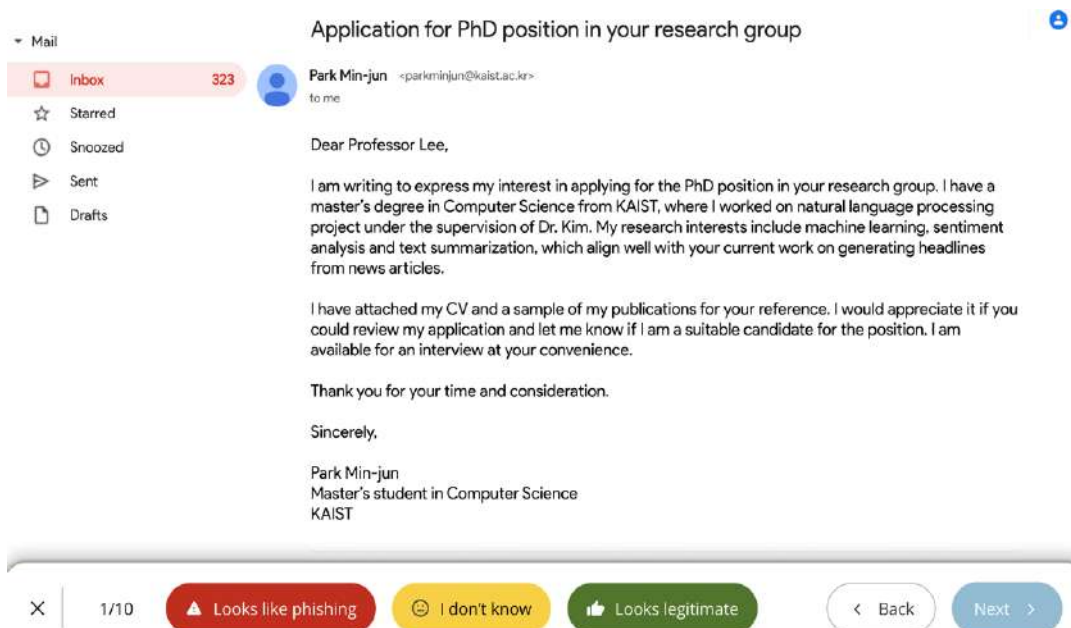
How it works

This quiz contains 10 questions.

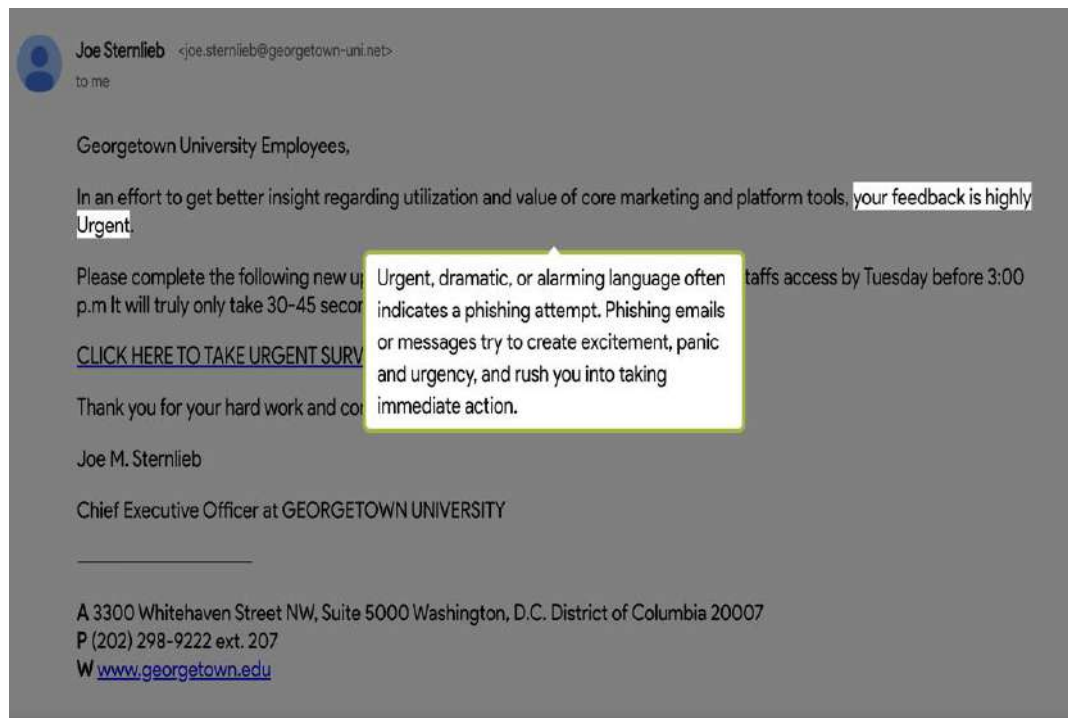
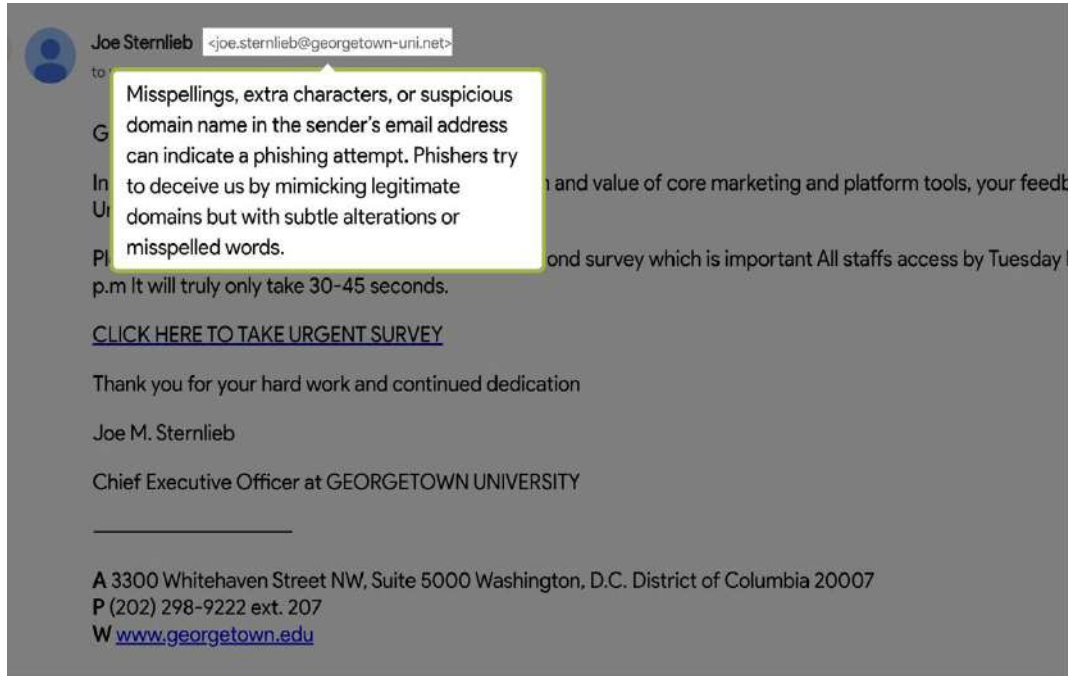
For each question, select whether the message shown seems like a phishing attempt or seems legitimate.

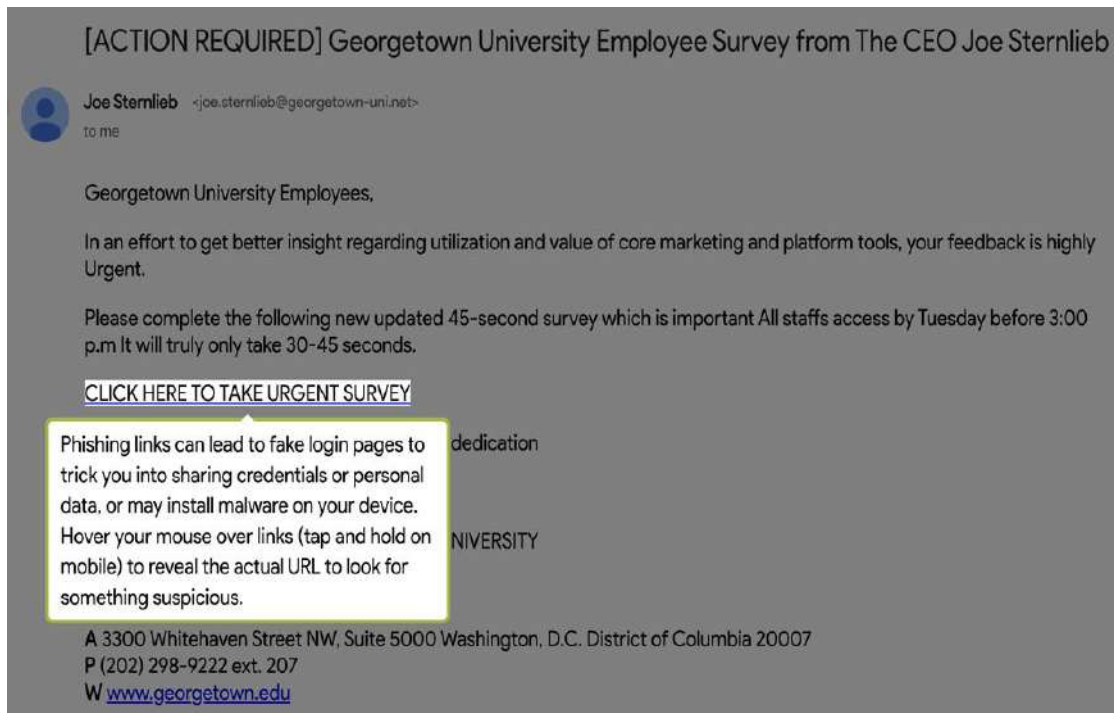


Pada setiap soal, jika memang tidak ada phishing dalam soal latihan, maka Anda bisa lanjut ke soal berikutnya dengan mengetuk “next” di sisi kanan bawah.

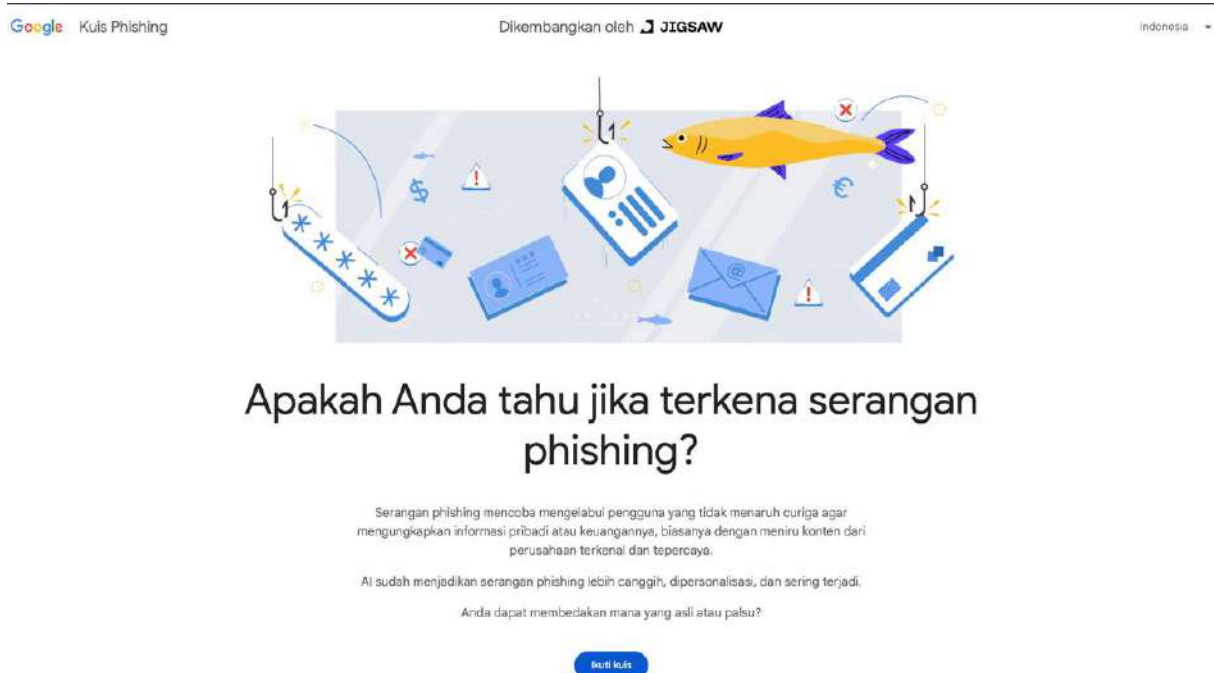


Nantinya jika ada soal yang memang phishing, meski jawaban Anda tepat atau salah, layanan ini akan memberikan informasi mengenai bagian mana dari pesan yang patut diduga terkait phishing, seperti beberapa tangkapan layar di bawah ini:



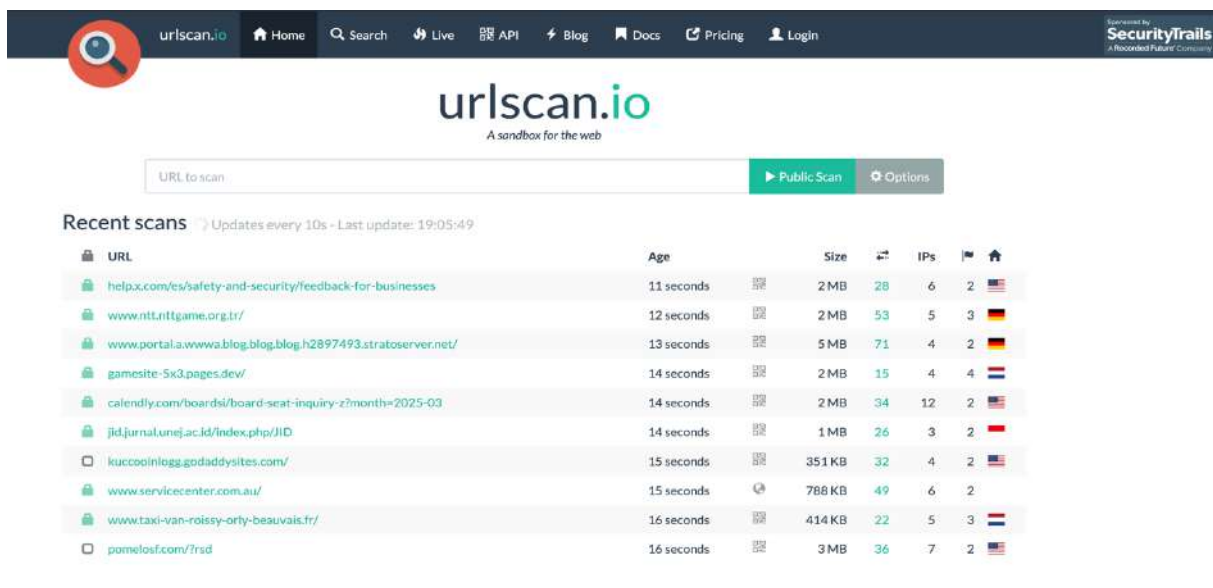


Fasilitas berlatih mengenali phishing lainnya, yang memakai Bahasa Indonesia, adalah [Kuis Phishing Google](#). Tampilannya seperti di bawah ini:



Cara menggunakannya tidak jauh berbeda dengan Shira. Diawali dengan membuat alamat surat elektronik. Proses selanjutnya sama. Setiap ada soal akan diminta memilih tiga opsi.

Selanjutnya, jika Anda mendapatkan sebuah pesan yang berisi tautan di dalamnya, Anda dapat melakukan pengecekan apakah tautan itu mengandung malware atau tidak. Caranya dengan mengakses [VirusTotal](#) atau [urlscan](#) dan masukkan tautan yang Anda dapatkan.



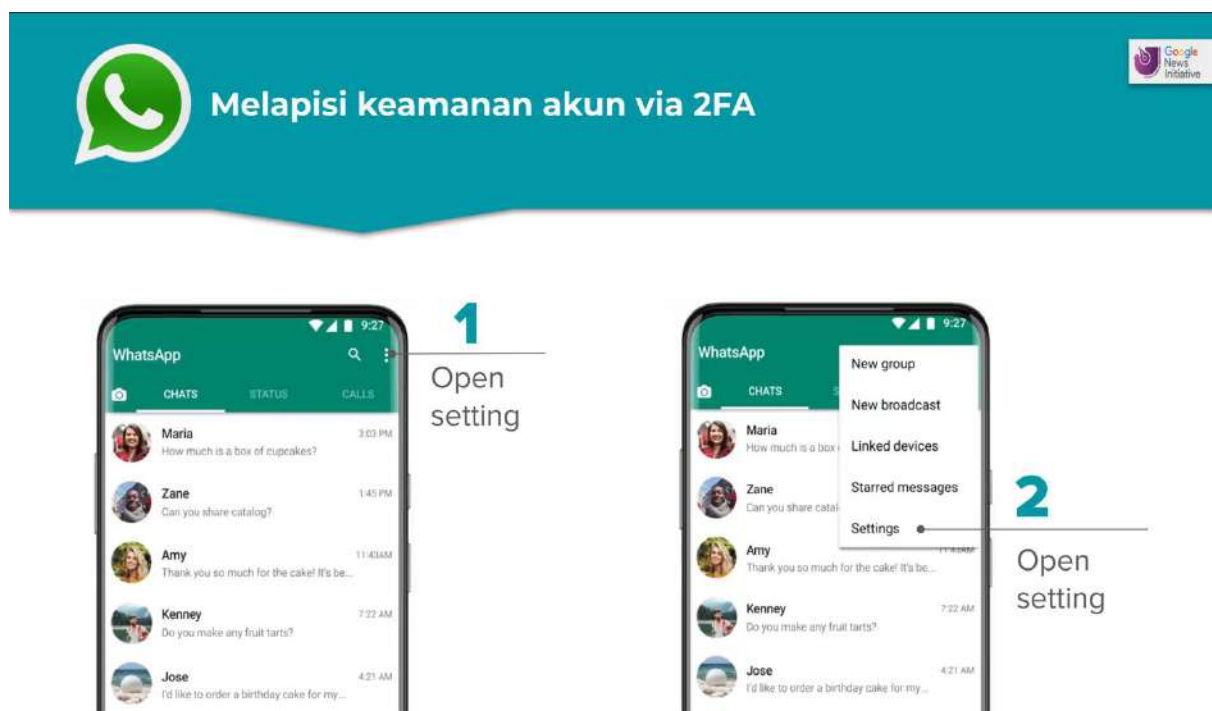
Kedua layanan ini akan menginformasikan apakah sebuah tautan mengandung malware atau tidak berdasarkan masukan dari pihak-pihak yang sudah melakukan pemeriksaan terlebih dulu pada tautan yang sama. Sebab, pelaku phishing kerap menggunakan tautan yang sama.

