
Demokrasi Digital dan Perlindungan Anak di Ruang Media Sosial
Prof Ir Rudy C Tarumingkeng, PhD
Guru Besar Manajemen dan AI Data Analyst
IBM-ASMI | RudyCT Academic Series
www.rudyct.com/cv.pdf
BELAJAR
BERKREASI
BERDISKUSI
BERPARTISIPASI
UNTUK
INDONESIA
YANG LEBIH BAIK
Ruang Digital Aman untuk Anak
PP TUNAS | PP No. 17 Tahun 2025
Permenkomdigi No. 9 Tahun 2026
Pembatasan akun di bawah 16 tahun berlaku pada platform digital berisiko tinggi sesuai aturan.
HAK ANAK DIGITAL
Aman
Privat
Bersuara & berpartisipasi
RISIKO YANG PERLU DIKELOLA
Perundungan siber
Konten berbahaya
Eksploitasi & penipuan
Penyalahgunaan data
TANGGUNG JAWAB BERSAMA
Platform: desain aman
Keluarga: dampingi
Sekolah: literasi digital
Pemerintah: aturan & pengawasan
Lindungi anak tanpa membungkam suara dan partisipasinya.

Demokrasi Digital dan Perlindungan Anak di Ruang Media Sosial

Hak untuk aman, berekspresi, memperoleh informasi, dan berpartisipasi

Prof Ir Rudy C Tarumingkeng, PhD
www.rudyct.com/cv.pdf

IBM-ASMI - RudyCT Academic Series

Naskah akademik populer | Status regulasi diperiksa hingga 31 Oktober 2026

Abstract

Artikel ini membahas hubungan antara demokrasi digital dan perlindungan anak di media sosial dengan pendekatan berbasis hak. Anak dipahami sebagai pengguna sekaligus warga muda yang berhak memperoleh informasi, berekspresi, berpartisipasi, menjaga privasi, dan terlindung dari kekerasan serta eksploitasi. Naskah memetakan risiko konten, kontak, perilaku, kontrak, kesehatan mental, misinformasi, dan penggunaan kecerdasan buatan; mengulas kerangka hukum Indonesia termasuk PP Nomor 17 Tahun 2025 dan Permenkomdigi Nomor 9 Tahun 2026; serta menilai batasan usia, desain aman, tanggung jawab platform, keluarga, sekolah, dan pemerintah. Kesimpulan utamanya: perlindungan yang efektif perlu mengurangi bahaya tanpa membungkam suara anak, dan harus dievaluasi melalui dampak nyata, akses pemulihan, privasi, serta kualitas partisipasi.

Kata Kunci: Demokrasi digital; perlindungan anak; media sosial; hak anak; privasi digital; literasi digital; PP TUNAS; keselamatan daring

Catatan ruang lingkup

Artikel ini membahas prinsip hak anak dan tata kelola media sosial berdasarkan sumber yang tersedia hingga 31 Oktober 2026. Uraian regulasi bersifat informatif; penerapan terhadap kasus tertentu harus merujuk teks hukum resmi dan keputusan lembaga yang berwenang.

Pendahuluan: anak di ruang publik digital

Media sosial telah menjadi ruang penting bagi anak untuk berkomunikasi, mencari pengetahuan, menunjukkan karya, membangun persahabatan, dan memahami peristiwa publik. Anak tidak hanya menjadi pengguna yang menerima konten, tetapi juga pencipta, penyebar, komentator, pengorganisasi kegiatan, dan peserta dalam percakapan sosial. Karena itu, pembicaraan tentang perlindungan anak di media sosial tidak dapat berhenti pada larangan atau pengawasan orang dewasa. Ia perlu menjawab bagaimana hak anak untuk aman dapat berjalan bersama dengan hak untuk berekspresi, memperoleh informasi, berpartisipasi, belajar, dan menjaga privasi. Demokrasi digital yang sehat harus mengakui anak sebagai warga yang sedang tumbuh, yang memiliki kapasitas berkembang dan suara yang perlu didengar.

Pada saat yang sama, media sosial dibangun dengan sistem rekomendasi, pengumpulan data, desain antarmuka, dan model bisnis yang dapat memengaruhi perilaku serta pilihan pengguna. Anak berhadapan dengan konten yang tidak selalu dipilih secara sadar, interaksi dari orang yang tidak dikenal, perundungan, manipulasi, komersialisasi perhatian, dan jejak data yang sulit dihapus. Tantangan kebijakan ialah mengurangi risiko tanpa mengubah internet menjadi ruang yang tertutup bagi anak atau menempatkan seluruh beban pada keluarga. Di Indonesia, PP Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik dalam Pelindungan Anak, yang dikenal sebagai PP TUNAS, dan Permenkomdigi Nomor 9 Tahun 2026 telah membentuk kerangka baru pengaturan platform. Artikel ini menguraikan dasar hak, risiko, perangkat hukum, pembagian tanggung jawab, dan ukuran pelaksanaan kebijakan tersebut.