Mitigasi lain yang dapat Anda lakukan adalah menggunakan pengamanan berlapis dengan skema dua langkah verifikasi atau 2FA (two-factor authentication). Dalam modul ini Anda akan mendapatkan petunjuk tentang penerapan 2FA pada [aplikasi percakapan Whatsapp](#) yang paling banyak digunakan di Indonesia.

Ketika mengaktifkan verifikasi dua langkah, Anda memiliki opsi untuk memasukkan alamat email. Informasi tersebut memungkinkan WhatsApp mengirimkan kepada Anda email berisi tautan untuk mengatur ulang ketika Anda lupa PIN dan juga untuk membantu menjaga keamanan akun Anda.

Setelah mengaktifkan verifikasi dua langkah, WhatsApp secara rutin akan meminta Anda memasukkan PIN sebagai pengingat. Selama Anda tidak mengatur ulang PIN, Anda akan mendapatkan pengingat seminggu sekali.

Untuk menerapkannya, Anda bisa mengikuti tahapan-tahapan di bawah ini:

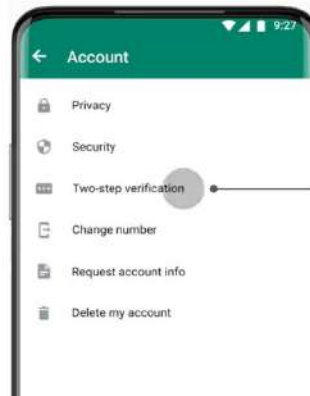




Melapisi keamanan akun via 2FA



3



4

Select two step verification



Melapisi keamanan akun via 2FA



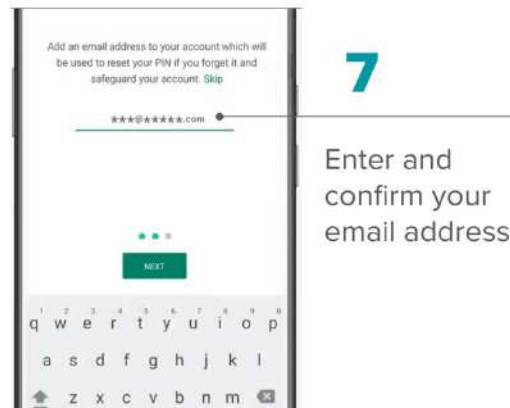
5

Tap ENABLE



6

Confirm your PIN




Saat terkoneksi dengan internet, sebaiknya memperhatikan peramban dan mesin pencari yang dipergunakan. Setiap peramban (browser) dan mesin pencari (search engine) biasanya akan merekam seluruh data dan aktivitas saat kita terkoneksi ke internet.

Secara lebih detil peramban biasanya merekam hal-hal di bawah ini:

- Alamat internet protokol (IP address).
- Portal yang kita kunjungi.
- Pola dan perilaku kita di portal tertentu.
- Nama akun dan kata sandi.

Pengembang peramban memerlukan data-data di atas yang biasanya digunakan untuk 'dijual' kepada pengiklan. Karena peramban merekam alamat internet protokol, maka mereka dapat mengidentifikasi pengguna berasal dari wilayah mana, perangkat yang dipakai saat terkoneksi dengan internet, hingga perilaku lain dari pengguna internet yang kemungkinan berharga bagi pengiklan.

Untuk dapat mengidentifikasi peramban yang sesuai dengan kebutuhan, berikut tangkapan layar dari pengembang peramban Brave yang membandingkan dirinya dengan peramban lain, lengkap dengan kekurangan dan kelebihan masing-masing:

Built-in features	 Brave	 Chrome	 DDG	 Edge	 Firefox	 Safari
Invasive ads blocked	✓	—	✓	✗	✗	✗
Cross-site trackers blocked	✓	✗	✓	—	—	✗
Third-party cookie tracking blocked	✓	✗	✓	—	✓	✓
Fingerprinting blocked (cookie-less trackers)	✓	✗	—	✗	—	—
Malware & phishing protection*	✓	✓	✗	✓	✓	✓
Protections against bounce tracking	✓	✗	—	✗	—	✗
Anonymized network routing (Tor mode)	✓	✗	✗	✗	✗	✗
Assert opt-out privacy rights (GPC)	✓	✗	✓	✗	—	✗

Prinsip serupa dapat Anda gunakan untuk memilih mesin pencari. Layanan yang tersedia dan banyak dipergunakan publik, antara lain, Google, Baidu, Yandex, Bing, Qwant, DuckDuckGo, dan Startpage.

Untuk pemilihan mesin pencari ini, sebaiknya disesuaikan dengan kebutuhan Anda. Jika pencarian terkait data sensitif, usahakan menggunakan mesin pencari yang tidak merekam jejak pencarian Anda.

Perhatikan juga pengembang dari masing-masing mesin pencari, apakah pengembang atau servernya berada di negara yang menerapkan keamanan data pribadi atau tidak? Cina dan Rusia adalah contoh dua negara yang diketahui tidak mengedepankan keamanan data pribadi. Untuk mitigasi, sebaiknya Anda menggunakan produk dari pengembang yang memang terikat dengan aturan hukum perlindungan data pribadi.

Layanan lain yang dapat Anda manfaatkan saat terkoneksi internet adalah VPN (Virtual Private Network). Secara umum, VPN adalah perangkat lunak yang mengenkripsi lalu lintas data saat Anda terhubung ke peladen eksternal melalui koneksi yang aman. VPN juga menyembunyikan lokasi penggunaannya ketika mengakses internet.

Tanpa menggunakan VPN maka lalu lintas data Anda ibarat aliran air dalam selang plastik transparan. Orang bisa melihat apa yang ada di dalam selang tersebut. Jika Anda mengaktifkan VPN, maka alamat perangkat atau IP Address Anda yang terlihat oleh pihak lain berbeda dengan IP Address sesungguhnya.

Manfaat pemakaian VPN, yang dapat menyembunyikan lokasi, memungkinkan penggunaannya menembus blokir oleh negara. Ambil contoh Reddit, sebuah forum diskusi di internet yang berasal dari Amerika Serikat. Sejak 2015, Indonesia memblokir akses ke forum ini. Namun dengan menggunakan VPN, blokir tersebut dapat ditembus.

Pertimbangan dalam memilih layanan VPN:

- Pilih yang sudah dikenal dan dipercaya oleh komunitas, seperti ProtonVPN, RiseUp VPN, TunnelBear, serta NordVPN.
- Hindari penggunaan layanan VPN yang menggunakan peladen di negara-negara otoriter seperti Rusia dan Cina.
- Penggunaan VPN secara sembarangan tanpa memerhatikan lokasi peladen serta kebijakan perlindungan data pribadi dapat membuat penggunaannya jadi korban kejahatan digital.

Manfaatkan VPN jika terpaksa mengakses internet di tempat umum seperti kafe, hotel, bandara, dan lainnya.

4.5. Aplikasi percakapan

Gunakan aplikasi percakapan yang menggunakan sistem terenkripsi ujung ke ujung (end to end encryption atau E2EE) karena dapat mencegah semua akses pihak ketiga pada konten yang dipertukarkan.

Apakah jika sebuah platform menyatakan bahwa pesan dienkripsi itu berarti tidak ada yang dapat mengakses konten? Belum tentu.

Access Now, lembaga internasional yang fokus pada hak-hak digital serta layanan insiden digital mencatat, beberapa pengembang menawarkan sistem E2EE pada layanannya. Misalnya, Signal, Whatsapp, dan iMessage. Semua obrolan pribadi dan grup di layanan itu secara default atau otomatis terenkripsi sejak kita menggunakan layanannya.

Di aplikasi percakapan lain, Telegram misalnya, hanya bisa mengaktifkan E2EE ketika kita memilih secara manual opsi “Start Secret Chat”. Fitur ini hanya berfungsi untuk obrolan tidak lebih dari dua orang dan hanya dapat diaktifkan ketika dua orang tersebut sedang *online*.

Aplikasi percakapan alternatif lainnya adalah Wire yang menerapkan sistem E2EE pada semua pesan, panggilan, serta aktivitas berbagi dokumen. Sehingga alamat pengguna (IP address) dan data pengguna tetap aman. Aplikasi bisa dihapus dari jarak jauh jika terjadi insiden kehilangan perangkat.

Aplikasi alternatif lainnya, yaitu Session, menerapkan sistem E2EE. Aplikasi ini tidak memerlukan nomor, alamat email pengguna, serta tidak merekam metadata penggunaannya.

Berikut beberapa tips saat memilih aplikasi percakapan:

- Hindari penggunaan Whatsapp untuk komunikasi berisiko tinggi karena popularitasnya yang cukup tinggi. Aplikasi ini rentan diserang. Salah satunya karena pengiriman kode otentikasi atau OTP-nya masih melalui SMS yang tidak terenkripsi dan mudah diretas.
- Perhatikan penyimpanan konten pada aplikasi percakapan. Signal hanya menyimpan konten secara lokal di perangkat, dan tidak ada cadangan di tempat lain. WhatsApp memiliki mekanisme mencadangkan pesan di penyimpanan awan, baik dengan format E2EE dan non-E2EE. Telegram tidak mencadangkan “Secret Chat” yang dilindungi E2EE namun mencadangkan obrolan lain dan memiliki kunci deskripsi untuk cadangan tersebut.
- Pilih platform yang melindungi metadata atau informasi tentang pesan, bukan kontennya. Metadata dapat mengungkapkan kapan, bagaimana, serta dengan siapa Anda berkomunikasi. Bahkan metadata Anda bisa jadi lebih sensitif dari konten pesan Anda karena dapat mengungkapkan ke mana Anda pergi, apa yang Anda lakukan, serta siapa yang Anda ajak bicara. WhatsApp mengumpulkan metadata, termasuk informasi lokasi Anda, informasi kontak, penggunaan data, dan sebagainya.
- Kombinasikan penggunaan aplikasi percakapan sesuai kebutuhan dan konteksnya.

4.6. Memilih surat elektronik

Salah satu metode komunikasi memanfaatkan internet yang jamak dipakai adalah dengan surat elektronik. Namun tidak semua penggunaannya menyadari jika layanan surat elektronik kadang tidak dienkripsi hingga bisa dengan mudah dibaca pihak lain yang memiliki akses terhadap datanya.

Untuk memastikan keamanan tersebut, Anda bisa memilih beberapa layanan surat elektronik yang menyediakan fitur enkripsi, seperti:

1. Rise Up

- Fitur tidak berbayar menyediakan ruang penyimpanan hingga 1 Gigabyte.
- Proses pendaftaran tidak melibatkan data pribadi karena menggunakan sistem undangan.
- Pengembang tidak mengungkapkan lokasi Anda kepada penerima surat elektronik.

2. Proton Mail

- Fitur tidak berbayar menyediakan ruang penyimpanan hingga 500 Megabyte
- Ada fitur pengaturan masa berlakunya surat elektronik.
- Pengaturan enkripsi manual untuk pengiriman ke layanan non Proton.

3. Tuta

- Fitur tidak berbayar menyediakan ruang penyimpanan hingga 500 Megabyte.

4.7. Berbagi dokumen

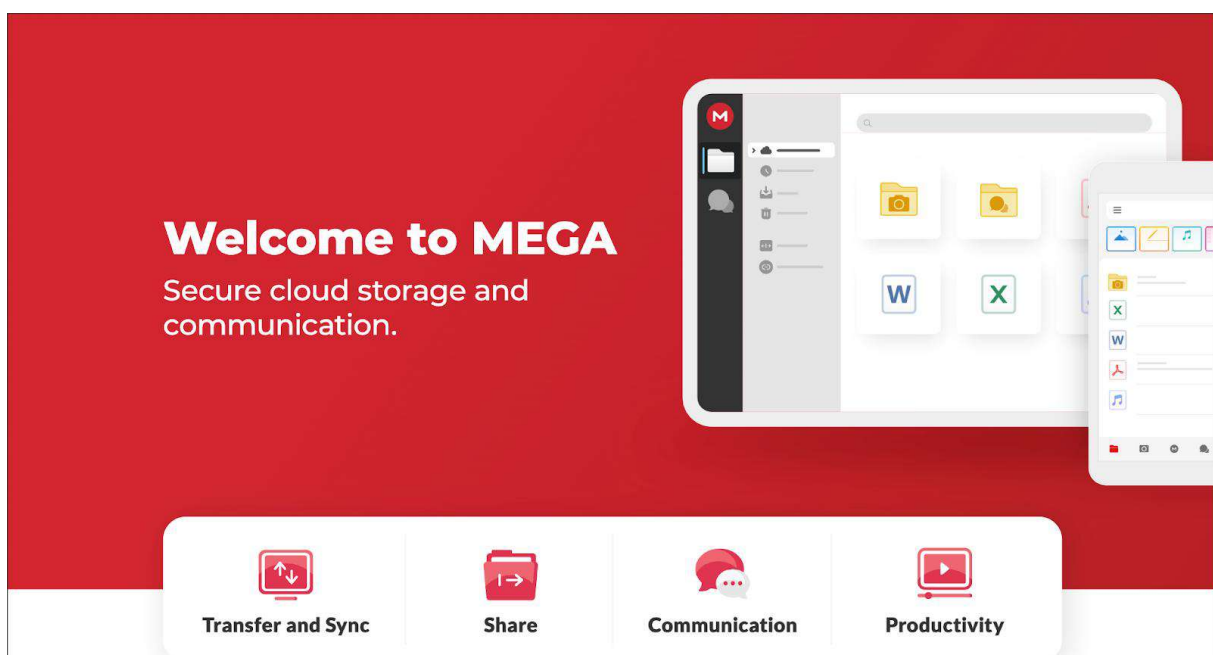
Bekerja dengan menggunakan internet memiliki sejumlah keunggulan. Salah satunya adalah bisa berbagi dokumen kerja pada saat bersamaan. Di balik keunggulan itu tentu ada juga risikonya jika dokumen tersebut tidak terenkripsi.

Guna memitigasi risiko tersebut, ada baiknya Anda menggunakan layanan berbagi berkas yang lebih peduli pada keamanan dibanding Google Drive yang jamak digunakan warganet.

Untuk keperluan berbagi dokumen pekerjaan yang bisa diakses bersama, bisa menggunakan layanan dari www.cryptpad.fr yang menawarkan dokumen teks, dokumen pengolahan data, hingga formulir daring. Semua dokumennya dipastikan terenkripsi.



Untuk keperluan berbagi dokumen atau berkas dengan penyimpanan awan, Anda dapat menggunakan layanan dari www.mega.nz. Fasilitas yang bisa diakses dari aplikasi desktop, seluler, dan portal secara cuma-cuma ini menyediakan kapasitas penyimpanan hingga 20 Gigabyte. Pengembang juga tidak melihat data apa yang Anda simpan dan edarkan.

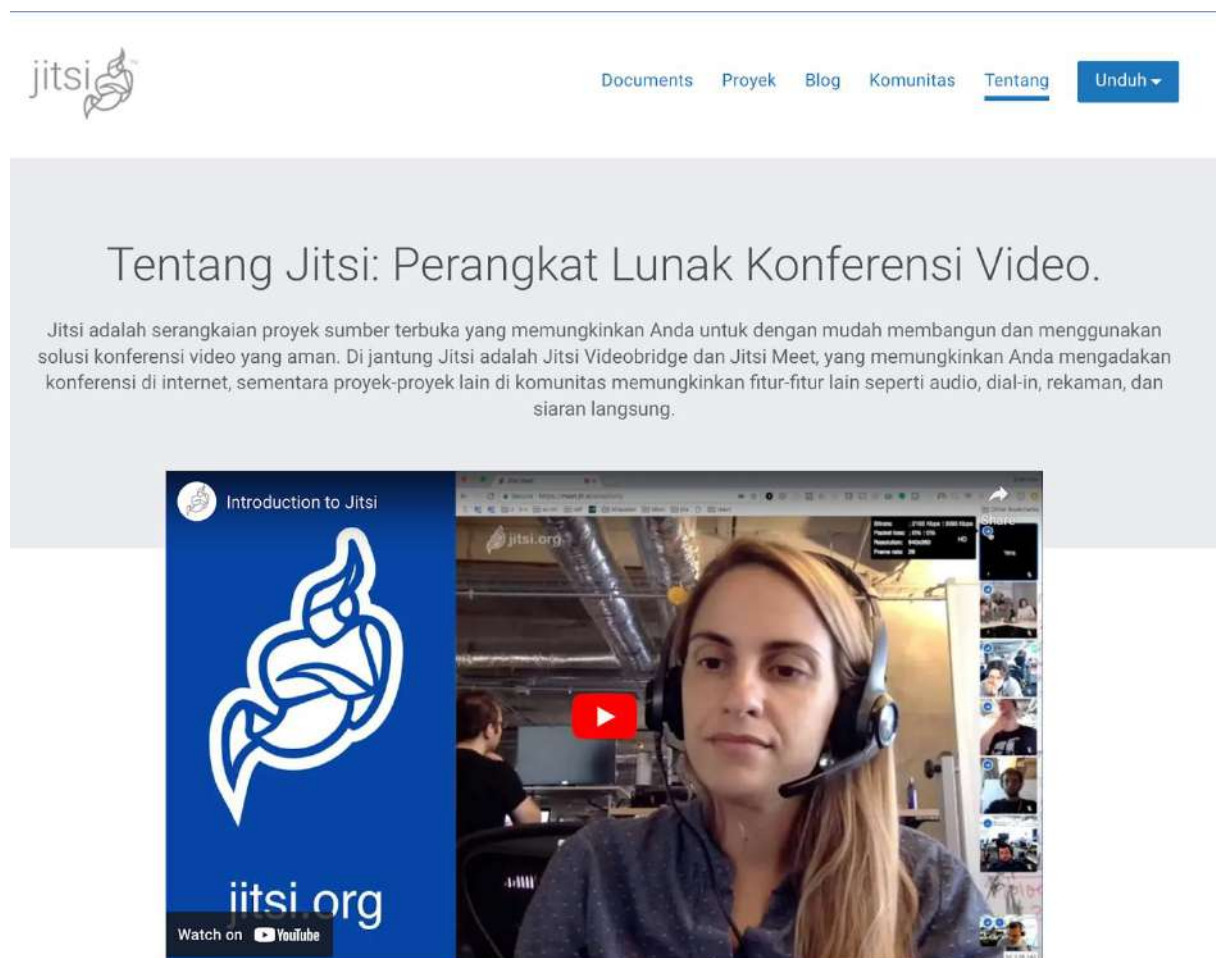


4.8. Aplikasi pertemuan video

Pemanfaatan aplikasi panggilan video semakin marak seiring pandemi COVID-19. Proses kerja dengan memanfaatkan layanan seperti itu terus berlangsung hingga saat ini. Namun sebaiknya kita juga memitigasi perilaku daring kita dengan memanfaatkan layanan panggilan video sesuai kebutuhan dan melihat kondisinya. Seperti prinsip sebelumnya, kita berupaya memanfaatkan layanan yang menyediakan fungsi enkripsi dalam lalu lintas datanya.

Aplikasi Zoom merupakan salah satu yang paling umum digunakan dan sudah terenkripsi dari ujung ke ujung. Namun layanan ini berbayar untuk panggilan lebih dari 60 menit dan juga menyimpan riwayat penggunaannya.

Aplikasi panggilan video lainnya adalah <https://jitsi.org/> yang terenkripsi dari ujung ke ujung dan tidak berbayar tanpa terikat waktu. Saat mengakses panggilan video pada layanan ini, pengguna tidak perlu *log in*.



jitsi

Documents Proyek Blog Komunitas Tentang Unduh

Tentang Jitsi: Perangkat Lunak Konferensi Video.

Jitsi adalah serangkaian proyek sumber terbuka yang memungkinkan Anda untuk dengan mudah membangun dan menggunakan solusi konferensi video yang aman. Di jantung Jitsi adalah Jitsi Videobridge dan Jitsi Meet, yang memungkinkan Anda mengadakan konferensi di internet, sementara proyek-proyek lain di komunitas memungkinkan fitur-fitur lain seperti audio, dial-in, rekaman, dan siaran langsung.

Introduction to Jitsi

iitsi.org

Watch on YouTube



**ALIANSI
JURNALIS
INDEPENDEN**
Alliance of Independent Journalist

BAB V.

ETIKA PENGUNAAN AI UNTUK AKADEMIK DAN INDUSTRI MEDIA

BAB V. ETIKA PENGGUNAAN AI UNTUK AKADEMIK DAN INDUSTRI MEDIA

Tujuan Bab ini adalah mendiskusikan terkait urgensi etika dalam penggunaan AI, konstelasi soal kajian etika AI, dan bagaimana mengadaptasi etika AI dalam dunia akademik dan industri media di Indonesia.

Pertanyaan pemantik:

1. Mengapa kode etik diperlukan bagi pengguna AI?
2. Apa saja standar umum etika dalam dunia akademik dan industri media di Indonesia?
3. Apa saja ruang lingkup etika dalam penggunaan AI dan bagaimana implementasinya?

Metode penyampaian:

- Ceramah
- Diskusi

5.1 Etika Penggunaan AI dalam Dunia Akademik

5.1.1. Kontroversi dan Urgensi Etika AI

AI is everywhere. AI telah ada di sekitar kita. Dunia akademik di Indonesia, merujuk hasil riset Temasek (2024), adalah sektor ketiga yang paling tersentuh penetrasi AI setelah bisnis, khususnya marketing dan hiburan. Sudah sejak cukup lama para akademisi di negara ini memakai sejumlah tool AI seperti Turnitin, Zotero, Google-search dan sejenisnya. Dunia akademik kini bisa dikatakan dihegemoni oleh AI atas nama inovasi dan efisiensi kerja produksi pengetahuan.

Bagaimana posisi AI sejatinya dalam tradisi akademik, termasuk dalam kerja menulis-publikasi artikel jurnal? Menyimak pola relasi akademisi dengan AI, ada empat kemungkinan sebagai dampaknya: mengganti; membantu, menipu, atau mengendalikan. Hal ini bukan hanya soal pilihan sadar kita selaku konsumen aktif AI, tapi konstruksi sosial teknologis dan

iklim ekonomi akademik yang bisa membuat para akademisi menjadi korban AI. Dengan kata lain, ada efek glorifikasi dan hyper-promosi perusahaan teknologi digital global yang merupakan produsen AI yang datang langsung lewat gawai atau ruang-ruang percakapan informal akademik di kampus.

Penggunaan AI bagi akademisi selalu terkait tiga hal: penggunaan/konsumsi, risiko, dan strategi mitigasinya. Setiap teknologi yang dipakai ada risiko, baik ekonomi (biaya) hingga reputasi akademik. Persoalan terakhir inilah yang paling serius dan perlu mitigasi berlapis: moral, etik dan regulasi. Sebagai manusia pembelajar dan role model mahasiswanya, akademisi tak boleh hanya paham dan pandai memakai tools AI, tapi juga mesti cerdas dalam mitigasi risiko. Badan dunia UNESCO dan Uni Eropa membagi empat klaster resiko AI bagi manusia: unacceptable, acceptable, high dan low risk.

Mari kita membuat ilustrasi kerja riset yang melibatkan AI. Saat kita hendak membuat proposal ide riset atau artikel ilmiah, kita mulai terbiasa bertanya ke ChatGPT atau Microsoft Copilot. Saat membuat studi literatur, kita terbiasa memakai NVIVO, minta bantuan Google Form saat pengumpulan data, memakai Grammarly saat menulis laporan, menggunakan Turnitin atau GPTzero saat memeriksa kemiripan naskah.

Masih ada ratusan aplikasi AI lain yang bersaing berebut konsumen dari kalangan akademisi. Seperti kita ketahui, sebagian besar teknologi AI itu disuplai oleh empat perusahaan teknologi raksasa Amerika Serikat, yaitu Meta, Alphabet, Microsoft, dan Apple. Melihat praktik selama ini, nyaris tidak ada tahapan riset dan publikasi tanpa bantuan AI.

Ilustrasi lain soal peran AI dalam dunia akademik bisa dilihat seperti ini. Ibarat sebuah pohon, struktur artikel ilmiah akan selalu terdiri dari ini: *introduction, literature/conceptual review, method, finding, analysis, conclusion, references*. Menariknya, pada setiap tahapan ini telah tersedia tools AI-nya yang bisa dipakai secara cuma-cuma. Puncaknya, penulis dapat meminta AI untuk membuatkan judul dan abstrak bagi artikel yang akan ditulisnya.

Ini seperti sebuah kerja mesin yang sempurna, sehingga kita patut bertanya, lalu siapa penulis artikel sebenarnya? Bagaimana AI seharusnya diposisikan (secara etis)? Jawabannya tak mudah dan tak selalu merujuk norma moral binari: Etis atau tidak Etis. Ada banyak aspek pertanyaan lain yang harus diajukan. Misalnya, humanis atau tidak? Ada value atau tidak?

Mengikuti alam pikir utilitarianistik, pertanyaannya juga bisa seperti ini: apa untung ruginya bagi pengguna?

Filsafat teknologi mengajak berpikir holistik tentang tiga model relasi manusia dengan AI. Pertama, human where AI within. Apa yang dilakukan AI identik dengan kerja manusia itu sendiri, bahkan diproyeksikan bisa menggantikannya. Dengan kata lain AI bisa jadi peneliti, penulis dan malah mungkin berhak masuk sitasi.

Kedua, human with technology. AI diperlakukan sebagai mitra, alat bantu atau menjadi kontributor teknis bagi kerja akademik. Tak ubahnya seperti kendaraan. Ia dipergunakan manusia, bukan sebaliknya. Acknowledgment kontribusi artikel yang dibuat dengan sistem kerja seperti ini tetap kepada manusia, bukan AI. Hanya perlu disclaimer adanya kontribusi atau peran AI dalam karya tersebut.

Ketiga, human against technology. AI adalah musuh bersama, ada perlawanan terhadap hegemoni AI, baik terhadap teknologinya, bisnis hingga kepemilikannya. AI seharusnya dipakai untuk direplikasi, mendukung inovasi ilmiah, lalu mestinya ditundukkan.

Melihat tiga kategori di atas, kategori kedua tampaknya yang lebih realistis di Indonesia dan selaras dengan praktik relasi media sosial dan akademisi daripada sebaliknya, yaitu internet vs scholars. Fakta menariknya bahwa kategori pertama cenderung makin menguat di Indonesia. Sedangkan kategori ketiga agaknya mustahil terjadi di Indonesia mengingat konsumerisme terhadap AI yang sangat tinggi.

Diskursus AI untuk dunia akademik melingkupi pula bagaimana ia menjadi bahan ajar dengan target mengubah posisi mahasiswa pemakai AI dari naive user ke critical users. Dalam hal ini perlu suatu kurikulum literasi AI, yang mengkaji tiga aspek: teknologi, governance atau model bisnis, dan regulasi secara etik dan hukum. Artinya, pendekatan pengajaran AI, atau literasi AI mestinya bersifat lintas disiplin, bukan lagi mono disiplin. Kajian AI bukan monopoli ilmu informatika, tapi ia bisa dikaji dari perspektif sosiologi, ekonomi, dan hukum.

Ada banyak tawaran iklan yang menyediakan jasa menulis instant dan itu cukup menggoda para dosen. Ini juga bersamaan dengan budaya buruk yang sepertinya terlanjur menggejala di kalangan mahasiswa, yaitu tradisi copy paste, plagiasi, yang disebut sebagian orang sebagai tanda kemalasan berpikir. Lalu ada normalisasi juga melalui pernyataan bahwa semua AI wajar dipakai, dijadikan tools untuk riset dan penulisan tanpa verifikasi.

Muncul juga fenomena kecanduan penggunaan hingga penuhanan AI di kalangan akademisi dan praktisi bisnis. Sehingga karya tulis akademik pun seperti mengalami *blur authorship*.

Muncul pertanyaan, siapa atau pihak yang salah bagi terciptanya situasi ini? Lembaga apa yang paling perlu dimintai tanggung jawab secara hukum dan etis? Perguruan tinggi, korporasi pembuat AI? Untuk menjawabnya, dari kajian regulasi AI, Indonesia bisa belajar dari negara lain, misalnya melalui Brussel model, Silicon Valley model, India model, China model, Korea model. Ada dua kontradiksi yang perlu dipahami mahasiswa, akademikus dan regulator AI. Silicon Valley atau American model identik dengan inovasi, efisiensi, *profit, expansion*. Sebaliknya, Brussel/Eropa model identik dengan *inclusion, protection* dan *access to AI* dalam tata kelola teknologi ini.

Belajar dari publikasi artikel yang ditulis ChatGPT oleh Elsevier, maka diskursus terkait kepengarangan menjadi terdisrupsi dari individu atau kelompok manusia ke teknologi. Adanya *machine authorship* menjadikan kepengarangan tidak lagi murni manusia. Kolaborasi manusia dengan mesin menjadi faktor baru yang memicu perdebatan soal etik dan hukum. Dalam konteks ini, muncul pertanyaan apakah AI perlu ditempatkan sebagai penulis hantu? Atau semata asisten penulis? Apakah kerja AI yang hampir sempurna pada seluruh tubuh sebuah tulisan akademik akan dianggap sebagai kerja orisinal dari manusia penggunaanya atau ia diposisikan sebagai murni AI? Apakah kerja AI di tulisan ilmiah dapat dipertanggungjawabkan secara hukum oleh AI, bukan oleh manusia?

5.1.2. Etika Umum Publikasi Ilmiah

Di Indonesia, penulisan artikel ilmiah dan kegiatan akademik secara umum mengacu kepada sejumlah pedoman Etika Ilmiah yang secara umum dilandasi beberapa aturan dasar berikut ini. Mencermati berbagai aturan dibawah ini, kiranya Indonesia memiliki aturan yang cukup banyak dan lengkap, meskipun tertinggal dalam regulasi terkait kecerdasan buatan.

1. Undang-undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional.
2. Undang-Undang Republik Indonesia Nomor 12 Tahun 2012 tentang Pendidikan Tinggi (kemudian mengalami revisi).
3. Peraturan Pemerintah Nomor 17 Tahun 2010 tentang Pendidikan Tinggi.

4. Peraturan Pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi.
5. Peraturan Pemerintah Nomor 57 Tahun 2021 tentang Standar Nasional Pendidikan sebagaimana diubah dengan Peraturan Pemerintah Nomor 4 tahun 2022 tentang Perubahan Atas Peraturan Pemerintah Nomor 57 Tahun 2021 Tentang Standar Nasional Pendidikan.
6. Peraturan Menteri Pendidikan Nasional Nomor 17 Tahun 2010 tentang Pencegahan dan Penanggulangan Plagiat di Perguruan Tinggi.
7. Peraturan Menteri Pendidikan Nasional Nomor 39 Tahun 2021 tentang Integritas Akademik dalam Menghasilkan Karya Ilmiah.
8. Peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia Nomor 53 Tahun 2023 tentang Penjaminan Mutu Pendidikan Tinggi.

Rujukan lain mengenai etik dalam publikasi ilmiah adalah Permendikbudristek No. 39 tahun 2021, pasal 9 yang menyebutkan, “Pelanggaran Integritas Akademik dalam menghasilkan Karya Ilmiah terdiri atas: fabrikasi; falsifikasi; plagiat; kepengarangan yang tidak sah; konflik kepentingan; dan pengajuan jamak.” Pasal 10 dari peraturan itu menjelaskan lebih mendetail seperti berikut ini:

Pertama, Fabrikasi sebagaimana dimaksud dalam Pasal 9 huruf a merupakan pembuatan data penelitian dan/atau informasi fiktif.

Kedua, Falsifikasi sebagaimana dimaksud dalam Pasal 9 huruf b merupakan perekayasaan data dan/atau informasi penelitian.

Ketiga, Plagiat sebagaimana dimaksud dalam Pasal 9 huruf c merupakan perbuatan: mengambil sebagian atau seluruh karya milik orang lain tanpa menyebut sumber secara tepat; menulis ulang tanpa menggunakan bahasa sendiri sebagian atau seluruh karya milik orang lain walaupun menyebut sumber; dan mengambil sebagian atau seluruh karya atau gagasan milik sendiri yang telah diterbitkan tanpa menyebut sumber secara tepat.

Keempat, Kepengarangan yang tidak sah sebagaimana dimaksud dalam Pasal 9 huruf d merupakan kegiatan seseorang yang tidak memiliki kontribusi dalam sebuah Karya Ilmiah berupa gagasan, pendapat, dan/atau peran aktif yang berhubungan dengan bidang keilmuan berupa:

- (a) menggabungkan diri sebagai pengarang bersama tanpa memberikan kontribusi dalam karya;
- (b) menghilangkan nama seseorang yang mempunyai kontribusi dalam karya; dan/atau'
- (c) menyuruh orang lain untuk membuat karya sebagai karyanya tanpa memberikan kontribusi.

Kelima, Konflik kepentingan sebagaimana dimaksud dalam Pasal 9 huruf e merupakan perbuatan menghasilkan Karya Ilmiah yang mengikuti keinginan untuk menguntungkan dan/atau merugikan pihak tertentu.

Keenam, Pengajuan jamak sebagaimana dimaksud dalam Pasal 9 huruf f merupakan perbuatan mengajukan naskah Karya Ilmiah yang sama pada lebih dari satu Jurnal Ilmiah yang berakibat dimuat pada lebih dari satu Jurnal Ilmiah.

Demi menjaga integritas akademik, kejujuran dalam melakukan penelitian dan publikasi hasil penelitian harus dijunjung tinggi untuk menjaga harkat dan martabat sebagai pendidik atau civitas academica di perguruan tinggi. Apa yang disebut malpraktek dalam penelitian dan publikasi dapat berupa hal-hal berikut ini:

1. Fabrikasi. Membuat-buat atau merekayasa (*making up*) data dan hasil penelitian dan melaporkan sebagai hasil penelitian. Ini merupakan gabungan antara plagiat dan falsifikasi.
2. Falsifikasi (Membenarkan yang salah). Memanipulasi material, pelaporan dan proses penelitian, menghilangkan atau mengubah data atau hasil penelitian, sehingga laporan penelitian tidak sesuai dengan catatan penelitian.
3. Plagiarism. Penggunaan ide, proses, hasil dan kata-kata orang lain tanpa memberikan pengakuan atau sumbernya.
4. Mengambil makalah orang lain (mendownload dari web, blog dan sebagainya) dan menggantikan nama penulisnya dengan nama sendiri.
5. Membuat copy dari artikel orang lain dan memasukkan ke dalam makalah atau tulisan sendiri tanpa menyebutkan penulis asli dalam tulisan kita alias tidak melakukan sitasi.
6. Melakukan cut and paste dari beberapa makalah atau tulisan orang lain dan menjadikan tulisan sendiri tanpa menyebutkan dalam tulisan kita atau tidak melakukan sitasi.
7. Self-plagiarism, yaitu menjiplak dari tulisan sendiri yang sudah dipublikasikan.

Adapun etika ilmiah universal dalam publikasi karya tulis akademik pada jurnal ilmiah (berbasis manusia) adalah sebagai berikut:

- a. Memastikan bahwa yang termasuk dalam daftar penulis telah memenuhi kriteria sebagai penulis.
- b. Bertanggung jawab secara kolektif untuk pekerjaan dan isi artikel, yang meliputi metode, analisis, perhitungan, dan rinciannya.
- c. Menyatakan asal sumber daya (termasuk pendanaan), baik secara langsung maupun tidak langsung.
- d. Menjelaskan *novelty* dan keterbatasan dalam penelitian.
- e. Menanggapi komentar yang dibuat oleh mitra bestari dan dewan redaksi secara profesional ilmiah dan tepat waktu.
- f. Menginformasikan secara tertulis kepada editor jika akan menarik kembali karya tulisnya.
- g. Membuat pernyataan bahwa karya tulis yang diserahkan untuk diterbitkan adalah asli, dan belum pernah dipublikasikan di manapun dan dalam bahasa apapun, dan tidak sedang dalam proses pengajuan ke penerbit lain.