Demokrasi digital sebagai ruang partisipasi

Demokrasi digital merujuk pada penggunaan teknologi untuk membentuk komunikasi publik, pertukaran gagasan, akses informasi, pembentukan opini,

dan partisipasi dalam keputusan bersama. Bagi orang dewasa, media sosial menjadi kanal kampanye, advokasi, kritik, dan pengawasan pemerintah; bagi anak, ia juga menjadi ruang belajar tentang isu lingkungan, pendidikan, kesehatan, kesetaraan, dan komunitas. Anak dapat menyebarkan karya seni, membentuk kelompok belajar, menggalang dukungan terhadap teman, atau menyampaikan pandangan mengenai kebijakan sekolah. Pengalaman ini menumbuhkan literasi kewargaan dan rasa bahwa pendapat mereka bernilai. Jika perlindungan dirancang hanya sebagai pembatasan akses, manfaat partisipasi dan pembelajaran tersebut dapat hilang.

Partisipasi anak perlu dimaknai lebih dari sekadar kemampuan membuat unggahan atau menekan tombol suka. Partisipasi bermakna mensyaratkan ruang yang aman, informasi yang dapat dipahami, kesempatan menyampaikan pandangan, dan tanggapan yang menunjukkan bahwa suara anak dipertimbangkan. Kerangka Lundy (2007) tentang ruang, suara, audiens, dan pengaruh berguna untuk menilai kualitas partisipasi: apakah anak diberi ruang untuk berbicara, didukung mengekspresikan pendapat, didengar oleh pihak yang berwenang, dan memiliki pengaruh yang sesuai usia. Prinsip ini relevan bagi konsultasi kebijakan digital, perancangan layanan sekolah, pengaturan komunitas daring, dan evaluasi kebijakan platform. Partisipasi bukan pembenaran untuk mengekspos anak pada risiko; ia menuntut perlindungan yang memungkinkan suara disampaikan dengan aman.

Hak anak di lingkungan digital

Konvensi Hak Anak PBB memberikan kerangka yang menyatukan perlindungan, partisipasi, dan pemenuhan kebutuhan tumbuh kembang. Hak atas kebebasan berekspresi dan akses informasi berkaitan dengan perlindungan dari kekerasan, eksploitasi, diskriminasi, serta campur tangan sewenang-wenang terhadap privasi. Komite Hak Anak PBB melalui Komentar Umum No. 25 menegaskan bahwa hak-hak anak berlaku juga di lingkungan

digital; negara perlu memastikan akses yang aman, perlindungan data, pendidikan digital, dan pemulihan ketika hak dilanggar (United Nations Committee on the Rights of the Child, 2021). Dengan demikian, ruang digital tidak berada di luar sistem hak asasi. Norma yang sama perlu diterjemahkan dalam desain produk, kebijakan sekolah, layanan keluarga, dan penegakan hukum.

Kepentingan terbaik anak merupakan pertimbangan utama, tetapi bukan slogan yang otomatis menyelesaikan perbedaan kepentingan. Penilaian harus mempertimbangkan usia, kematangan, kebutuhan khusus, konteks budaya, tingkat risiko, manfaat layanan, dan pandangan anak. Hak perlindungan tidak boleh digunakan secara berlebihan untuk membungkam kritik atau menghapus akses anak terhadap informasi yang berguna. Sebaliknya, hak berekspresi juga tidak membenarkan eksploitasi, pengungkapan identitas korban, atau penyebaran konten berbahaya. Pendekatan berbasis hak menuntut proporsionalitas: pembatasan harus memiliki dasar yang jelas, diperlukan untuk tujuan perlindungan, menggunakan cara yang paling tidak membatasi, dan dapat ditinjau. Anak harus diperlakukan sebagai subjek hak yang berkembang, bukan hanya sebagai objek pengawasan.

Memahami peta risiko: empat kategori

Salah satu cara untuk memetakan risiko online adalah membedakan risiko konten, kontak, perilaku, dan kontrak. Risiko konten muncul ketika anak melihat materi yang mengganggu, tidak sesuai usia, menyesatkan, atau menghasut kebencian. Risiko kontak terjadi ketika orang asing atau pelaku berniat jahat mendekati anak melalui pesan, pertemanan, atau fitur siaran langsung. Risiko perilaku mencakup perundungan, penghinaan, penyebaran foto tanpa izin, doxing, dan tekanan kelompok. Risiko kontrak muncul dari layanan yang mengumpulkan data secara berlebihan, mendorong pembelian, memanipulasi perhatian, atau membuat anak menyetujui syarat yang tidak dipahami. Kategori

ini dapat beririsan; satu pengalaman dapat melibatkan pesan manipulatif, pengumpulan data, dan penyebaran gambar sekaligus.

Peta risiko bukan daftar untuk menakut-nakuti orang tua. Fungsinya membantu merancang pencegahan dan respons yang tepat. Paparan konten membutuhkan pengaturan rekomendasi, moderasi, pelabelan, dan literasi kritis. Risiko kontak memerlukan pengaturan pesan privat, pelaporan, dan edukasi mengenali manipulasi. Perundungan membutuhkan aturan komunitas, dukungan bagi korban, intervensi sekolah, serta proses akuntabilitas yang tidak mempermalukan anak. Risiko kontrak memerlukan desain privasi, pembatasan iklan tertarget, penjelasan yang sesuai usia, serta pengawasan regulator. Risiko harus dilihat dari kemungkinan terjadinya dan dampaknya, bukan hanya viralitas suatu kasus. Anak yang menerima dukungan sosial dapat pulih dengan lebih baik daripada anak yang mengalami masalah serupa dalam isolasi, sehingga respons perlu memasukkan relasi dan konteks.