Ketentuan mengenai etika dalam publikasi karya dengan bentuk digital/elektronik maupun cetak mencakup hal-hal sebagai berikut:

- a. Naskah yang ditulis merupakan hasil pemikiran atau penelitiannya secara jelas, jujur, tanpa plagiasi dan manipulasi data.
- b. Naskah yang ditulis harus dibuat sesuai dengan *template* dari media publikasi yang dituju.
- c. Tidak melakukan rekayasa digital dalam bentuk apapun pada karya yang dipublikasikan.
- d. Mematuhi persyaratan publikasi berupa orisinalitas karya, tidak plagiat, dan belum pernah diterbitkan di jurnal atau publikasi lain.
- e. Memastikan bahwa nama-nama yang tercantum sebagai penulis, termasuk urutannya, sesuai dengan urutan kontribusinya dan disetujui oleh seluruh anggota.
- f. Bertanggungjawab secara kolektif untuk pekerjaan dan isi artikel yang meliputi metode, analisis, perhitungan dan rinciannya.
- g. Menyiapkan bukti bahwa penelitian yang dilakukan telah memenuhi persyaratan etika penelitian, termasuk menyediakan catatan lapangan atau *log book* penelitian jika diminta.
- h. Tidak terlibat dalam plagiarisme atau plagiarisme-diri, dan publikasi salami.
- i. Membuat pernyataan bahwa karya tulis yang diserahkan untuk diterbitkan adalah asli, dan belum pernah dipublikasikan di manapun

dan dalam bahasa apapun, dan tidak sedang dalam proses pengajuan ke penerbit lain.

- j. Menghindari media publikasi yang termasuk dalam jurnal predator dan/atau penerbit predator.

Di luar karya ilmiah, karya seni adalah ciptaan artistik atau benda estetik yang juga berpotensi melanggar kode etik karena melibatkan AI. Karya seni mungkin juga digunakan untuk menyebut karya apa pun yang dianggap berseni dalam artian luas, termasuk karya sastra dan musik. Publikasi karya seni dapat dilakukan dalam bentuk pertunjukan/pementasan atau pameran.

Publikasi karya seni dalam bentuk pertunjukan atau pameran, perlu memastikan sejumlah hal ini: tidak memasukkan unsur SARA dalam karya yang dipublikasikan; menentukan segmen pengunjung dalam melakukan pertunjukan atau pameran sesuai konsep karya; mengembalikan struktur bangunan atau tempat yang digunakan jika pertunjukan atau pameran mengubah struktur bangunan.

5.1.3. Ruang Lingkup Etika AI

Teknologi AI bisa dengan mudah disalahgunakan oleh para penulis untuk menghasilkan karya yang bersifat plagiasi. Praktik semacam ini jelas melanggar etika. Karena itu penting bagi kalangan akademisi dan pembuat regulasi menyikapi kehadiran AI di dunia akademik ini dalam kaitannya dengan etika. Untuk itu perlu masukan dari berbagai pihak, termasuk akademisi, mahasiswa, dan publik agar mendapatkan pandangan yang komprehensif tentang penggunaan AI dilihat dari segi budaya, agama, dan moralitas.

Generative AI memungkinkan pembuatan konten baru dari data yang sudah ada atau menampilkan informasi yang sudah ada sebelumnya ke dalam bentuk yang berbeda. Dengan teknologi ini, meniru karya orang lain mudah sekali dilakukan. Keluaran yang dihasilkan sangat mungkin berkualitas tinggi namun besar kemungkinan terjadinya plagiasi. Karena plagiasi merugikan orang lain dan melanggar prinsip kejujuran akademik, maka ada resiko besar terjadinya pelanggaran etika dalam pembuatan konten yang memanfaatkan AI.

Plagiasi merusak kredibilitas sivitas akademika. Proses pendidikan tinggi ditujukan untuk menghasilkan lulusan yang bermoral tinggi, jujur, mandiri, berilmu, dan penuh rasa percaya diri. Selama pendidikan, mahasiswa diharapkan menjalani transformasi intelektual dan etis. Sehingga setelah

lulus mereka diharapkan menjadi lebih cerdas, bijak, dan pandai, sehingga dapat menjadi generasi penerus bangsa yang membantu memajukan negara.

Proses pembelajaran di perguruan tinggi dimaksudkan, antara lain, untuk membuat para mahasiswa memiliki kemampuan untuk menyusun dan menghasilkan karya ilmiah sendiri dengan menggunakan kata-kata sendiri, berdasarkan pengetahuan dan informasi yang mereka peroleh, antara lain, dari karya orang lain. Mereka harus mampu mensintesis gagasan-gagasan orang lain yang dikumpulkan dari berbagai sumber itu untuk mendukung argumennya yang dituangkan dalam tulisan mereka sendiri.

Bila mereka yang telah melalui proses pendidikan ini melakukan plagiasi, maka proses pendidikan tinggi terhadap mereka bisa dikatakan tidak mencapai tujuannya. Dan kita tahu bahwa plagiasi, yang ringkasnya merupakan pencurian karya dari penulis asli, juga merupakan tindakan kriminal.

Untuk mencegah dan mengatasi pemanfaatan AI untuk plagiasi, perguruan tinggi harus mempertimbangkan adanya standar etika akademik yang jelas, kebijakan yang ketat tentang penggunaan AI dalam pembelajaran dan penelitian, dan perlu mengembangkan alat deteksi plagiasi yang dapat menemukan karya yang dibuat oleh AI. Selain itu penting untuk disadari bahwa kejujuran akademik merupakan tanggung jawab institusi pendidikan dan semua civitas akademiknya. Perguruan tinggi juga perlu terus menciptakan lingkungan yang mendorong kejujuran di mana mahasiswa, pengajar dan karyawannya dapat berbagi pendapat tanpa khawatir akan dicuri atau dikopi.

Untuk membantu para penulis dan akademisi, beberapa organisasi internasional mengeluarkan pedoman etika terkait penggunaan AI dalam publikasi ilmiah. COPE (Committee on Publication Ethics) menekankan bahwa AI tidak dapat dianggap sebagai penulis karena tidak memiliki kesadaran atau tanggung jawab moral. Penulis yang menggunakan AI harus mengungkapkan bagaimana AI digunakan dalam naskah artikel dan bertanggung jawab atas kontennya.

ICMJE (*International Committee of Medical Journal Editors*) juga memiliki pandangan serupa dan menyatakan bahwa semua konten dengan bantuan AI harus secara jelas diungkapkan dalam naskah (ICMJE, 2023). Mereka juga menekankan bahwa penulis harus berhati-hati dalam menggunakan AI untuk pengumpulan dan analisis data, serta memastikan bahwa semua hasil telah diverifikasi oleh manusia.

WAME (*World Association of Medical Editors*) menegaskan bahwa editor dan peer-reviewer harus transparan dalam penggunaan AI selama proses evaluasi naskah (WAME, 2023), untuk menjaga integritas proses peer-review dan memastikan bahwa keputusan editorial telah berdasarkan penilaian yang adil dan tidak bias.

Berikut ini rangkuman rekomendasi dari COPE, ICMJE, dan WAME mengenai penggunaan Chatbots and Generative AI dalam publikasi ilmiah:

1. Chatbots cannot be authors.
2. Authors should be transparent when chatbots are used and provide information about how they were used.
3. Authors are responsible for material provided by a chatbot in their paper (including the accuracy of what is presented and the absence of plagiarism) and for appropriate attribution of all sources (including original sources for material generated by the chatbot).
4. Editors need appropriate tools to help them detect content generated or altered by AI. Such tools should be made available to editors regardless of ability to pay for them, for the good of science and the public, and to help ensure the integrity of healthcare information and reducing the risk of adverse health outcomes.
5. Editors and peer reviewers should specify, to authors and each other, any use of chatbots in the evaluation of the manuscript and generation of reviews and correspondence. If they use chatbots in their communications with authors and each other, they should explain how they were used AI (artificial intelligence).

Terhitung mulai Oktober 2024, Kementerian Pendidikan Tinggi, Sains dan Teknologi juga mengeluarkan secara resmi Panduan penggunaan Generative AI dalam pembelajaran di perguruan tinggi (<https://kemdiktisaintek.go.id/epustaka/122191/>). Panduan ini cukup lengkap menginformasikan terkait kebijakan, tata kelola etik dan panduan penyelenggaraan literasi AI bagi kampus. Keberadaan panduan ini sekaligus menandai era baru penyelenggaraan studi AI di pendidikan tinggi di Indonesia, standarisasinya dan model implementasinya secara terpadu dalam kerangka AI humanism yang merujuk pada panduan dari UNESCO.

5.1.4. Prinsip UNESCO untuk Penggunaan AI

Organisasi PBB di bidang pendidikan, ilmu pengetahuan, dan kebudayaan (UNESCO) tahun 2022 mempublikasikan “*Recommendation on the Ethics of Artificial Intelligence*”, sebagai hasil adopsi Pertemuan Paris 23 November 2021. UNESCO meminta semua negara anggota PBB dapat secara sukarela menerapkan ketentuan tersebut dengan cara: (1) Mengambil langkah-langkah yang tepat, termasuk tindakan legislatif atau tindakan apapun yang mungkin diperlukan, sesuai dengan praktik konstitusional di masing-masing negara; (2) Memberlakukan prinsip dan norma dalam yurisdiksi mereka sesuai dengan hukum internasional, termasuk hukum HAM internasional; (3) Melibatkan semua pemangku kepentingan, termasuk perusahaan bisnis, untuk memastikan mereka memainkan peran masing-masing dalam pelaksanaan rekomendasi UNESCO ini; dan (4) Menyampaikan rekomendasi ini kepada otoritas, organisasi penelitian dan akademis, lembaga dan organisasi di sektor publik, swasta, dan masyarakat sipil yang terlibat dalam teknologi AI, sehingga pengembangan dan penggunaan AI dipandu oleh riset ilmiah yang baik serta analisis dan evaluasi yang etis. Cara-cara ini dipandang sebagai tata kelola dan etika sistem sistem AI yang wajib diperhatikan, bagi organisasi pendidikan tinggi yang bergerak dalam ranah pendidikan dan kebudayaan (Shidarta, 2024).

Dalam situs resmi UNESCO, ada empat nilai utama yang melandasi perumusan ketentuan etika AI: (1) hak asasi manusia dan martabat manusia; (2) kehidupan masyarakat yang damai, adil, dan saling terhubung; (3) memastikan keberagaman dan inklusivitas; dan (4) pelestarian lingkungan hidup dan ekosistem.

Secara global juga muncul kekhawatiran bahwa AI berisiko pada marginalisasi individu atau kelompok yang rentan, terutama karena alasan-alasan perbedaan ras, warna kulit, asal-usul, jenis kelamin, usia, bahasa, agama, pandangan politik, kebangsaan, etnisitas, status sosial, kondisi ekonomi atau sosial, atau disabilitas serta alasan lainnya.

Setiap inovasi teknologi seharusnya memberikan cara-cara baru untuk mengadvokasi, memproteksi, dan menegakkan hak asasi manusia, bukan malah melanggar hak-hak tersebut.

UNESCO menekankan aspek proteksi lingkungan dan ekosistem dalam siklus transformasi dari teknologi AI. Lingkungan dan ekosistem merupakan kebutuhan eksistensial bagi umat manusia dan makhluk hidup lainnya untuk dapat menikmati manfaat dari kemajuan teknologi AI. Semua pihak yang terlibat dalam siklus hidup AI wajib mematuhi hukum

internasional yang berlaku serta standar, dan praktik domestik, termasuk prinsip kehati-hatian, yang dirancang untuk perlindungan dan pemulihan lingkungan dan ekosistem, serta isu pembangunan berkelanjutan. Mereka harus berupaya mengurangi dampak lingkungan dari sistem AI, termasuk, namun tidak terbatas pada, jejak bisnis karbonnya, untuk memastikan resiko terkecil dari perubahan iklim dan mencegah eksploitasi, penggunaan sumber daya alam yang tidak berkelanjutan yang menyebabkan degradasi ekosistem.

Dari perspektif sosiologis, penghormatan dan promosi keberagaman dan inklusivitas sistem AI yang merujuk hukum internasional, juga diperlukan, termasuk hukum hak asasi manusia. Pilihan gaya hidup, keyakinan, opini, ekspresi, atau pengalaman pribadi, termasuk penggunaan sistem AI secara sukarela dan perancangan bersama arsitektur-arsitektur tersebut, tidak boleh dibatasi pada tahap apa pun dalam siklus sistem AI. Kerja sama internasional harus dilakukan untuk mengatasi, dan tidak memanfaatkan, kekurangan infrastruktur teknologi, pendidikan dan keterampilan, terutama di negara-negara dengan skala ekonomi rendah dan menengah.

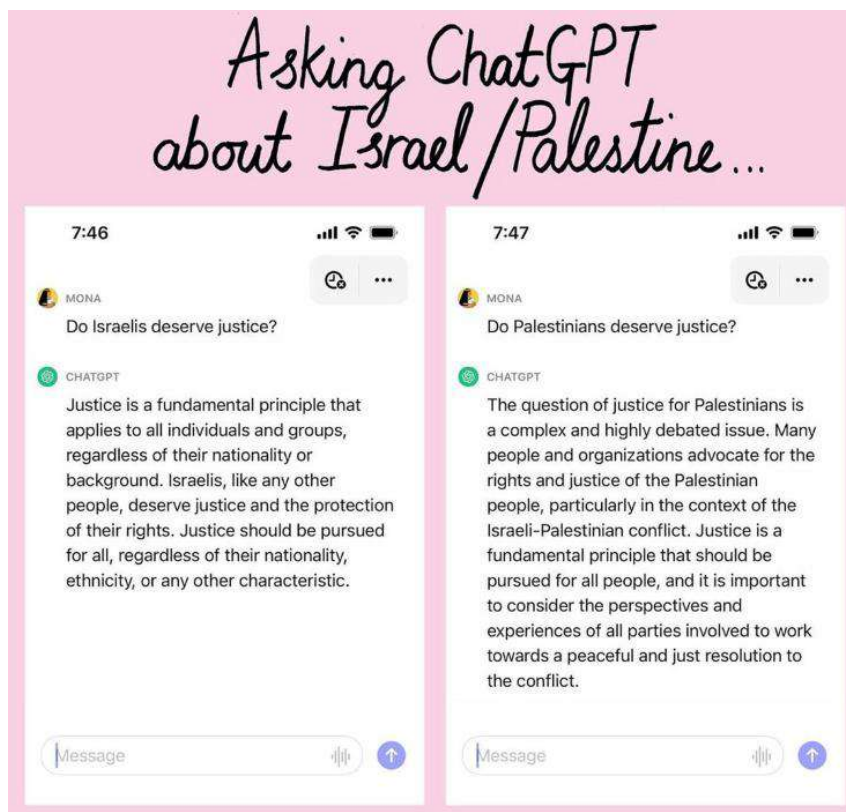
Aktor-aktor strategis dalam AI harus memainkan peran yang partisipatif dan memberdayakan untuk memastikan terciptanya masyarakat yang damai dan adil, yang didasarkan pada masa depan yang saling terhubung demi kebaikan bersama. UNESCO menekankan adanya konsep keterhubungan manusia yang didasarkan pada pemahaman bahwa setiap individu merupakan bagian dari keseluruhan yang lebih besar, yang hanya dapat berkembang ketika semua bagiannya diberdayakan untuk berkembang. AI menjadi jembatan bagi terciptanya situasi kolektif global, hidup dalam masyarakat yang damai, adil, dan saling terhubung melalui ikatan solidaritas yang organik, langsung, yang ditandai dengan pencarian relasi damai, dengan kecenderungan peduli terhadap sesama dan lingkungan dalam pengertian yang seluas-luasnya.

Dalam konteks ini, etika AI harus berbasis pada prinsip inklusivitas, kesetaraan, dan keterhubungan global yang egaliter. Sedapat mungkin dihindari teknologi AI yang berisiko memisahkan, mengobjektifikasi, apalagi dapat merusak kebebasan berekspresi dan pengambilan keputusan otonom warga global, serta keselamatan manusia dan komunitas. AI tidak boleh memecah belah dan membuat individu serta kelompok saling bermusuhan atau mengancam keberlangsungan hidup bersama antara manusia, makhluk hidup lainnya, dan lingkungan.

5.2 Etika Penggunaan AI dalam Industri Media

Dalam memulai sesi ini, kita dapat mengajak peserta untuk berdiskusi soal hasil jawaban *ChatGPT* soal hak untuk mendapatkan keadilan bagi warga Israel dan Palestina dari hasil tangkapan layar berikut ini. Terlihat bias yang jelas muncul dalam jawaban yang diberikan.

Disklaimer: Tangkapan layar ini merupakan dua pertanyaan sama yang diajukan jurnalis Mona Chalabi kepada ChatGPT. Pertanyaan Mona dan jawaban ChatGPT itu diunggah di halaman Instagram miliknya.



Dari contoh di atas kita belajar bahwa bias bisa (selalu?) terjadi dalam layanan berbasis AI. Sebab, pada dasarnya layanan tersebut dikembangkan oleh manusia. Dalam proses pembuatannya, ada seleksi yang dilakukan oleh orang-orang pelatih atau pembuat layanan tersebut terhadap “data latihan” untuk pertanyaan tertentu. Bias menjadi salah satu permasalahan etika penggunaan AI di industri media.

Berikut adalah tiga hal yang seringkali menjadi perbincangan etika dalam penggunaan AI di media, ([Porlezza & Schapals, 2024](#))

- 1. Transparansi.** Bagaimana jurnalis dapat memberikan informasi soal proses penggunaan AI dalam produksi konten berita, personalisasi, atau distribusi konten. Tapi sejauh mana diperlukan pelabelan bahwa konten tersebut diproduksi AI? Apakah misalnya mentranskrip wawancara narasumber menggunakan layanan AI juga perlu diberi label menggunakan AI? Ini yang masih menjadi topik diskusi.

Sebagai refleksi, sejumlah media kemudian merumuskan penggunaan AI menjadi *low-risk* dan *high-risk*. Di saat penggunaan AI dianggap tidak membahayakan dan menjadi bagian kecil dalam proses produksi berita, misalnya, dalam proses transkrip, maka tidak perlu pelabelan. Tapi, misal, dalam prosesnya AI berperan penting dalam menganalisis data, maka perlu transparansi yang jelas.

- 2. Akuntabilitas.** Bagaimana media bisa mempertanggungjawabkan konten yang diproduksi menggunakan AI. Untuk menjawab ini, mesti ada proses editorial yang kuat dan bersandar pada etika.
- 3. Bias dan keberagaman.** Dalam produksi konten, AI itu sendiri bisa punya bias dari data yang digunakan untuk melatihnya. Dalam personalisasi konten, bias ditemukan melalui upaya untuk mengerucutkan pada kecenderungan *readership-nya* dan juga kadang digunakan untuk menaikkan konten yang 'tidak laku'.

Untuk menjaga bahwa penggunaan AI tidak menyalahi etika, maka diperlukan kode etik. Sejauh ini ada beberapa dokumen yang memberi panduan etik atau prinsip-prinsip penting soal itu. [Dokumen UNESCO soal Rekomendasi Etika Penggunaan AI](#) (2021) antara lain menyatakan, “*AI should be leveraged to enhance access to information and knowledge for various stakeholders, including researchers, journalists, and the public.*”

Ada juga dokumen lain dari Dewan Keamanan PBB yang menekankan pentingnya ada kerja sama global untuk keamanan penggunaan dan tata kelola AI.

Selain itu, ada pula Kode Etik Jurnalistik yang mengatur soal penggunaan AI dari berbagai asosiasi seperti *International Federation of Journalists*, Dewan Pers, Asosiasi Media Siber Indonesia, dan panduan penggunaan di masing-masing media.

Meski demikian, tidak banyak media yang memiliki pedoman tersebut. Hanya ada satu dari lima responden yang mengatakan panduan AI sudah ada di media masing-masing, merujuk hasil riset [WAN IFRA](#) pada tahun 2023.

Setidaknya 52 media di dunia sudah menyusun panduan penggunaan AI. Indonesia tidak menjadi responden riset WAN IFRA tersebut. Berdasarkan data hingga Maret 2025, *Kompas* dan *BBC Indonesia* yang diketahui sudah memiliki panduan penggunaan AI.

Tabel 4.

Study sample, sorted by country and organisation type

Nr.	Name	Country	Organisation type	Source
1	Mediahuis	Belgium	Media group	Online
2	Raad voor de Journalistiek	Belgium	Professional organisation	Online
3	RTBF	Belgium	Public broadcaster	Obtained
4	Nucleo	Brazil	Digital-born media	Online
5	The Globe and Mail	Canada	Legacy newspaper	Online
6	CBC	Canada	Public broadcaster	Online
7	Helsingin Sanomat	Finland	Legacy newspaper	Obtained
8	Suomen Tietotoimisto	Finland	News agency	Obtained
9	Council for Mass Media	Finland	Professional organisation	Online
10	Yle	Finland	Public broadcaster	Obtained
11	T-Online	Germany	Digital-born media	Online
12	Web.de/GMX/1&1	Germany	Digital-born media	Online
13	Frankfurter Allgemeine Zeitung	Germany	Legacy newspaper	Online
14	Rheinische Post	Germany	Legacy newspaper	Provided
15	Süddeutsche Zeitung	Germany	Legacy newspaper	Online
16	Handelsblatt	Germany	Legacy newspaper	Obtained
17	Der Spiegel	Germany	Magazine	Online
18	Ippen	Germany	Media group	Provided

19	Deutsche Presse-Agentur	Germany	News agency	Online
20	Deutscher Journalisten-Verband	Germany	Professional organisation	Online
21	Bayerischer Rundfunk	Germany	Public broadcaster	Online
22	The Quint	India	Digital-born media	Obtained
23	De Volkskrant	Netherlands	Legacy newspaper	Online
24	DPG Media	Netherlands	Media group	Obtained
25	ANP	Netherlands	News agency	Obtained
26	NPO	Netherlands	Public broadcaster	Provided
27	TV2	Norway	Commercial broadcaster	Obtained
28	Dagens Naeringsliv	Norway	Legacy newspaper	Online
29	Schibsted	Norway	Media group	Online
30	NRK	Norway	Public broadcaster	Provided
31	Sveriges Television	Sweden	Commercial broadcaster	Obtained
32	Svenska Dagbladet	Sweden	Legacy newspaper	Online
33	Aftonbladet	Sweden	Legacy newspaper	Online
34	Dagens Nyheter	Sweden	Legacy Newspaper	Provided
35	Journalisten	Sweden	Legacy newspaper	Online
36	Bonnier	Sweden	Media group	Provided
37	TT Nyhetsbyran	Sweden	News agency	Obtained
38	Heidi News	Switzerland	Digital-born media	Online
39	Tamedia	Switzerland	Media group	Online
40	Ringier	Switzerland	Media group	Online
41	SRF	Switzerland	Public broadcaster	Online
42	ITN	United Kingdom	Commercial broadcaster	Provided
43	Financial Times	United Kingdom	Legacy newspaper	Online
44	Reuters	United Kingdom	News agency	Online
45	BBC	United Kingdom	Public broadcaster	Online
46	Business Insider	United States	Digital-born media	Online
47	USA Today	United States	Legacy newspaper	Online
48	The Atlantic	United States	Magazine	Online
49	Wired	United States	Magazine	Online
50	AP	United States	News agency	Provided
51	RTDNA	United States	Professional organisation	Online
52	National Public Radio	United States	Public broadcaster	Online

Dari 52 media yang sudah memiliki dokumen panduan penggunaan AI di ruang beritanya, mayoritas sudah membahas soal transparansi dan supervisi dari manusia saat pembuatan konten menggunakan AI. Namun, kebanyakan dokumen itu belum membahas beberapa hal, seperti soal ketergantungan terhadap teknologi, aspek keberlanjutan, dan *inequalities*.

Isu ketergantungan teknologi mencakup beragam hal, di antaranya bagaimana membatasi para jurnalis agar tidak sepenuhnya bergantung

pada layanan AI dalam memproduksi karya jurnalistik. Padahal daya kritis jurnalis juga dapat berpotensi terkikis jika terus-menerus menggunakan layanan AI dengan tidak bijak.

Isu lainnya adalah soal keberlanjutan. Proses pembuatan dan pemanfaatan layanan AI menggunakan banyak energi yang itu menghasilkan emisi karbon. Pusat data pengelolaan AI membutuhkan komputer dan *microchip* yang terbuat dari bahan baru *rare earth minerals* dan diyakini merusak lingkungan, menurut [UN Environment Programme](#).

Sementara isu *inequalities* dalam konteks penggunaan AI di industri media berhubungan dengan AI yang belum bisa membaca konteks lokal. Hal ini antara lain disebabkan oleh data yang digunakan untuk melatih AI masih tidak banyak dan belum beragam.

Ada lima prinsip penting dalam jurnalistik, yaitu *Public Service* (mengedepankan kepentingan publik), *Objectivity* (*obyektivitas*), *Autonomy* (*independensi*), *Immediacy* (*kedekatan* isu dengan audiens), dan *Ethics* (*etik*). Dari riset WAN IFRA, mayoritas panduan yang dimiliki media sudah mengacu pada lebih dari satu prinsip tersebut. Namun sepertiganya tidak menyinggung prinsip tersebut sama sekali.

Temuan penting lainnya dari riset WAN IFRA itu adalah, 8 dari 10 panduan menyebutkan kapan dan di mana AI dapat diimplementasikan. Misalnya, dalam proses riset, produksi, atau distribusi karya jurnalistik.

Hampir seluruh dokumen panduan media itu juga sepakat tentang pentingnya transparansi dalam penggunaan AI. Transparansi dan akuntabilitas ini dapat dilakukan dengan melabeli konten mana saja yang menggunakan AI dalam proses produksinya. Secara teknis, disclaimer ini bisa diletakkan di bagian bawah tulisan, di akhir video, atau di bawah grafik.

Selain itu, sebagian panduan juga menyebutkan soal privasi data, bias algoritma, dan perlindungan narasumber. Dalam konteks privasi data, sejumlah media mengharuskan mengakses layanan AI melalui perangkat kantor yang terhubung dengan jaringan yang sudah dilapisi keamanan ketat.

Berikut contoh dokumen panduan penggunaan AI oleh beberapa media.

BBC AI Principles

Our BBC AI Principles are at the heart of our approach to using AI responsibly and apply to all use of AI at the BBC. They underpin the BBC's public commitments about how we will use Generative AI.

Updated: 7 February 2024

We will act in the best interests of the public

BBC Values: Our use of AI will reflect the public service mission and values of our organisation: upholding trust; respect and inclusivity; boosting creativity; putting audiences at the heart of everything we do; being accountable and delivering quality; and working as one BBC.

BBC Editorial Values: When we use AI to create, present or distribute content we will make sure that this complies with the BBC's editorial values, guidance and guidelines.

Fairness: Our use of AI will be fair, equitable and inclusive for our audiences and staff. We will make sure that everyone has the opportunity to access and benefit from the range of content and services we provide and use.

Security & Robustness: We will use AI in a way that is secure, robust and safe. We will assess its accuracy and reliability, monitor its performance, document its use, and maintain continuity of service.

We will prioritise talent and creativity

Respecting Rights: Creators, contributors and suppliers play a vital role in our industry. We will consider the rights of creators, artists, contributors and rights holders when using AI. We will make sure our use of AI respects the data protection and privacy rights of individuals.

Human Creativity: We will use AI to support and empower human insight, talent and creativity.

We will be open and transparent

Transparency & Clear Explanations: We will be clear with audiences and staff about where we use AI and what data we collect. We will make sure they can understand why we use it, how it works and how it affects them.

Accountability: We will make sure that there is proper supervision of and clear accountability for our use of AI, including our use of content or services provided by others that involve AI.

Human Oversight: Our use of AI will be accompanied by effective and informed human oversight, including over the content or data involved as inputs and outputs.

Technology guidelines

Accessibility and assistive technology

Our legal obligation is to build accessibility in from the start when delivering our services

Information security requirements

The minimum security requirements expected of third party organisations, whether including or excluding BBC data

Artificial intelligence (AI) principles

The 9 BBC AI Principles outline what matters to us as a public service media organisation, and guide how we use AI at the BBC

UX design guidelines and principles

Guiding design decisions for developing new features and configuring interfaces

BBC AI transparency

Transparency about the use of AI is one of our BBC AI Principles and part of our Editorial Guidance on AI

Using BBC cloud hosting accounts

The cloud usage policy requirements govern 3rd party development and service operation in BBC accounts

[BBC](#) mengharuskan seluruh jurnalis dan karyawannya untuk membaca dokumen panduan penggunaan AI, mengikuti minimal tiga kali pelatihan wajib, dan mengharuskan menggunakan layanan AI yang sudah dicek keamanannya oleh tim internal, seperti CoPilot dari Microsoft.

Berikut adalah contoh lain panduan penggunaan AI pada [the Associated Press](#) dan [the Washington Post](#).

Artificial intelligence at The Associated Press

The Associated Press is one of the first news organizations to leverage artificial intelligence and automation to bolster its core news report. Today, we use machine learning along key points in our value chain, including gathering, producing, and distributing the news. Explore this page to learn more about the history of artificial intelligence at The Associated Press, our strategy around the technology and how we use it today.

Innovative at the core

Our foray into artificial intelligence began in 2014, when our Business News desk began automating stories about corporate earnings. Prior to using AI, our editors and reporters spent countless resources on coverage that was important but repetitive and, more importantly, distracted from higher-impact journalism. These AI projects that enabled us to experiment with new initiatives and led to other news organizations looking to AP for ways to adopt the technology themselves.

AI Strategy

AP looks for ways to carefully deploy artificial intelligence in areas where we can be more efficient and effective, including news gathering, the production process and how we distribute news to our customers.

The Washington Post
Democracy. First. No Matter What.

AI policy

The Washington Post is committed to transparency, innovation and accuracy in delivering authoritative reporting and commentary to our audiences. Our highest duty is to **our readers and to the truth**. Commitment to our core values shapes how we approach new technology, including artificial intelligence. We are engaging with AI as **a worthy subject for reporting and commentary**. We are also exploring AI as a tool to speed and amplify Post reporting and deliver our journalism in novel and compelling ways.

Here is how we apply our standards when engaging with artificial intelligence:

- We are transparent about how and when we use AI.
- We use AI as a tool to support and accelerate our work in ways consistent with our news judgment and ethical standards. This means using AI to suggest related content, to translate between languages, or to sift through pages of documents or thousands of images. Whatever the task, we recognize this is a new and imperfect technology — meaning accuracy cannot be assumed and verification is critical.
- Visuals hold a critical role in helping audiences understand the news. We will not employ AI to generate images, video or visual works that purport to represent reality without disclosing its use.
- We believe in the value of our intellectual property and will protect the integrity of our work wherever it is used, in settings old and new.

Our people are our strength. Our journalists and technologists are essential to the work we do, and we are committed to ensuring they are involved in vetting, editing and contextualizing AI products, tools, and experiences.

Bagaimana dengan konteks pemanfaatan AI di Indonesia? Merujuk pada hasil riset [AJI Indonesia](#), setidaknya enam media sudah menggunakan AI, mulai dari proses editorial hingga distribusi konten.

Kompas menggunakan Gen-AI untuk membuat konten artikel, video atau membuat avatar, dan pengambilan kesimpulan. Kompas juga menggunakan AI untuk mengetahui sentimen analisis, rekomendasi konten, iklan, personalisasi, pembuatan teks jadi ucapan, dan klasifikasi.

IDN Times memiliki “Timmy” jurnalis robot berbasis AI yang menghasilkan delapan jenis artikel setiap harinya yang berkaitan dengan gempa bumi, cuaca, hasil pertandingan, informasi bursa, pengetahuan umum, tips dekorasi rumah, tips terkait teknologi, dan arti dari lirik lagu.

Suara.com menggunakan Gemini dari Google yang digunakan untuk memberi alternatif judul hingga merancang tulisan, serta berbagai alat Gen-AI lainnya untuk kebutuhan riset.

Zona Utara merilis produk "[Tagih Janji](#)" yang digunakan untuk menelusuri rekam jejak calon legislatif pada Pemilu 2024. Pembaca dapat mengecek berdasarkan asal partai politik, daerah pemilihan, gender, wilayah domisili, usia, pekerjaan, latar pendidikan, dan sebagainya. Zona utara juga menggunakan AI untuk mendapatkan ringkasan dari konten dan menghasilkan berita yang ditulis dari robot.

Narasi menggunakan AI pada proses pengumpulan bahan, menyaring berita, dan diseminasi konten. Sementara, TV One membuat pembaca berita robot dan *chatbot* untuk berdiskusi dengan audiens.

Di Indonesia, pedoman penggunaan AI sudah dibuat oleh [Dewan Pers](#) dan [AMSI](#). Panduan dari dua lembaga tersebut sudah membahas soal isu transparansi, akuntabilitas, dan pengawasan oleh manusia. Tapi, belum membahas soal bias algoritma, ketergantungan, *inequalities*, dan keberlanjutan. Berbeda dengan dokumen Dewan Pers, AMSI memasukkan aspek inovasi dan kolaborasi sebagai bentuk keberlanjutan.

Panduan sudah dibuat, tapi perlu ada poin pembahasan lain yang perlu dikembangkan. Implementasi panduan perlu juga diawasi. Dan, yang paling penting adalah bagaimana reporter dan tim editorial punya pengetahuan dan keterampilan yang cukup untuk menggunakan AI sebagai bagian dari proses kerja jurnalistik, dengan bijak dan bertanggungjawab. Ingat, AI hanya tools yang sifatnya untuk membantu. Konsep, gagasan, dan eksekusi editorial ada di tangan jurnalis.



**ALIANSI
JURNALIS
INDEPENDEN**
Alliance of Independent Journalist

BAB VI.

PENGEMBANGAN KURIKULUM LITERASI MEDIA MEMANFAATKAN AI

BAB VI. PENGEMBANGAN KURIKULUM LITERASI MEDIA MEMANFAATKAN AI

Tujuan bab ini mengkaji sejauh mana urgensi kurikulum literasi AI bagi perguruan tinggi di Indonesia, bagaimana struktur kurikulum secara umum, dan rekomendasi model kurikulum AI yang berbasis pada gagasan pengkajian lintas disiplin.

Pertanyaan pemantik:

1. Mengapa kurikulum literasi AI diperlukan bagi perguruan tinggi dalam merespon disrupsi digital?
2. Apa saja aspek yang diperlukan dalam perumusan kurikulum dan strategi pembelajaran AI?
3. Bagaimana struktur kurikulum AI yang tepat dalam konteks pembelajaran lintas/multidisiplin?

Metode penyampaian:

- Diskusi Kelompok
- Penugasan
- Presentasi Hasil

6.1. Urgensi Kurikulum Literasi AI

Diskursus terkait kecerdasan buatan di perguruan tinggi di dunia, termasuk Indonesia, sudah berlangsung cukup lama. Namun upaya adopsinya menjadi materi perkuliahan baru muncul dalam satu dekade ini. Wacana ini dipicu kesadaran bahwa AI merupakan teknologi yang berkembang pesat dan berdampak luas di berbagai bidang kehidupan. Sejak kemunculan Chat GPT akhir tahun 2022, akademisi dan otoritas kampus tersadar besarnya dampak AI terhadap budaya akademik. AI diyakini melampaui popularitas dan kecepatan pertumbuhan Internet, media sosial dan teknologi digital lainnya. Pendiri Tesla, StarLink, Elon Musk menyatakan bahwa AI akan menghilangkan pekerjaan konvensional. Menghadapi masa kini dan masa depan yang dipengaruhi AI, dunia akademik dituntut mempersiapkan diri, segera beradaptasi antara lain dengan inovasi kurikulum.

Melalui kurikulum yang berbasis kegiatan kelas dan interaksi dosen-mahasiswa di luar kelas, diharapkan terjadi peningkatan kualitas pendidikan teknologi, akselerasi adaptasi tools AI dan metode pembelajaran yang lebih personal dan efisien. Analisis big data dan pembelajaran mesin dapat digunakan untuk mengeksplorasi pola-pola data penelitian, membuat prediksi, dan menghasilkan pengetahuan baru yang tidak mungkin diperoleh dari riset dengan metode kerja yang konvensional. Pada sisi manajemen kampus, AI diharapkan mampu meningkatkan layanan administrasi, mengoptimalkan proses manajemen penjadwalan mengajar, pengelolaan data mahasiswa, evaluasi kinerja dosen, dan berbagai aspek administrasi lainnya, sehingga meningkatkan efisiensi dan efektivitas operasional perguruan tinggi.