Perundungan siber dan kekerasan berbasis teknologi

Perundungan siber dapat berlangsung melalui pesan, komentar, grup kelas, akun anonim, permainan daring, atau penyebaran foto dan video. Sifatnya yang persisten dan mudah disalin dapat membuat pengalaman terasa terus hadir, bahkan setelah anak meninggalkan sekolah. Penghinaan yang tampak ringan bagi pengunggah dapat menjadi pengalaman berat ketika dilihat banyak orang, disimpan, dan dikirim ulang. Korban mungkin merasa malu, takut, kehilangan konsentrasi, menjauh dari pertemanan, atau enggan datang ke sekolah. Namun respons tidak boleh hanya menuntut korban menghapus akun atau menjauh dari internet. Tindakan seperti itu dapat membuat korban kehilangan dukungan sosial dan memindahkan konsekuensi dari pelaku kepada orang yang dirugikan.

Sekolah dan keluarga sebaiknya memiliki protokol yang mengutamakan keselamatan dan pemulihan. Anak perlu tahu cara menyimpan bukti tanpa

menyebarkannya lebih luas, memblokir atau melaporkan akun, meminta bantuan orang dewasa tepercaya, dan mengakses layanan konseling. Sekolah harus membedakan konflik sesaat dari pola perundungan, tetapi tetap menangani setiap ancaman serius. Pelaku yang masih anak juga membutuhkan proses yang mendidik dan proporsional, tanpa menghapus pertanggungjawaban. Pendekatan restoratif dapat membantu ketika aman dan disetujui pihak terdampak, namun tidak tepat dipaksakan dalam kasus kekerasan, ancaman, pelecehan seksual, atau relasi kuasa yang timpang. Platform perlu menyediakan alat pelaporan yang mudah, memberi informasi tentang hasil tindak lanjut, dan mencegah akun pelaku mengulangi pola serupa.

Eksploitasi seksual dan ancaman keselamatan

Risiko paling berat termasuk bujuk rayu untuk tujuan seksual, pemerasan seksual, produksi atau penyebaran materi seksual anak, perdagangan orang, dan upaya memindahkan komunikasi ke kanal tertutup. Pelaku dapat memakai pujian, hadiah virtual, ancaman, rasa malu, atau hubungan emosional palsu untuk memperoleh kepercayaan anak. Anak yang dihubungi tidak patut disalahkan, sekalipun ia pernah mengirim gambar atau membalas pesan. Tanggung jawab harus diarahkan kepada pelaku dan sistem yang gagal mencegah atau merespons risiko. Respons awal harus tenang, mengutamakan keselamatan, tidak menyebarkan ulang materi, serta melibatkan layanan berwenang dan tenaga terlatih. Penghapusan konten harus dilakukan melalui mekanisme yang aman, tanpa menjadikan anak korban sebagai objek pemeriksaan yang berulang.

Pencegahan memerlukan kerja bersama platform, keluarga, sekolah, lembaga perlindungan anak, aparat penegak hukum, dan layanan kesehatan. Platform harus merancang fitur pesan, pencarian, rekomendasi, dan siaran langsung agar mengurangi kemungkinan orang dewasa yang tidak dikenal

mendekati anak secara privat. Sistem pelaporan perlu memungkinkan pelaporan tanpa memaksa korban mengunggah kembali konten berbahaya. Aparat dan pendamping perlu memahami bukti digital, menjaga kerahasiaan, dan meminimalkan pertanyaan berulang yang dapat menambah trauma. Layanan bagi korban harus tersedia di berbagai daerah, tidak hanya di kota besar. Kebijakan perlindungan juga harus menghindari pemblokiran massal konten edukasi seksual atau kesehatan reproduksi yang sah; moderasi harus bisa membedakan eksploitasi dari informasi pendidikan dan dukungan korban.

Privasi, jejak digital, dan data anak

Setiap tindakan digital dapat menghasilkan data: pencarian, lokasi, wajah, minat, kontak, durasi penggunaan, pola tidur, dan respons emosional. Data ini dapat dipakai untuk menyesuaikan layanan, tetapi juga untuk membuat profil, menargetkan iklan, memengaruhi pilihan, atau memperkirakan keadaan anak. Anak belum tentu memahami bahwa satu foto atau komentar dapat disalin, dicari kembali, dan digunakan dalam konteks yang tidak pernah ia bayangkan. Jejak digital yang dibuat oleh orang dewasa tentang anak—misalnya unggahan keluarga atau sekolah—juga dapat melanggar privasi anak dan membentuk jejak permanen tanpa persetujuannya. Prinsip minimisasi data berarti layanan hanya mengumpulkan informasi yang sungguh diperlukan dan tidak menyimpan lebih lama dari tujuan yang sah.

Perlindungan data anak bukan sekadar meminta persetujuan dengan menampilkan tombol panjang yang tidak terbaca. Penjelasan harus sesuai usia; pilihan harus benar-benar dapat dipahami; dan anak maupun wali perlu mengetahui bagaimana data digunakan, disimpan, dibagikan, dan dihapus. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memberi perhatian khusus pada pemrosesan data pribadi anak dan mensyaratkan persetujuan orang tua atau wali sesuai ketentuan. Namun persetujuan tidak melegitimasi pengumpulan yang berlebihan atau desain

manipulatif. Sistem verifikasi usia juga perlu dirancang agar tidak meminta salinan identitas atau biometrik jika ada cara yang lebih minim data. Privasi dan perlindungan dapat berkonflik jika verifikasi menyimpan informasi sensitif; karena itu regulator perlu mengevaluasi risiko kebocoran dan penggunaan sekunder.