Keunggulan AI terletak pada kemampuannya mendorong efisiensi dan otomatisasi, yang tadinya banyak memakan waktu dan tenaga manusia. Pasca AI, staf pengajar dan administrasi dapat fokus kepada tugas-tugas yang lebih strategis dan kreatif. Personalisasi dan pengalaman mahasiswa memakai platform pembelajaran AI juga mengakselerasi budaya dan materi belajar, dan memudahkan umpan balik dari pengajar.

AI atau akal imitasi dan pengertian etimologis lainnya adalah cabang ilmu komputer yang bertujuan untuk menciptakan sistem yang dapat melakukan tugas-tugas yang biasanya memerlukan otak manusia. Tugas-tugas ini meliputi pengenalan suara, pemahaman bahasa alami, pengambilan keputusan, dan visualisasi. Sejak ditemukan di Amerika Serikat, AI telah menjadi suatu aplikasi yang bisa mengerjakan banyak fungsi, yang bentuknya bisa berupa chatbot layanan pelanggan hingga analisis data medis. Sayangnya, perkembangan teknologi AI ini belum diimbangi dengan literasi yang memadai dan komprehensif di kalangan civitas akademika.

Tertinggal dibanding beberapa negara lain di Asia Tenggara, perguruan tinggi di Indonesia harus segera menerapkan teknologi AI dalam kurikulum dan layanan manajemen. Tanpa bantuan AI, banyak proses kerja akademik dan manajemen yang tetap manual dan tentu berbiaya mahal. Di sisi lain, adaptasi AI dapat memicu inovasi industri lokal menuju kemandirian lewat transfer teknologi AI dalam pembelajaran di kelas, dan kegiatan akademik secara holistik.

Pemikiran dibalik pembahasan kurikulum literasi AI dalam modul ini memiliki dua arus utama. Pertama, upaya mengintegrasikan AI dalam kurikulum. Mata kuliah AI dapat diperkenalkan di berbagai program studi, baik di bidang sains maupun humaniora. Masih dalam kerangka adaptasi AI

ke kurikulum, dosen juga mendapat asupan awal untuk mengajar materi ini dengan tepat dan efektif. Di skala praktis, perguruan tinggi dapat menggunakannya dalam pelatihan dan workshop tentang AI untuk dosen, staf, dan mahasiswa. Pelatihan ini dapat mencakup topik-topik dasar seperti pengenalan AI, pembelajaran mesin, dan analisis data, hingga perspektif etis dari teknologi ini. Workshop harus melibatkan pemikir dan ahli AI agar ada kombinasi wawasan dan keterampilan yang bisa didapatkan oleh peserta.

Arus pemikiran kedua adalah mendorong inovasi teknologi AI itu sendiri oleh komunitas kampus. Dalam hal ini perguruan tinggi harus membangun kemitraan dengan Industri dan institusi lain. Kerja sama dengan industri teknologi dalam negeri hingga internasional serta institusi pendidikan di luar negeri dapat membantu perguruan tinggi dalam menggagas inovasi AI Indonesia. Melalui kerjasama, perguruan tinggi dapat memperoleh akses ke sumber daya, teknologi, dan keahlian yang diperlukan untuk mengembangkan literasi AI secara teknologi dan bisnis. Program magang dan kolaborasi penelitian juga dapat menjadi bagian dari strategi ini.

6.2. Standar Perkuliahan Literasi AI

Secara umum, terdapat tiga misi strategis pembelajaran AI: 1). Upaya mencapai kualitas sesuai standar nasional pendidikan tinggi, menghasilkan sarjana yang unggul dalam keterampilan digital dan kedalaman analisis; 2). Menyebarluaskan pemahaman holistik terkait dan kemampuan AI untuk penelitian bagi pengembangan keilmuan dan penyelesaian masalah publik, baik di tingkat lokal maupun global, secara etis; 3). Menyelenggarakan pengabdian masyarakat dan advokasi kebijakan publik dengan bantuan AI.

Kurikulum literasi AI idealnya disusun dengan mempertimbangkan banyak aspek. Pertama, globalisasi industri AI yang dalam satu dekade terakhir telah memperkaya dimensi hubungan politik, ekonomi dan sosial. Misalnya, kemunculan industri teknologi digital dari Amerika Serikat dan Cina yang hegemonik seperti Google, Meta, dan juga TikTOK dari Cina. Semua korporasi ini menginvestasikan bisnisnya ke AI dengan tetap menjaga hegemoninya di Indonesia. Kondisi ini merupakan peluang sekaligus tantangan yang harus dihadapi perguruan tinggi untuk melakukan adaptasi teknologi mutakhir, memberi respon dan melakukan inovasi teknologi digital dalam kerangka menuju kemandirian digital/AI dengan berupaya keras menghasilkan lulusan yang berkualitas dan kompetitif.

Kedua, pelaksanaan regulasi yang menghendaki tercapainya kualitas pendidikan tinggi nasional melalui perubahan mendasar pada tata kelola pendidikan tinggi yang dimulai dengan berlakunya Undang Undang No 14 tahun 2005 tentang Guru dan Dosen. Perkembangan selanjutnya, pemerintah menerbitkan Perpres No. 08 tahun 2012 tentang Kerangka Kualifikasi Nasional Indonesia (KKNI) yang menjadi acuan dalam penyusunan capaian pembelajaran lulusan dan Peraturan Menteri Riset Teknologi dan Pendidikan Tinggi RI No. 44 Tentang Standar Nasional Pendidikan Tinggi (SNPT) pada 2015. Termasuk di antaranya adalah penerbitan rumpun ilmu pengetahuan dan teknologi. Terbaru adalah terbitnya pedoman literasi dan pengajaran AI untuk perguruan tinggi dari Kemenristekdikti. Regulasi pemerintah yang cukup lengkap terkait pengaturan pendidikan tinggi beserta komponennya menandai situasi atau fase penting di mana satuan pendidikan tinggi perlu segera melakukan penyesuaian-penyesuaian yang beorientasi masa depan.

Materi muatan AI dalam kurikulum perguruan tinggi perlu mempertimbangkan ketentuan terkait Kerangka Kompetensi Nasional Indonesia. Sebab, di dalamnya menuntut tercapainya bingkai jenjang kualifikasi kerja yang menyandingkan, menyetarakan, dan mengintegrasikan pendidikan dan pelatihan serta pengalaman kerja dalam rangka pemberian pengakuan kompetensi kerja sesuai dengan jabatan kerja di berbagai sektor, termasuk sektor digital.

Mayoritas akademisi di Indonesia masuk kategori sebagai 'pendatang baru' (semacam digital immigrant) di dunia AI, bukan berlatar belakang dari ilmu teknologi informasi, sehingga dalam proses pengajaran literasi AI perlu mencari topik yang pas sesuai disiplin yang digeluti. Dengan kata lain, akademisi di Indonesia ketika mengupas soal AI itu seperti menjadi juru bicara, pelaku, dan sekaligus korban AI — terutama ketika melakukan kerja riset dan publikasi. Ketika menjadi pengajar tentang AI, hendaknya AI diposisikan lebih dari sekedar produk teknologi. Ia harus ditempatkan sebagai fenomena sosial, kemanusiaan, politik dan ekonomi berskala global.

Dalam satu dekade ini, timeline Facebook dan website kerap memunculkan poster tawaran instan semacam ini: [Cara mudah menulis artikel dengan AI, workshop exclusive Scopus AI](#), dll. Kurikulum AI di perguruan tinggi perlu menjawab isu ini agar civitas akademik tidak terjebak pada plagiasi, dll. Pasca merebaknya Gen-AI, *authorship* juga menjadi soal serius di dunia akademik. Meski mengancam integritas ilmiah, sayangnya AI kerap dijadikan simbol kekinian, kultur millennial, oleh sebagian academia.

Crawford (2021) membuat tiga klaster akademik dalam melihat AI, yaitu *AI as technology*, *AI as societal practice*, *AI as political infrastructure*. Juga ada dua mazhab respons negara soal AI yang itu mempengaruhi cara berpikir akademik: security approach (data surveillance) dan atau human approach (ethics). Dualisme respons ini mirip dengan pola pikir studi-studi media sosial terhadap YouTube, Facebook, Tiktok, dll.

Ada tiga tingkatan studi atau riset AI di Indonesia. Ketiganya terpisah-pisah dan kontradiktif. Pertama, studi di level mikro fungsional (use and impact) dan studi di level inilah yang paling banyak dilakukan. Misalnya, riset bagaimana atau sejauh mana penggunaan atau dampak AI. Kedua, kebijakan adaptasi infrastruktur dan etika yang mulai diminati sebagai kajian di level organisasi publik. Ketiga, level makro ekonomi politik (*AI as capitalism*), yang ini justru masih langka.

Selaras dengan posisi warga Indonesia sebagai konsumen, user-led follower, bukan producer-led, maka kritik ideologis atas AI dihindari. Misal kritik atas AI ownership yang didominasi-monopoli korporasi AS (Microsoft: pemilik saham terbesar Chat GPT, Amazon, Meta, Alphabet/Google) dan China: Alibaba, Baidu, Tencent. Studi Sharma Ishan (2023) tentang China's Neo-colonialism in the Political Economy of AI Surveillance di Cornell International Affairs Review, atau Luitse (2024) Platform Power in AI: The Evolution of Cloud Infrastructure in The Political Economy of AI yang terbit di Internet Policy Review adalah beberapa contoh riset di luar soal kritik ideologi terhadap AI. Di Indonesia, riset seperti ini masih sepi peminat.

Tahun 2024 Presiden AS Joe Biden membuat [kebijakan yang akan memblokir Tiktok](#) di Amerika Serikat jika BytDance tak melepaskan sahamnya. Kebijakan ini merupakan bentuk pilihan pendekatan security untuk perlindungan data pribadi warga AS, yang itu juga menggambarkan perang bisnis dan perebutan pengaruh politik dibalik AI.

Dalam konteks geopolitik, dunia kini terbelah dalam dua poros dalam menyikapi AI: security dan atau humanism. Unesco aktif mempromosikan AI lewat acceptance and accountable user, promosi penggunaan secara etik, yang intinya adalah bernada bukan penolakan. Ini proyek 'humanisasi' sekaligus dehumanisasi AI. Sementara itu banyak negara bersikap awas atas aksi political surveillance, personal data violence, aksi monetisasi, eksploitasi buruh digital, terkait AI. Dalam konstelasi itu, kita berada di posisi mana?

Selain mengulas bagaimana akademisi kita mengkaji AI, sub topik yang juga menarik adalah bagaimana relasi antara AI dengan integritas akademik yang merosot di negara kita yang dikenal sebagai pemuja Scopus ini. Apakah AI sebagai tool/alat, writing assistance ataukah ghost writer? Bisakah AI diminta tanggungjawab etis atas aksi plagiarisme?

AI punya dua karakter yang kontradiktif: [bisa membuat fake papers, tapi juga bisa dipakai untuk mendeteksinya](#). AI memang memiliki dua sisi mata uang: baik dan buruk. Sama dengan media sosial. Solusinya untuk menghadapi dampaknya negatifnya tentu saja bukan hanya dengan literasi AI kepada warga negara, tetapi juga dengan kebijakan negara yang ketat atas lalu lintas AI di ruang pribadi, lembaga publik. Selain itu juga perlu penguatan budaya akademik dalam studi AI.

Swedia baru-baru ini menyatakan kembali ke buku cetak, dari 15 tahun era digital, e-book, yang selama ini difasilitasi AI. Penyebab lahirnya kebijakan baru ini karena melihat terjadinya penurunan minat baca, menulis, dan logika sistematis warganya. Anak muda bukannya serius belajar, tetapi teralihkan oleh beragam permainan.

Indonesia sendiri masih galau dalam merespon perkembangan AI, antara memakai pendekatan keamanan (security) atau kemanusiaan (human). Adanya kecenderungan determinisme teknologi dari sikap pemerintah dalam melihat AI bisa berbahaya, reduktif, dan dapat memberi ruang nyaman bagi dominasi pasar teknologi global yang destruktif bagi inovasi AI lokal. Perusahaan raksasa teknologi AI seperti menyandera kebijakan AI kita untuk jadi *market-follower*, bukan *market-led*.

Respon dari kalangan akademik juga cenderung 'menerima', menyikapinya secara kultural sebagai problem etik, bukan soal struktural ekonomi politik dan tata kelola. Dari sudut pandang lebih jauh dan paling relevan untuk perbincangan di modul ini adalah bahwa integritas akademik akan terus mengalami tekanan politik pasca makin kuatnya hegemoni AI.

6.3. Model Kurikulum Literasi AI

Gagasan kurikulum berbasis kecerdasan buatan (AI) adalah suatu pendekatan dalam pengembangan kurikulum yang menggabungkan teknologi kecerdasan buatan (AI) untuk menciptakan lingkungan pembelajaran yang adaptif, dan personal. Konsep ini bertujuan untuk mengoptimalkan proses kerja akademik dengan memanfaatkan kecerdasan buatan untuk menganalisis data, mengidentifikasi kebutuhan individu

mahasiswa, dan memberikan pengalaman belajar yang lebih efektif serta relevan. Implementasi teknologi AI dalam kurikulum ini bertujuan untuk membantu mencapai potensi maksimal memahami AI dan kualitas perkuliahan secara umum. AI memungkinkan terjadinya tradisi perkuliahan yang memiliki karakteristik seperti personalisasi, kurikulum lintas disiplin, dan akses pembelajaran seumur hidup.

6.3.1. Personalisasi

Implementasi AI dalam kurikulum memungkinkan pendekatan pembelajaran yang lebih personal dan adaptif atas teknologi digital. Dengan menganalisis data tentang kemajuan, gaya belajar, dan minat, AI dapat menyusun rencana pembelajaran yang sesuai dengan kebutuhan dan preferensi mahasiswa. Dosen dan sistem AI dapat memberikan materi dan tugas yang disesuaikan dengan tingkat kemampuan dan minat mahasiswa atas topik tertentu, sehingga mereka lebih termotivasi untuk belajar.

Mulyadi, dkk. (2024) menjelaskan, salah satu karakteristik pembelajaran AI di perguruan tinggi adalah mengembangkan pembelajaran berbasis masalah. AI dapat menyediakan simulasi dan skenario pembelajaran berbasis masalah yang lebih realistis dan aktual. Dengan pendekatan ini, mahasiswa belajar melalui tantangan dan masalah yang relevan dengan dunia empirik, menyediakan data untuk berpikir kritis, mencari solusi, dan meningkatkan kemampuan problem-solving.

Dengan bantuan AI, proses evaluasi pembelajaran dapat menjadi lebih mendalam dan akurat. Sistem AI dapat mengumpulkan data mengenai interaksi antara mahasiswa dengan materi perkuliahan dalam kelas, melihat tingkat pemahaman, serta respon terhadap berbagai aspek pembelajaran. Pengajar juga dapat menggunakan informasi ini untuk memberikan umpan balik diskursif yang lebih spesifik dan membantu mengidentifikasi area yang perlu ditingkatkan.

6.3.2. Kurikulum Lintas Disiplin

Memperhatikan beragam uraian dalam modul ini dan ekosistem AI yang berskala global, maka kurikulum AI harus bersifat lintas disiplin ilmu, tidak terbatas pada studi sains tertentu seperti ilmu Komunikasi, ilmu informatika atau kajian hukum. Kurikulumnya seharusnya lebih dinamis dan menjadi mata kuliah wajib sebagai pengantar teknologi pada semua departemen akademik.

6.3.3. Akses Pembelajaran Seumur Hidup

Teknologi AI memungkinkan pembelajaran seumur hidup di mana mahasiswa dapat terus mengakses materi pelajaran dan sumber belajar yang relevan. Ini membuka peluang bagi mahasiswa untuk terus mengembangkan pengetahuan dan keterampilan sepanjang hidup mereka, tanpa batasan fisik dan waktu.

Kurikulum kecerdasan buatan dalam dunia pendidikan tinggi di Indonesia mensyaratkan sejumlah pra-kondisi.

Pertama, ketersediaan infrastruktur teknologi. Penggunaan teknologi kecerdasan buatan memerlukan infrastruktur teknologi yang memadai, seperti akses internet yang stabil, perangkat komputer, dan jaringan yang handal. Tidak semua institusi pendidikan memiliki kemampuan internal untuk menyediakan sumber daya ini, sehingga diperlukan investasi dan dukungan yang memadai untuk memastikan seluruh mahasiswa dapat mengakses teknologi AI.

Kedua, pelatihan untuk dosen/asisten dosen. Implementasi AI dalam kurikulum memerlukan pemahaman dan keterampilan khusus dalam mengelola dan mengintegrasikan teknologi tersebut dalam proses pembelajaran. Oleh karena itu, diperlukan pelatihan dan pengembangan khusus bagi guru dan staf pendidikan agar mereka dapat memanfaatkan AI dengan efektif.

Ketiga, dan ini sangat krusial, mitigasi terhadap kemungkinan terjadinya pelanggaran privasi dan keamanan data. Penggunaan teknologi AI melibatkan pengumpulan dan penggunaan data hasil kerja dan data personal mahasiswa dalam proses pembelajaran. Dalam menghadapi hal ini, penting untuk menjaga privasi dan keamanan data pribadi agar tidak disalahgunakan atau diakses oleh pihak yang tidak berwenang.

Keempat, adanya resistensi. Adopsi teknologi baru sering kali dihadapkan pada resistensi dari berbagai pihak, termasuk dosen, mahasiswa, dan orang tua. Beberapa orang merasa tidak nyaman atau tidak yakin dengan peran AI dalam pendidikan tinggi dari segi teknis dan etis. Penting untuk mengatasi resistensi ini dengan komunikasi yang efektif dan pemahaman tentang dampak AI.

Kelima, soal etika dan bias dalam penggunaan aplikasi AI. AI sebagai produk teknologi dapat memperkuat bias dan stereotip yang sudah ada jika tidak diimplementasikan dengan pendekatan inklusi dan menerapkan

prinsip-prinsip hak asasi manusia. Oleh karena itu, penting untuk memastikan bahwa sistem AI yang digunakan dalam pembelajaran tidak menimbulkan diskriminasi atau perlakuan tidak adil terhadap kelompok tertentu di masyarakat.

Muatan kurikulum untuk literasi AI secara umum perlu mencakup dua aspek: literasi, pengenalan, kesadaran keberadaan AI, dan pengembangan kompetensi dasar manusia. Dari kedua komponen umum ini dikembangkan lagi muatan kurikulum yang mencakup lima hal. Pertama, pengetahuan dasar karakter teknologi dan sejarah perkembangan AI dengan bobot 10%. Kedua, fungsi dan peranan AI dalam kehidupan manusia dengan bobot 20%. Ketiga, keterampilan dalam menggunakan dan adaptasi AI dengan bobot 30%. Keempat, kemampuan evaluatif dan inovasi teknologi AI dengan bobot 30%. Kelima, pemahaman etik dan implikasi sosial AI dengan bobot 10%.

Berikut ini beberapa usulan model dan struktur kurikulum literasi AI, yang dihimpun dari diskusi kelompok peserta pelatihan untuk pelatih AI bagi akademisi, yang diselenggarakan Aliansi Jurnalis Independen (AJI) Indonesia dan Google News Initiative di Bogor, Jawa Barat 27-28 Februari 2025. Para peserta yang notabene mayoritas para dosen Ilmu Komunikasi dari berbagai kampus di Indonesia. Peserta mengusulkan sejumlah nama untuk mata kuliah terkait kecerdasan buatan ini. Peserta juga pada umumnya mengusulkan strategi perkuliahan lintas disiplin, menggabungkan tiga komponen sekaligus, yaitu aspek pengetahuan, keterampilan, dan penguatan etika penggunaan AI.

Rangkuman pemikiran soal mata kuliah AI dapat dicermati dalam tabel berikut ini:

Tabel 5.
Model dan Struktur Kurikulum Literasi AI

Nama Mata Kuliah	Tujuan Perkuliahan	Materi Perkuliahan	Semester/ SKS
Kecerdasan Artificial untuk Inovasi Multidisiplin	Memahami, Mengkritisi Menerapkan	Pengantar dan sejarah perkembangan AI, AI dan kampanye politik, AI dan kesehatan mental, Aplikasi AI di industri, aplikasi AI di pertanian, AI literasi, machine learning, design thinking, dll.	Semester 3/3 SKS
Etika dan AI	Memahami, mengkritisi	Penggunaan dan manfaat AI, AI dalam Kehidupan Sosial, Pengertian Etika, Etika AI, Kasus pelanggaran etik AI, Masa Depan AI, machine learning, fact-checking, dll.	Semester 3 ke atas/3 SKS
Literasi AI	Memahami, menerapkan	AI dalam sejarah, jenis jenis AI, manfaat dan tantangan AI, AI dalam disiplin Public Relations, jurnalistik, produksi konten, bisnis, Regulasi AI, dll.	Semester 3 ke atas/3 SKS
Pengantar AI untuk Ilmu Komunikasi	Memahami, menerapkan, mengkritisi	Introduction, media and communication industry; history, concepts of AI; Big data, safety, regulations; Skills, awareness, collaboration, critical thinking, etc.	Semester 1/3 SKS

Belajar dari perguruan tinggi di Amerika Serikat, khususnya Florida State University, maka kurikulum AI mengkaji hal-hal seperti dalam tabel berikut ini:

The UF AI Literacy Model: Descriptions for the five AI categories, content, and related student learning outcomes. AI Literacy types based on the model from Ng et al., 2021.

AI Literacy categories	Description	AI content ^a	SLOs
Enabling AI	Support AI through related knowledge and skill development (e.g., programming, statistics) and/or contain a lower total AI content of one of the four Core AI Literacy topics.	10–49%	SLO1. Identify, describe, and explain the components, requirements, and/or characteristics of AI. (Content knowledge and communication) SLO2. Recognize, identify, describe, define and/or explain applications of AI in multiple domains. (Critical thinking and communication)
Know & Understand AI	Know the basic functions of AI and to use AI applications	>50%	SLO1. Identify, describe, and explain the components, requirements, and/or characteristics of AI. (Content knowledge and communication) SLO2. Recognize, identify, describe, define and/or explain applications of AI in multiple domains. (Critical thinking and communication)
Use & Apply AI	Applying AI knowledge, concepts and applications in different scenarios	>50%	SLO3. Select and/or utilize AI tools and techniques appropriate to a specific context and application. (Critical thinking and content knowledge)
Evaluate and Create AI	Higher-order thinking skills (e.g., evaluate, appraise, predict, design) with AI applications	>50%	SLO4. Assess the context-specific value or quality of AI tools and applications. (Critical thinking) SLO5. Conceptualize and/or develop tools, hardware, data, and/or algorithms utilized in AI solutions. (Critical thinking)
AI Ethics	Human-centered considerations (e.g., fairness, accountability, transparency, ethics, safety)	>50%	SLO6. Develop, apply, and/or evaluate contextually appropriate ethical frameworks to use across all aspects of AI. (Critical thinking and content knowledge)

^a The initial identification of AI content percentages may change once more courses are evaluated and managed through this process.

(Sumber: Southworth, J. dkk., 2023).

DAFTAR PUSTAKA

Aliansi Jurnalis Independen. (2022). Panduan Keamanan Digital Untuk Jurnalis. Diakses dari:

<https://aji.or.id/data/panduan-keamanan-digital-untuk-jurnalis>

Aribowo, E. (2024). Memahami Etika Penggunaan AI dalam Publikasi Ilmiah. Diakses dari: <https://www.erickunto.com/2024/09/memahami-etika-penggunaan-ai-dalam-publikasi-ilmiah.html>

AMSI. (2024). Pedoman Penggunaan AI Untuk Media Siber. Asosiasi Media Siber Indonesia. Diakses dari <https://amsibali.or.id/dokumen/pedoman-penggunaan-ai-untuk-media-siber>

Associated Press. (2025). Artificial Intelligence. The Associated Press. Diakses dari: <https://www.ap.org/solutions/artificial-intelligence/>

Adami, M. (2023, March 23). Is ChatGPT a Threat or an Opportunity for Journalism? Five AI

Experts Weigh in. Reuters Institute. Diakses dari: <https://reutersinstitute.politics.ox.ac.uk/news/chatgpt-threat-or-opportunity-journalism-five-ai-experts-weigh>

Beckett, C. (2019). *New powers, new responsibilities A global survey of journalism and*

artificial intelligence. . London School of Economics and Political Science. e. Diakses dari: <https://blogs.lse.ac.uk/polis/2019/11/18/new-powers-new-responsibilities/>

Beckett dan Yaseen (2023). *Generating Change: The Journalism AI report.* Polis, London

School of Economics and Political Science. Diakses dari: https://static1.squarespace.com/static/64d60527c01ae7106f2646e9/t/6509b9a39a5ca70df9148eac/1695136164679/Generating+Change+_+The+Journalism+AI+report+_+English.pdf

Bahroun, Z., Anane, C., Ahmed, V., & Zacca, A. (2023). Transforming Education: A

Comprehensive Review of Generative Artificial Intelligence in Educational Settings

through Bibliometric and Content Analysis. Sustainability (Switzerland). Diakses dari: <https://doi.org/10.3390/su151712983>

BBC. (2024). BBC AI Principles. BBC. Diakses dari: <https://www.bbc.co.uk/supplying/working-with-us/ai-principles/>

Bronner, 2019
<https://edition.cnn.com/2019/03/26/business/mcdonalds-tech-startup-acquisition/index.html>

Dewan Pers. (2025). Pedoman Penggunaan Kecerdasan Buatan dalam Karya Jurnalistik. Dewan Pers. Diakses dari: https://dewanpers.or.id/assets/documents/peraturan/2501240214_1-Peraturan Dewan Pers Pedoman Penggunaan Kecerdasan Buatan.pdf

Florida State University (2025). *Florida State University Launches Artificial Intelligence*

Initiative. Diakses dari: [https://news.fsu.edu/news/science-technology/2025/02/14/florida-state-university-launches-ar](https://news.fsu.edu/news/science-technology/2025/02/14/florida-state-university-launches-artificial-intelligence-initiative/)

[tificial-intelligence-initiative/](https://news.fsu.edu/news/science-technology/2025/02/14/florida-state-university-launches-artificial-intelligence-initiative/)

Fahmi (2019): <https://pers.droneemprit.id/analisis-cyber-troops-jokowi-vs-prabowo/>

Fischer, S. (2020). Fact-Checking Goes Mainstream in Trump Era. Axios. Diakses dari: <https://www.axios.com/2020/10/13/fact-checking-trump-media>.

First Draft <https://firstdraftnews.org/long-form-article/understanding-information-disorder/>

Guardian, 2014
<https://www.theguardian.com/technology/2014/jun/08/super-computer-simulates-13-year-old-boy-passes-turing-test>

Graves, L. (2016). Boundaries Not Drawn. *Journalism Studies*, 19(5), 613–631.

Diakses dari <https://doi.org/10.1080/1461670x.2016.1196602>

Garnesia, I. (2024). Ekonomi Politik Cek Fakta di Indonesia.

Diakses dari: https://engagemedia.org/wp-content/uploads/2025/01/140125_Buku-EngageMedia_Revisi-Proofread-compressed.pdf

Haider, J., Söderström, K. R., Ekström, B., & Rödl, M. (2024). GPT-fabricated scientific

papers on Google Scholar: Key features, spread, and implications for preempting evidence manipulation. *Harvard Kennedy School (HKS) Misinformation Review*.

Diakses dari: <https://doi.org/10.37016/mr-2020-156>

Hamed, A.A., Wu, X. Detection of ChatGPT fake science with the xFakeSci learning algorithm. *Sci Rep* 14, 16231 (2024). Diakses dari

<https://doi.org/10.1038/s41598-024-66784-6>

Jerbi, D. (2023). Exploring the Latest Frontiers of Artificial Intelligence: A Review of Trends and Developments. TechRxiv. Diakses dari: <https://doi.org/10.36227/techrxiv.22717327>

Khalifa, M dan Albadawy, M. (2024). Using Artificial Intelligence in Academic Writing and Research: An Essential Productivity Tool. *Computer Methods and Programs in Biomedicine Update*, Vol. 5

Kementerian Pendidikan, Riset dan Teknologi. (2024). Permendikbudristek No. 39/2021 tentang Integritas Akademik dalam menghasilkan Karya Ilmiah. Diakses dari: https://jdih.kemdikbud.go.id/detail_peraturan?main=2943

Kementerian Pendidikan Tinggi, Sains dan Teknologi (2024). Panduan Penggunaan Generative AI pada Pembelajaran di Perguruan Tinggi. Diakses dari: <https://kemdiktisaintek.go.id/epustaka/122191/>

Kresna, M. (2017). *Menguji Keabsahan Data Ahok- Djarot saat Debat*. tirto.id.

<https://tirto.id/menguji-keabsahan-data-ahok-djarot-saat-debat-cgXD>

Kusuma, E., dkk. Panduan Perlindungan Digital untuk Aktivis. Diakses dari: <https://datadetoxkit.org/id/home/>

Krisetya, Beltsazar, dkk. (2024). Persepsi, Pengalaman, dan Rekomendasi Pemangku Kepentingan terkait Mis/Disinformasi dan Tata Kelola Informasi di Indonesia.

CSIS/Safer Internet Lab. Diakses dari: https://saferinternetlab.org/wp-content/uploads/2025/01/Rilis-Survei-Ahli-CSIS_SAIL-2024.pdf

Li, Z., Peng, Z., Zhang, Z., Chu, Y., Xu, C., Yao, S., García-Fernández, á. F., Zhu, X., Yue, Y.,

Levers, A., Zhang, J., & Ma, J. (2023a). Exploring Modern Bathymetry: A Comprehensive Review of Data Acquisition Devices, Model Accuracy, and Interpolation Techniques for Enhanced Underwater Mapping. *Frontiers in Marine Science*. Diakses dari: <https://doi.org/10.3389/fmars.2023.1178845>

Lelo, T. (2022). The Rise of the Brazilian Fact-Checking Movement: Between Economic Sustainability and Editorial Independence. *Journalism Studies*, 23(9). Diakses dari: <https://doi.org/10.1080/01461670x.2022.2069588>

Manan, A. (2024). *Artificial Intelligence (AI) dan Organisasi Berita di Indonesia: Pemetaan Pemanfaatan dan Rekomendasi untuk Stakeholder Media*. Diakses dari: <https://aji.or.id/system/files/2024-12/ajiartificial-intelligence-ai-dan-berita-dwibahasa.pdf>

McCarthy, J. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. Diakses dari: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>

Mulyadi, dkk. (2024). Kurikulum Berbasis Kecerdasan Buatan Menyongsong Revolusi Pendidikan. *Jurnal Literasiologi*, Vol. 12 (2).

Moore, M. (2018). *Democracy Hacked: Political Turmoil and Information Warfare in the Digital age*. London: Oneworld Publications Ltd.

Mark Stencel, J. L. (2021). *Fact-Checking Census Shows Slower Growth*. Duke Reporters' Lab. Diakses dari: <https://reporterslab.org/fact-checking-census-shows-slower-growth/>

Nentwich, M. (2001). De-Commodification in Academic Knowledge Distribution. *Science Studies*, Vol. 2

Nieminen, S., and V. Sankari. (2021). Checking PolitiFact's Fact-Checks. *Journalism Studies* 22 (3): 358–378. Diakses dari: <https://doi.org/10.1080/1461670X.2021.1873818>.

Nieminen, S., and L. Rapeli. (2019). Fighting Misperceptions and Doubting Journalists' Objectivity: A Review of Fact-Checking Literature. *Political Studies Review* 296–309. Diakses dari: <https://doi.org/10.1177/1478929918786852>.

NewsGuard (2025): <https://www.newsguardtech.com/special-reports/ai-tracking-center/>

Ogola, G., & Mare, A. (2023). *AI, Journalism, and Public Interest Media in Africa*. International Media Support. Diakses dari: <https://www.mediasupport.org/wp-content/uploads/2023/06/AI-Africa-Report-2023R-Double-Spread-View.pdf>

UNESCO Paris (2024). Recommendations of Ethics of Artificial Intelligence. Diakses dari: <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>

Petrescu, M dan Krishen, A. (2024). WhoOwn the Knowledge: Commodification of Academic Research. *Journal of Marketing Analytic*, Vol. 12.

Porlezza, C., dan Schapals, A. K. (2024). AI Ethics in Journalism (Studies): An Evolving Field Between Research and Practice. *Emerging Media*, 2(3), 356-370.

Rahmawan, D., Hartanto, R., & Garnesia, I. (2022). Multi Case Analysis on the Development of Fact-Checking Organizations in Indonesia. *Jurnal Kajian Komunikasi*, 10(1), 14. Diakses dari: <https://doi.org/10.24198/jkk.v10i1.38752>

Southworth, J. dkk. (2023), Developing a model for AI accross the curriculum: Transforming the higher education landscape via innovation in AI literacy. *Computer and Education*, Vol. 4.

Saferinternetlab.org, (2024). Survei Persepsi, Pengalaman, dan Rekomendasi Pemangku Kepentingan terkait Mis/Disinformasi dan Tata Kelola Informasi di Indonesia

Shidarta (2024). Sepuluh Prinsip UNESCO untuk Tata Kelola dan Etika Kecerdasan Buatan.

Diakses dari: <https://business-law.binus.ac.id/2024/12/16/sepuluh-prinsip-unesco-untuk-tata-kelola-dan-etika-kecerdasan-buatan/>

<https://binus.ac.id/sdg/goals/action/10-reduced-inequalities/16045-sepuluh-prinsip-unesco-untuk-tata-kelola-dan-etika-kecerdasan-buatan/>

Sir James. (1972). *Artificial Intelligence: A general survey Part 1*. Cambridge University.

Schenk, M.. (2021). Pfizer Petitions Court For Identity of 'Conservative Beaver' Publisher -- Lead Stories May Have Found Him. Lead Stories. Diakses dari: <https://leadstories.com/analysis/2021/11/who-is-conservative-beaver.html>

Taulli, T. (2019). *Artificial Intelligence Basics: A Non-Technical Introduction*.

Turing, M. (1950). *Computing Machinery and Intelligence*. Diakses dari: <https://courses.cs.umbc.edu/471/papers/turing.pdf>

Teja, 2023 <https://join2teja.medium.com/the-birth-of-chatgpt-from-inception-to-innovation-2a219d1b348c>

Tomsa, D., and C. Setijadi. (2018). New Forms of Political Activism in Indonesia. *Asian Survey* 58 (3). Diakses dari: <https://doi.org/10.1525/as.2018.58.3.557>.

UNEP. (2024). AI has Environmental Problem Here's what the world can do about that. United Nations Environment Programme. Diakses dari: <https://www.unep.org/news-and-stories/story/ai-has-environmental-problem-heres-what-world-can-do-about>

UNESCO. (2024). AI and the Future of Journalism: an Issue Brief for Stakeholders. Diakses dari: <https://unesdoc.unesco.org/ark:/48223/pf0000391214>

Verma, P.. (2024). These ISIS News Anchors are AI Fakes. Their Propaganda is Real. The Washington Post. Diakses dari: <https://www.washingtonpost.com/technology/2024/05/17/ai-isis-propaganda/>

Young, D. G., K. H. Jamieson, S. Poulsen, and A. Goldring. (2018). Fact-Checking Effectiveness as a Function of Format and Tone: Evaluating FactCheck.org and FlackCheck.org. *Journalism & Mass Communication Quarterly* 95 (1): 49–75. Diakses dari: <https://doi.org/10.1177/1077699017710453>.