Kesehatan mental: bukti yang perlu dibaca cermat

Diskusi publik sering menghubungkan media sosial secara langsung dengan depresi, kecemasan, gangguan tidur, dan masalah citra tubuh. Penelitian memang menemukan asosiasi antara penggunaan bermasalah dan gejala tertentu, tetapi hubungan tersebut tidak selalu membuktikan bahwa media sosial menjadi penyebab tunggal. Tinjauan sistematis Saleem, Young, dan Yousuf (2024) menemukan asosiasi antara penggunaan media sosial yang bermasalah dan gejala depresi maupun kecemasan, sambil menekankan heterogenitas studi serta perlunya penelitian longitudinal yang lebih kuat. Odgers dan Jensen (2020) juga mengingatkan bahwa dampak teknologi digital pada remaja beragam dan tidak tepat disederhanakan menjadi satu kesimpulan untuk semua anak. Bentuk penggunaan, dukungan sosial, pengalaman sebelumnya, dan kondisi keluarga dapat mengubah dampaknya.

Karena itu kebijakan sebaiknya tidak semata-mata menghitung menit layar. Anak dapat menghabiskan waktu lama untuk belajar, berbicara dengan teman yang jauh, atau membuat karya; sebaliknya penggunaan singkat dapat tetap berisiko jika melibatkan ancaman atau eksploitasi. Indikator yang lebih berguna mencakup apakah penggunaan mengganggu tidur, pembelajaran, hubungan sosial tatap muka, aktivitas fisik, dan kesejahteraan anak; apakah anak merasa mampu berhenti; serta apakah pengalaman online mendukung atau merusak rasa aman. Orang tua dan pendidik perlu mendengarkan pengalaman anak sebelum membuat kesimpulan. Platform harus menilai dampak fitur seperti rekomendasi tanpa akhir, notifikasi berulang, perbandingan sosial, dan fitur

yang mendorong keterlibatan intensif pada kelompok usia yang berbeda (Orben, 2020; Valkenburg et al., 2022).

Misinformasi, polarisasi, dan ruang kritik anak

Anak menjumpai informasi politik, kesehatan, lingkungan, dan peristiwa sosial melalui rekomendasi serta percakapan teman sebaya. Kemampuan mengevaluasi sumber tumbuh seiring pengalaman; gambar yang diedit, judul sensasional, dan video yang dipotong dapat terlihat meyakinkan. Di ruang demokrasi, literasi kritis perlu melatih anak membedakan fakta, opini, satire, propaganda, dan iklan; memeriksa sumber asli; serta memahami mengapa suatu konten direkomendasikan. Tujuannya bukan mengarahkan anak kepada satu pandangan politik, melainkan memperkuat kemandirian berpikir dan tanggung jawab berbagi. Kurikulum digital yang netral secara partisan harus mengajarkan proses penilaian informasi, termasuk kesediaan mengoreksi kesalahan sendiri.

Perlindungan anak tidak boleh dijadikan dalih untuk menekan kritik yang sah. Anak memiliki hak untuk berpendapat tentang sekolah, lingkungan, pelayanan publik, dan isu yang memengaruhi hidupnya. Namun ketika anak terlibat dalam diskusi publik, identitas, lokasi, dan data pribadinya harus dilindungi dari serangan serta doxing. Kebijakan moderasi perlu membedakan kritik, satire, dan advokasi dari ancaman atau pelecehan. Konten yang melibatkan anak dalam kampanye politik juga memerlukan kehati-hatian agar tidak ada eksploitasi citra, manipulasi emosional, atau penyebaran informasi sensitif. Demokrasi digital yang melindungi anak tidak membuat mereka diam; ia menyediakan cara aman agar partisipasi tidak berujung pada intimidasi atau pembalasan.

Ketimpangan akses dan inklusi digital

Anak tidak mengalami ruang digital dengan kondisi yang sama. Kualitas jaringan, kepemilikan perangkat, literasi keluarga, bahasa, disabilitas, lokasi, pendapatan, dan ketersediaan pendampingan memengaruhi akses serta risiko. Anak di wilayah dengan koneksi terbatas dapat kehilangan peluang belajar, sementara anak yang berbagi perangkat mungkin tidak memiliki ruang privat untuk berkonsultasi atau melaporkan masalah. Anak penyandang disabilitas dapat menghadapi fitur yang tidak aksesibel dan risiko pelecehan yang khas. Anak dalam situasi pengasuhan alternatif, migrasi, atau konflik keluarga mungkin tidak memiliki orang dewasa yang mampu mendampingi secara konsisten. Kebijakan yang hanya menekankan kontrol orang tua berpotensi menguntungkan keluarga yang memiliki waktu, pendidikan, perangkat, dan sumber daya lebih besar.

Inklusi berarti menyediakan layanan perlindungan dan literasi dalam berbagai bentuk: tatap muka, materi sederhana, bahasa yang mudah, audio, teks, dan dukungan aksesibilitas. Sekolah perlu memiliki kebijakan perangkat dan penggunaan internet yang tidak menghukum anak yang tidak mampu membeli gawai. Pemerintah daerah dapat menjalin kerja sama dengan perpustakaan, puskesmas, pusat layanan keluarga, dan organisasi masyarakat untuk memberi akses konsultasi. Platform harus menguji fitur dengan anak dari kelompok beragam, bukan hanya pengguna perkotaan yang terhubung baik. Kesenjangan digital juga mengandung dimensi kualitas: memiliki akses bukan berarti mempunyai kemampuan menilai informasi, menjaga privasi, dan mencari bantuan. Karena itu pemerataan akses harus berjalan bersama peningkatan kapabilitas dan perlindungan yang nyata.

Kerangka hukum Indonesia

Kerangka perlindungan anak di Indonesia dibangun dari beberapa lapisan. Konvensi Hak Anak diratifikasi melalui Keputusan Presiden Nomor 36 Tahun

1990. Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak telah diubah, antara lain melalui Undang-Undang Nomor 35 Tahun 2014 dan Undang-Undang Nomor 17 Tahun 2016. Undang-Undang Nomor 27 Tahun 2022 mengatur pelindungan data pribadi, termasuk pemrosesan data anak. Undang-Undang Informasi dan Transaksi Elektronik telah diubah melalui Undang-Undang Nomor 1 Tahun 2024. Masing-masing memberi dasar bagi perlindungan yang berbeda: keselamatan dan tumbuh kembang, privasi dan pemrosesan data, serta tata kelola komunikasi elektronik. Penerapannya perlu dibaca secara harmonis, bukan sebagai aturan yang berdiri sendiri.

Tonggak paling baru ialah PP Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik dalam Pelindungan Anak, ditetapkan 27 Maret 2025, dan aturan teknisnya Permenkomdigi Nomor 9 Tahun 2026, berlaku sejak 6 Maret 2026. Aturan teknis mengatur batas usia minimum, penilaian risiko produk, layanan, dan fitur, verifikasi usia, desain perlindungan, klasifikasi akun anak, jejaring sosial, pengawasan, pengaduan, dan kewajiban penyelenggara sistem elektronik. Pemerintah mulai menerapkan penonaktifan atau pembatasan akun anak di bawah 16 tahun pada platform digital berisiko tinggi, khususnya media sosial dan layanan jejaring, mulai 28 Maret 2026 (Kementerian Komunikasi dan Digital Republik Indonesia, 2026a, 2026b). Rincian cakupan harus selalu merujuk naskah hukum dan penetapan risiko resmi, sebab tidak semua layanan digital memiliki klasifikasi yang sama.

PP TUNAS dan pembatasan usia: tujuan serta batasnya

Kebijakan pembatasan akun pada layanan berisiko tinggi dirancang untuk mengurangi paparan anak terhadap fitur dan praktik yang belum sesuai usia, serta mendorong tanggung jawab platform. Kebijakan ini menggeser beban dari keluarga saja kepada perusahaan yang mengoperasikan layanan dan negara yang mengawasi. Dalam penjelasan pemerintah, layanan yang masuk tahap awal mencakup sejumlah media sosial dan layanan jejaring populer.

Aturan juga mensyaratkan penyelenggara melakukan penilaian mandiri, verifikasi, menetapkan profil risiko, dan menerapkan langkah perlindungan. Penting bagi publik untuk memahami bahwa pendekatan ini tidak identik dengan pemutusan internet anak secara umum. Tujuan yang dinyatakan adalah pengelolaan akses berdasarkan profil risiko dan rentang usia, dengan kewajiban platform yang berbeda menurut jenis layanan.

Pembatasan usia memiliki keterbatasan. Anak dapat menggunakan akun milik orang lain, berpindah ke aplikasi yang tidak terklasifikasi, atau mengakses layanan tanpa mendaftar. Sistem age assurance dapat salah mengklasifikasikan anak dan orang dewasa, meminta data sensitif, atau menutup akses ke layanan pendidikan dan dukungan. Aturan yang terlalu mengandalkan usia dapat mengabaikan perbedaan kematangan dan kebutuhan anak, sekaligus mendorong eksploitasi data identitas. Karena itu kebijakan perlu dikombinasikan dengan desain aman untuk semua usia, pengaturan privasi default, kontrol pesan dan rekomendasi, saluran pengaduan, transparansi, dan pendidikan. Anak perlu diberi penjelasan tentang alasan kebijakan, cara banding jika terjadi kesalahan, dan pilihan akses terhadap informasi yang sah dan sesuai kebutuhannya.

Pelaksanaan kebijakan dan akuntabilitas platform

Pada evaluasi enam bulan PP TUNAS yang disampaikan Komdigi pada September 2026, pemerintah melaporkan 252 produk, layanan, dan fitur dari 94 penyelenggara sistem elektronik telah menyelesaikan penilaian mandiri sampai 6 September. Dari jumlah tersebut, 60 telah melalui verifikasi dan 42 ditetapkan profil risikonya; pemerintah menyatakan sekitar 28 juta anak telah memperoleh perlindungan melalui sejumlah langkah platform. Komdigi juga menyebut masih ada penyelenggara yang belum memenuhi kewajiban dan memberi kesempatan menyelesaikan penilaian mandiri hingga 31 Desember 2026 (Kementerian Komunikasi dan Digital Republik Indonesia, 2026c). Angka-

angka ini merupakan laporan administratif pemerintah dan perlu dibedakan dari evaluasi independen tentang perubahan pengalaman, paparan risiko, atau hasil kesejahteraan anak.