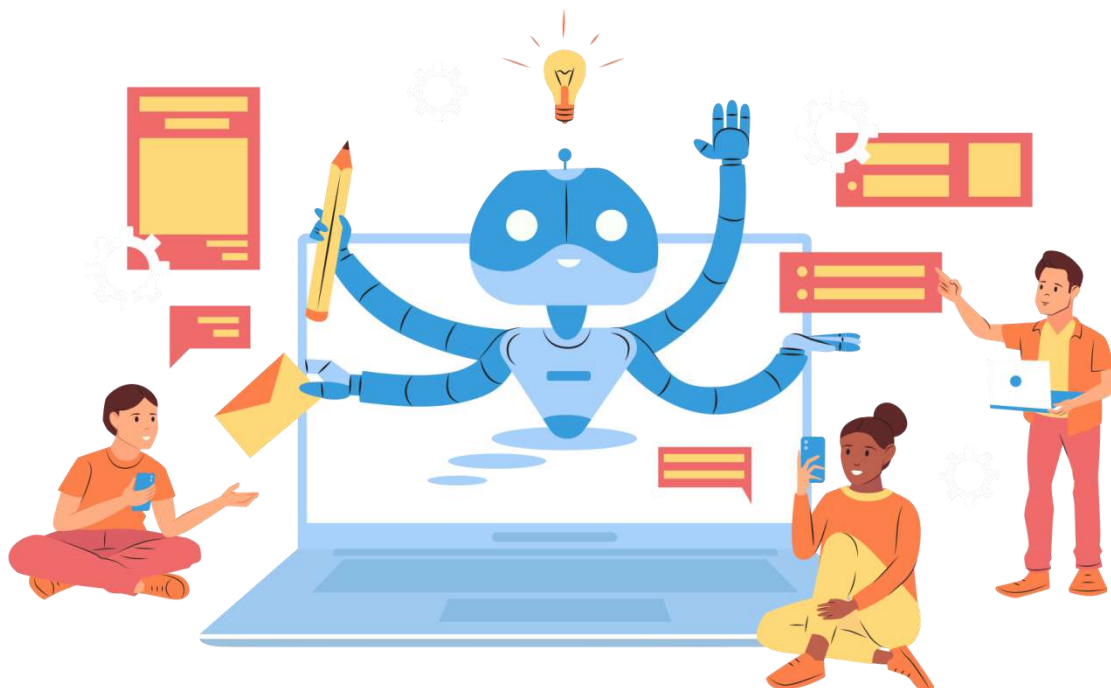
Yuniar, N. (2018). *Media di Indonesia Lolos Verifikasi International Fact Checking Network*.

Antara News. [https:// www.antaraneews.com/berita/679232/media-di-indonesia-lolos-verifikasi-international-fact-checking-network](https://www.antaraneews.com/berita/679232/media-di-indonesia-lolos-verifikasi-international-fact-checking-network)

Wendratama, dkk, (2023). Pengaturan Konten Ilegal dan berbahaya di Media Sosial.

PR2Media Yogyakarta, Diakses dari: [https://pr2media.or.id/publikasi/pengaturan-konten-ilegal-dan-berbahaya-di-media-sosial-riset-pengalaman-pengguna-dan-rekomendasi-kebijakan/We Are Social \(2025\):
<https://wearesocial.com/id/blog/2025/02/digital-2025/>](https://pr2media.or.id/publikasi/pengaturan-konten-ilegal-dan-berbahaya-di-media-sosial-riset-pengalaman-pengguna-dan-rekomendasi-kebijakan/We%20Are%20Social%20(2025):https://wearesocial.com/id/blog/2025/02/digital-2025/)

Welch, 2018
<https://www.theverge.com/2018/5/8/17332070/google-assistant-makes-phone-call-demo-duplex-io-2018>



LAMPIRAN: EVALUASI PESERTA/PEMBACA

Evaluasi untuk peserta/pembaca modul ini diuraikan dalam bentuk kuesioner berisi pertanyaan seputar isi model yang diajukan sebelum (pre-test) dan sesudah (post-test) pelatihan. Pertanyaan Pre-Post Test ini dapat diubah sesuai dengan kebutuhan pelatih ketika menyampaikan materi kepada peserta.

Bagian 1

1. Pemanfaatan kecerdasan buatan atau *artificial intelligence* (AI) bermula dari kemenangan Deep Blue atas Grandmaster Garry Kasparov pada tahun 1997.
 - A. Benar.
 - B. **Salah.**
2. Pemanfaatan AI oleh media bisa berlaku dalam tahapan proses produksi di bawah ini, kecuali:
 - A. Pengumpulan berita/konten.
 - B. Riset dan analisis untuk membuat konten.
 - C. Distribusi konten.
 - D. Pemeriksaan etika jurnalistik.
 - E. **Semua benar.**

Bagian 2

1. Berikut adalah alat pengecekan fakta berbasis AI, kecuali:
 - A. Reverse Search.
 - B. TinEye.
 - C. InVid.
 - D. **DALL.E.**
2. Seseorang tidak mengetahui kebenaran sebuah informasi tapi membagikan informasi yang keliru tersebut di media sosial. Hal ini disebut:
 - A. **Misinformasi.**
 - B. Disinformasi.
 - C. Malinformasi.

Bagian 3

1. AI dapat memfasilitasi/membantu akademisi dalam studi literatur untuk pembuatan artikel ilmiah atau riset seperti di bawah ini, kecuali:
 - A. Mencari artikel atau data riset terdahulu yang relevan.
 - B. Mengorganisasi data dan konteks dalam setiap artikel terdahulu.
 - C. Mencegah munculnya artikel yang melanggar etika penulisan akademik.
 - D. Melakukan pemeriksaan kemiripan dan atau indikasi plagiasi.
2. Berikut ini keterbatasan bantuan AI dalam riset akademik dan industri, kecuali:
 - A. Aktualitas data.
 - B. Kedalaman analisis.
 - C. Akurasi sumber data.
 - D. Kreativitas visualisasi data.
 - E. Membaca foto tabel data dari hasil *print* dan mengubahnya menjadi format Excel.

Bagian 4

1. Berikut adalah prinsip-prinsip keamanan digital, kecuali:
 - A. Kenyamanan berbanding lurus dengan keamanan.
 - B. Keamanan digital terkait erat dengan perilaku.
 - C. Bersifat personal dan kontekstual.
 - D. Bagian dari keamanan holistik.
2. Dari rangkaian pola password di bawah ini, mana yang paling kuat berpotensi dalam konteks dijebol oleh peretas?
 - A. Aku@58
 - B. Kuambilbuluhsebatang
 - C. 1LOv3U_
 - D. StrongPassword#1945

Bagian 5

1. Permendikbud No. 39/2021 mengatur pencegahan pelanggaran integritas akademik dalam penulisan berbasis AI, yang itu meliputi:
 - A. Fabrikasi.
 - B. Falsifikasi.
 - C. Plagiat.
 - D. **Semua A, B, C benar.**
2. Berikut ini beberapa problematika utama penggunaan aplikasi AI dalam penulisan akademik dan industri, kecuali:
 - A. Kepengarangan palsu/hantu.
 - B. Bias informasi yang ter-fabrikasi.
 - C. Problem hukum akuntabilitas karya.
 - D. **Hak cipta atas karya berbasis aplikasi AI.**

Bagian 6

1. Berikut ini beberapa tantangan dalam literasi digital AI di perguruan tinggi, kecuali
 - A. Privacy.
 - B. Reusing.
 - C. Moderating.
 - D. **Financing.**
2. Pendekatan kebijakan berbasis manusia / humanisasi Ai diterapkan oleh badan dunia UNESCO dalam bentuk kampanye penerapan...
 - A. **Kode Etik Penggunaan AI.**
 - B. Pembatasan Akses Aplikasi AI tertentu.
 - C. Pencegahan Monopoli Bisnis AI.
 - D. Semua A,B dan C benar.

BIO DATA PENULIS



Masduki adalah pengurus pusat Aliansi Jurnalis Independen (AJI) Indonesia bidang riset (2024-2027) dan dosen tetap pada Jurusan Ilmu Komunikasi, Fakultas Psikologi dan Ilmu Sosial Budaya, Universitas Islam Indonesia sejak 2004 hingga sekarang. Ia memperoleh gelar master dalam kajian jurnalisme di Ateneo De Manila University, Manila, Filipina (2006) dan gelar Doktor (Dr.rer.soc) pada tahun 2019 dari

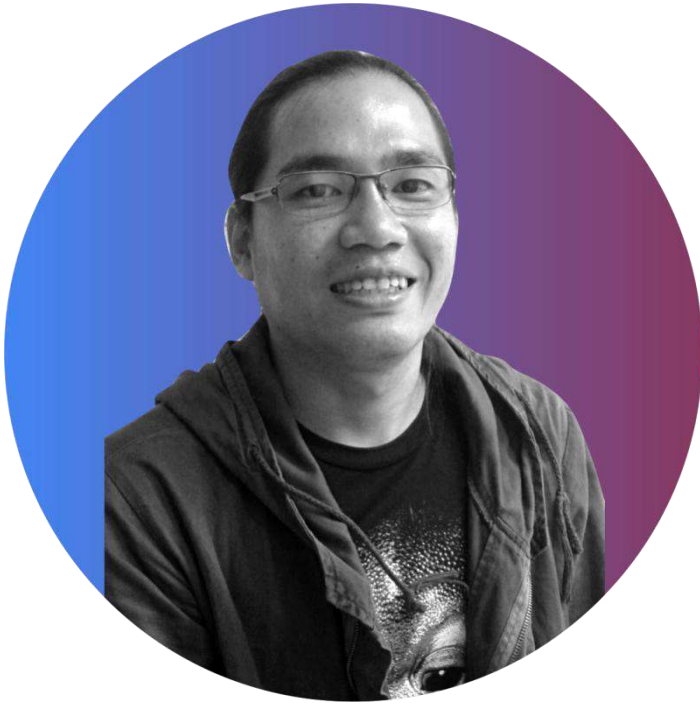
Institute of Communication Studies and Media Research (IfKW) University of Munich, Germany. Selama studi S-3 di Munich, Jerman (2015-2019), ia menjadi prinsipal investigator untuk Indonesia dalam riset multinasional the World of Journalism Study (WJS).

Masduki menjadi jurnalis radio pada periode 1998-2004, Ketua Aliansi Jurnalis Independen cabang Yogyakarta (2002-2004), anggota Majelis Etik Nasional AJI (2008-2017), Direktur Program dan Produksi Radio Republik Indonesia (RRI) 2010-2013. Ia memiliki minat riset pada kajian perbandingan sistem media, jurnalisme, kebijakan dan tata kelola media publik dan aktivisme media (*media activism*). Masduki menghasilkan sejumlah buku akademik antara lain: *Kebebasan Pers dan Kode Etik Jurnalistik* (2004); *Regulasi Penyiaran: Dari Otoriter ke Liberal* (2007); *Tata Kelola Lembaga Penyiaran Publik Global* (2017). ia juga aktif menulis yang karyanya bisa dinikmati pada beberapa jurnal internasional bereputasi, seperti *Assessing Indonesian Journalist Threats: Cases, Actors and Motives* (Media Asia, 2017); *Political Economy of Sport Broadcasting: Assessing Indonesian PSB Policy in Sport Broadcasting* (Gazette, 2017); *In Media We Trust* (Journalism Studies, 2017); dan *Journalism and The Islamic Worldview* (Journalism Studies, 2017). Ia tinggal di nDalem Manis, Lemponsari, Ngaglik, Sleman, Yogyakarta.



Aghnia Adzkia adalah Jurnalis Data dan Visual BBC World Service yang meliput isu lingkungan, hukum, politik, dan seni di kawasan Asia Timur dan Asia Tenggara. Liputan investigasinya tentang plasma dan kebun sawit di Indonesia, kolaborasi BBC dengan Mongabay dan The Gecko Project, memenangkan The Society of Publishers in Asia (SOPA) Awards pada 2023 lalu.

Ia juga pendiri komunitas jurnalis dan pegiat data, Journocoders Indonesia, dan melatih lebih dari 250 wartawan dan akademisi di seluruh Indonesia dan Asia. Pada 2022, bersama Journocoders dan kolaborator lain, Aghnia menyelenggarakan *Data and Computational Journalism Conference* di Indonesia dengan mengundang berbagai pembicara dari Amerika, Eropa, Asia, dan Australia. Ia juga pelatih cek fakta yang tergabung dalam jaringan Google News Initiative sejak 2019. Ia lulusan sarjana Ilmu Komunikasi UGM pada 2013 dan meraih gelar master dalam kajian jurnalisme digital dan data dari Goldsmiths, University of London pada 2017. Pada 2024 Aghnia juga mengikuti program *short course* terkait mis/disinformasi dari Queensland University of Technology, Brisbane, yang diselenggarakan bersama Australia Awards.



Adi Marsiela, adalah anggota Aliansi Jurnalis Independen (AJI) Kota Bandung yang juga Koordinator Bidang Internet AJI Indonesia sejak 2021. Ia pernah menjadi Sekretaris AJI Bandung (2011-2014), Ketua AJI Bandung (2014-2017). Karirnya diawali dari jurnalis lepas untuk Suara Pembaruan sejak 2003 hingga 2021. Ia juga menulis untuk beberapa media seperti The Jakarta Post, Project Multatuli, dan

mengirimkan konten dan foto untuk kantor berita EPA, AFP, dan Anadolu Agency.

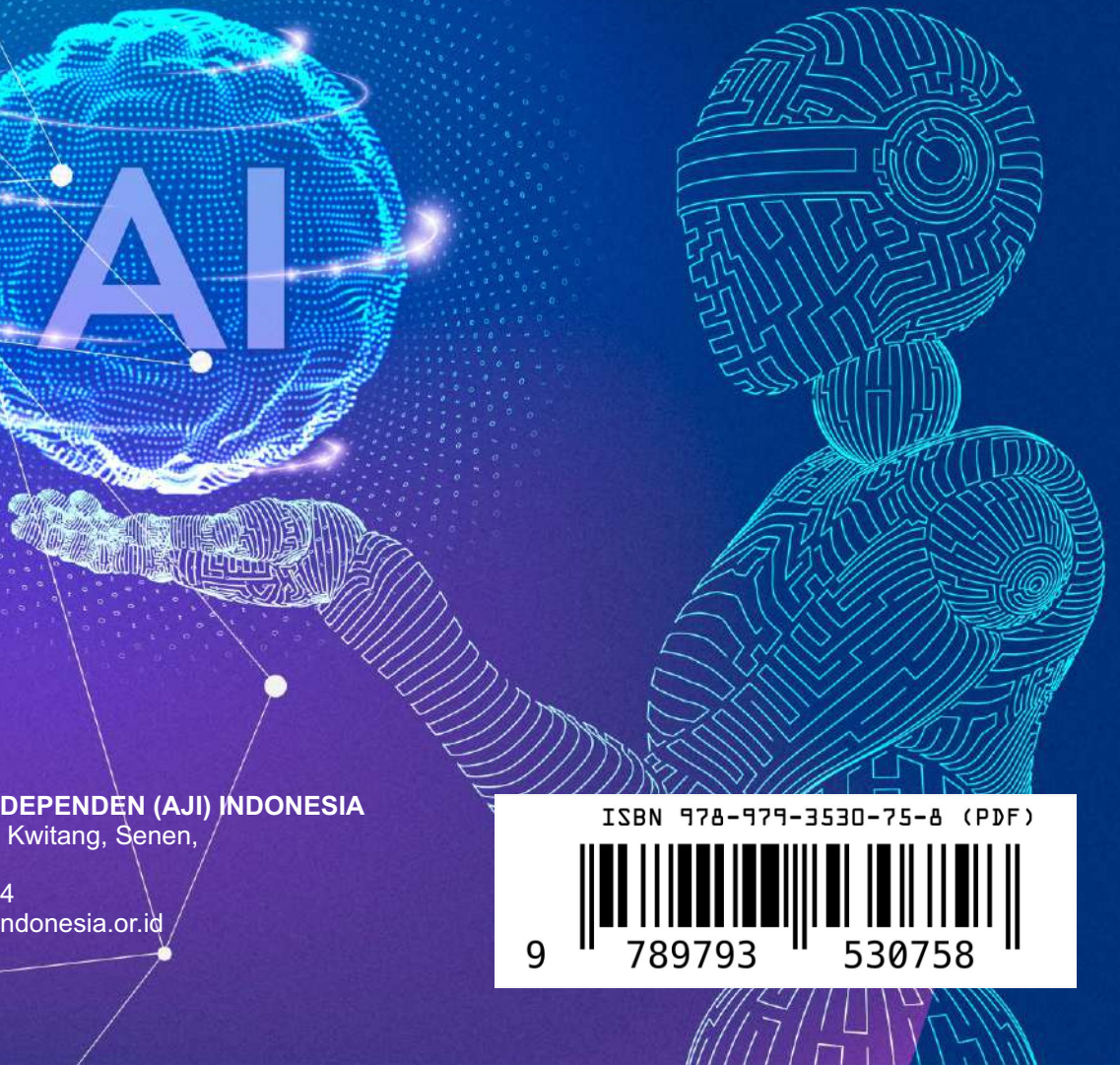
Adi menyelesaikan pendidikan sarjana bidang kajian jurnalistik dari Fakultas Ilmu Komunikasi Universitas Padjadjaran pada 2005. Selain menjadi jurnalis lepas, ia terlibat aktif dalam pengembangan modul serta pelatihan jurnalisisme data, cek fakta, serta keamanan jurnalis. Pada 2006, Adi mendapatkan Anugerah Adiwarta Sampoerna untuk kategori penulisan berita sosial serta berita seni dan musik.

Adi juga berkontribusi dalam penyusunan "Buku Saku Advokasi bagi Jurnalis dan Media" yang diterbitkan oleh AJI, Perangkat Penilaian Risiko bagi Jurnalis di portal AJI, modul belajar Keselamatan bagi Jurnalis Lingkungan bersama International Media Support. (IMS) yang diluncurkan pada Global Investigative Journalism Conference 2023 di Swedia. Terkait teknologi AI, Adi ikut menyusun Asesmen Penggunaan Kecerdasan Buatan (AI) dalam Media di Indonesia: Tantangan, Peluang, dan Pengembangan Standar Etika (AJI) yang dipublikasikan pada awal 2025.



**ALIANSI
JURNALIS
INDEPENDEN**
Alliance of Independent Journalist

KECERDASAN ARTIFISIAL DALAM ARUS INFORMASI DAN MEDIA



ALIANSI JURNALIS INDEPENDEN (AJI) INDONESIA
Jl. Kembang Raya No.6 Kwitang, Senen,
Jakarta Pusat 10420
Telepon : (6221)3151214
E-mail : sekretariat@ajiindonesia.or.id
Web : www.aji.or.id

ISBN 978-979-3530-75-8 (PDF)



9

789793

530758