Akuntabilitas platform harus menguji apakah kebijakan benar-benar menurunkan risiko dan memperbaiki respons, bukan hanya apakah formulir telah diisi. Platform perlu menerbitkan ringkasan penilaian risiko, jumlah dan jenis laporan, waktu respons, tindakan terhadap pelanggaran, tingkat banding yang berhasil, kesalahan klasifikasi usia, dan insiden kebocoran data dengan perlindungan identitas. Data harus diaudit pihak independen dan dapat diperiksa regulator. Anak serta organisasi perlindungan anak perlu dilibatkan dalam pengujian pengalaman pelaporan dan pengaturan privasi. Transparansi tidak berarti membuka data pribadi korban atau memberi pelaku panduan menghindari moderasi. Pelaporan agregat yang memadai memungkinkan publik mengetahui apakah kewajiban platform berdampak nyata dan apakah perlu ada penyesuaian kebijakan.

Tanggung jawab platform: safety by design

Perlindungan yang baik dimulai ketika layanan dirancang, bukan setelah seorang anak mengalami kerugian. Safety by design mengharuskan tim produk mempertimbangkan risiko sejak pengembangan fitur, menguji dampak terhadap kelompok usia berbeda, dan mengurangi pengaturan yang secara default meningkatkan paparan. Contohnya ialah akun anak bersifat privat sejak awal, lokasi tidak dibagikan secara otomatis, pesan dari orang asing dibatasi, rekomendasi konten sensitif dibatasi, iklan tertarget tidak mengeksploitasi profil anak, dan notifikasi tidak mendorong penggunaan tanpa henti. Tombol lapor dan blokir perlu mudah ditemukan; pelaporan harus menjelaskan langkah berikutnya dan menyediakan bantuan manusia untuk kasus berat. Prinsip ini memindahkan perlindungan dari pilihan individu yang rumit menjadi tanggung jawab teknis penyedia layanan.

Desain aman tidak cukup jika algoritma tetap mengutamakan keterlibatan tanpa memeriksa konsekuensinya. Sistem rekomendasi dapat mengulang konten yang membuat pengguna bertahan, termasuk materi ekstrem atau yang memperburuk citra tubuh, kecemasan, dan kebencian. Platform perlu menilai bagaimana sinyal keterlibatan bekerja bagi anak, mengurangi penguatan konten berisiko, memberi kontrol rekomendasi yang mudah, dan tidak menggunakan pola gelap yang mendorong pembelian atau berbagi data. Pengujian harus mempertimbangkan bias terhadap bahasa daerah, ekspresi budaya, disabilitas, dan kelompok minoritas. Bila platform mendeteksi kemungkinan anak berada dalam bahaya, respons harus memprioritaskan dukungan dan rujukan, bukan sekadar menghapus unggahan lalu menutup kasus.

Peran keluarga: pendampingan dan kepercayaan

Keluarga berperan penting karena anak memerlukan hubungan aman untuk bertanya dan menceritakan pengalaman yang membuat tidak nyaman. Pendampingan efektif bukan pemeriksaan diam-diam terhadap setiap pesan, melainkan percakapan rutin tentang aplikasi yang digunakan, teman online, cara kerja rekomendasi, batas berbagi informasi, dan pilihan meminta bantuan. Aturan keluarga dapat disepakati bersama: kapan gawai digunakan, bagaimana menjaga tidur, aplikasi mana yang sesuai usia, dan apa yang dilakukan saat menerima pesan mengganggu. Anak lebih mungkin meminta pertolongan jika tidak takut langsung dimarahi atau kehilangan akses perangkat. Orang tua dapat mencontohkan perilaku digital yang sehat, menghargai privasi anak, dan meminta izin sebelum mengunggah foto atau cerita tentang mereka.

Kontrol orang tua dapat membantu, tetapi tidak menggantikan desain platform dan kebijakan publik. Pemantauan rahasia yang berlebihan dapat merusak kepercayaan, mendorong anak menyembunyikan masalah, dan membuat anak yang lebih tua kehilangan ruang perkembangan. Penggunaan

kontrol perlu disesuaikan dengan usia dan risiko, dijelaskan secara terbuka, serta ditinjau bersama anak. Keluarga juga berbeda dalam waktu, kemampuan digital, dan akses perangkat; karena itu kebijakan tidak boleh menganggap setiap anak memiliki satu orang tua yang selalu tersedia. Dukungan bagi pengasuh, materi edukasi singkat, serta saluran bantuan harus diberikan melalui sekolah, layanan kesehatan, dan komunitas. Relasi yang responsif melengkapi perangkat teknis: anak belajar mengambil keputusan, bukan hanya tunduk pada larangan.

Sekolah sebagai ruang literasi dan kewargaan digital

Sekolah dapat mengembangkan literasi digital yang menggabungkan keterampilan teknis, penilaian informasi, keamanan, etika, dan partisipasi. Anak perlu belajar membaca sumber, mengenali iklan dan konten sintetis, memahami bahwa jumlah pengikut bukan ukuran kebenaran, menjaga kata sandi, dan mengetahui batas berbagi data. Pendidikan kewargaan digital juga mengajarkan cara berdebat tanpa merendahkan, menyampaikan kritik, melindungi teman, serta mengoreksi informasi yang keliru. Materi harus dekat dengan pengalaman anak dan tidak hanya berupa ceramah tentang bahaya. Simulasi pelaporan, diskusi kasus, proyek membuat konten bermanfaat, dan konsultasi dengan organisasi anak dapat meningkatkan kemampuan menerapkan pengetahuan dalam situasi nyata.

Sekolah memerlukan prosedur penanganan insiden yang melindungi korban dari stigma. Guru perlu mengetahui cara mendokumentasikan kejadian, menjaga bukti, berkomunikasi dengan keluarga, dan merujuk kasus kepada layanan yang tepat. Sekolah hendaknya tidak menyita perangkat atau mempermalukan anak di depan kelas sebagai respons otomatis. Jika konflik terjadi di luar jam sekolah tetapi berdampak pada keselamatan atau proses belajar, sekolah dapat bekerja sama dengan pihak terkait tanpa mengambil alih seluruh ranah privat anak. Kebijakan perangkat harus menjamin akses belajar

bagi siswa yang tidak memiliki gawai. Pendidikan digital juga perlu memasukkan suara siswa dan menjelaskan batas penggunaan data sekolah, aplikasi pembelajaran, serta rekaman aktivitas mereka.

Peran pemerintah dan koordinasi layanan

Pemerintah pusat bertanggung jawab menetapkan standar, mengawasi platform, mengatur klasifikasi risiko, mengembangkan sistem pengaduan, dan menegakkan sanksi sesuai hukum. Pemerintah daerah perlu memastikan layanan pendampingan, perlindungan sosial, konseling, dan rujukan tersedia dekat dengan anak. Komunikasi antara kementerian, kepolisian, lembaga perlindungan anak, pendidikan, kesehatan, serta pemerintah lokal perlu memiliki protokol dan titik kontak yang jelas. Tanpa koordinasi, anak dapat diminta menceritakan ulang pengalaman kepada banyak petugas atau kasus berhenti di tengah rujukan. Layanan terpadu harus menjelaskan apa yang akan terjadi setelah laporan, siapa yang menjaga kerahasiaan, dan bagaimana keluarga dapat memperoleh informasi tentang kemajuan penanganan.

Penegakan juga membutuhkan kapasitas teknis. Pengawas harus memahami audit algoritma, perlindungan data, keamanan informasi, dan pengalaman anak. Regulator perlu memiliki kewenangan dan sumber daya untuk memeriksa bukti, meminta penjelasan platform, dan menindaklanjuti pengaduan. Mekanisme sanksi harus bertahap dan proporsional, tetapi cukup kuat untuk mendorong kepatuhan, termasuk tindakan terhadap pelanggaran berulang atau kelalaian serius. Pemerintah perlu mempublikasikan keputusan dan dasar penetapan risiko secara transparan. Konsultasi publik dengan anak dan pakar independen membantu memastikan bahwa regulasi tidak hanya efektif di atas kertas, tetapi juga dapat diterapkan tanpa mengorbankan akses informasi, kebebasan berekspresi, atau privasi.

Mekanisme pengaduan dan pemulihan

Sistem pelaporan yang baik mudah ditemukan, menyediakan bahasa yang jelas, dapat diakses oleh penyandang disabilitas, dan memungkinkan anak meminta bantuan dengan atau tanpa pendamping. Anak perlu tahu perbedaan antara melaporkan konten, akun, ancaman, eksploitasi, dan keadaan darurat. Platform sebaiknya memberikan nomor kasus, perkiraan waktu respons, status tindak lanjut, dan cara mengajukan banding. Untuk pelaporan pelanggaran privasi, anak dan wali perlu dapat meminta koreksi atau penghapusan data sesuai dasar hukum. Penanganan kasus harus meminimalkan pengumpulan data korban, membatasi akses staf, dan mencegah materi berbahaya tersebar melalui proses verifikasi.

Pemulihan tidak sama dengan menurunkan konten. Korban perundungan atau eksploitasi mungkin membutuhkan konseling, dukungan keluarga, bantuan hukum, perlindungan dari ancaman, dan pemulihan hubungan sosial. Layanan harus tersedia tanpa menyalahkan korban atau memaksanya melakukan mediasi dengan pelaku. Proses peradilan yang melibatkan anak perlu ramah anak, menjaga identitas, dan menghindari pertanyaan berulang yang tidak diperlukan. Platform harus bertanggung jawab mempertahankan bukti secara sah ketika ada dugaan tindak pidana, sambil menjaga agar akses terhadap data dibatasi. Evaluasi keberhasilan penanganan perlu mengukur keselamatan setelah tindakan, kualitas komunikasi, dan kepuasan korban atas proses, bukan sekadar berapa banyak konten yang dihapus.

AI generatif, deepfake, dan manipulasi

Perkembangan kecerdasan buatan menambah kemungkinan anak membuat karya, menerjemahkan materi, memperoleh bantuan belajar, dan berpartisipasi dalam komunitas kreatif. Namun teknologi generatif juga dapat digunakan untuk membuat gambar intim palsu, meniru suara, menyebarkan identitas, melakukan penipuan, atau membuat konten yang mengeksploitasi

anak. Deepfake dapat merusak reputasi walaupun gambar tersebut tidak autentik; korban tetap dapat mengalami trauma dan pemerasan. Platform harus menyediakan deteksi dan pelaporan yang sesuai, prosedur penghapusan cepat, pelabelan konten sintetis, dan perlindungan terhadap penggunaan wajah atau suara tanpa izin. Sistem harus dirancang agar anak tidak harus membuktikan sendiri bahwa materi yang dibuat secara sintetis adalah palsu sebelum mendapat bantuan.

Literasi AI perlu membantu anak memahami bahwa keluaran generatif dapat keliru, bias, atau dimanipulasi. Anak perlu mengetahui bahwa mengunggah foto teman untuk membuat gambar baru tanpa izin dapat melanggar hak dan menimbulkan bahaya. Sekolah dapat mengajarkan penggunaan AI yang menghormati privasi, persetujuan, dan atribusi, serta cara melaporkan deepfake. Pemerintah perlu memetakan risiko yang berubah cepat, berkonsultasi dengan pakar dan komunitas anak, serta menghindari larangan menyeluruh terhadap teknologi yang bermanfaat. Tanggung jawab utama tetap pada pelaku dan penyedia layanan; pendidikan bukan cara untuk memindahkan kewajiban pencegahan dari institusi kepada anak yang menjadi sasaran.

Risiko overregulasi dan prinsip proporsionalitas

Perlindungan dapat menimbulkan efek samping jika aturan terlalu luas atau tidak transparan. Verifikasi usia yang invasif dapat memaksa seluruh pengguna, termasuk orang dewasa, mengunggah identitas. Penyaringan yang berlebihan dapat menghapus informasi kesehatan, pendidikan, bantuan kekerasan, atau suara kelompok minoritas. Pemblokiran akses tanpa mekanisme keberatan dapat membuat anak kehilangan ruang dukungan. Kebijakan yang tidak disertai evaluasi juga dapat mendorong migrasi ke platform yang kurang diawasi. Karena itu setiap pembatasan perlu diuji atas tujuan sah, kebutuhan, proporsionalitas, dampak terhadap kelompok berbeda, perlindungan data, dan

prosedur banding. Penilaian semacam ini tidak meniadakan perlindungan; ia membuat perlindungan lebih akurat dan dapat dipertanggungjawabkan.

Regulator harus menjaga keseimbangan antara kewajiban platform dan kebebasan pengguna. Pembatasan konten harus menjelaskan kategori yang dilarang dan alasan, menyediakan proses tinjauan manusia, serta mencegah penggunaan kebijakan keselamatan untuk menekan kritik. Pengawasan independen dapat memeriksa angka kesalahan penghapusan dan dampak kebijakan terhadap akses. Bila verifikasi usia diperlukan, metode yang lebih menjaga privasi seperti token usia atau verifikasi di perangkat perlu dievaluasi dibandingkan pengumpulan salinan identitas terpusat. Anak dan orang tua harus memperoleh informasi sederhana tentang cara meminta koreksi. Prinsip proporsionalitas mengharuskan negara memilih cara yang paling sedikit membatasi hak untuk mencapai tingkat keselamatan yang diperlukan.

Indikator evaluasi kebijakan

Evaluasi perlindungan anak di media sosial perlu bergerak melampaui jumlah akun yang ditutup atau platform yang menandatangani komitmen. Indikator dampak dapat mencakup frekuensi dan waktu respons terhadap laporan, proporsi kasus yang memperoleh tindak lanjut, insiden berulang, akses terhadap layanan pemulihan, pemahaman anak tentang cara mencari bantuan, serta persepsi rasa aman. Indikator desain dapat menilai apakah akun anak bersifat privat secara default, apakah pesan dari orang asing dibatasi, apakah rekomendasi konten berisiko dikurangi, dan apakah iklan tertarget dibatasi. Indikator hak meliputi kesalahan verifikasi usia, permintaan data yang tidak perlu, penghapusan konten sah, akses kelompok rentan, dan kualitas partisipasi anak dalam evaluasi.

Data harus dipilah menurut usia, gender, disabilitas, wilayah, dan kondisi sosial dengan perlindungan privasi yang ketat. Peningkatan laporan tidak selalu berarti keselamatan memburuk; bisa jadi anak mulai percaya pada mekanisme

pelaporan. Sebaliknya, penurunan laporan dapat terjadi karena rasa takut atau saluran yang tidak berfungsi. Karena itu statistik harus dipadukan dengan survei pengalaman, wawancara aman, audit independen, dan penilaian dampak hak anak. Pemerintah perlu menerbitkan metodologi dan keterbatasan data agar angka tidak dipakai secara berlebihan. Anak, organisasi masyarakat, akademisi, dan penyedia layanan perlu mendapatkan ruang menilai hasil dan merekomendasikan perbaikan kebijakan secara berkala.

Contoh penerapan: kasus hipotetis

Misalkan seorang siswa kelas delapan membuat unggahan tentang masalah sampah di lingkungan sekolah. Unggahan itu mendapat perhatian luas, kemudian beberapa akun anonim mengejek dan menyebarkan lokasi rumahnya. Respons yang hanya meminta siswa menghapus akun dapat membatasi partisipasinya dan membiarkan ancaman tetap ada. Langkah lebih baik dimulai dengan memastikan keselamatan, menyimpan bukti secara terbatas, melaporkan akun pengancam, meninjau pengaturan lokasi, dan menghubungkan siswa dengan orang dewasa tepercaya. Sekolah dapat membantu menghentikan perundungan dan menyediakan dukungan tanpa menyuruh siswa berhenti mengkritik. Platform perlu menilai sebaran ancaman, memberi kabar tentang tindak lanjut, dan mencegah akun yang sama mengulangi tindakan.

Contoh lain ialah anak yang menerima permintaan foto pribadi dari akun yang mengaku seusia. Pengasuh sebaiknya tidak menyalahkan atau menghukum anak karena menanggapi pesan. Mereka perlu mengamankan anak, menghentikan komunikasi, menghindari menyebarkan materi, dan menghubungi saluran yang tepat. Platform harus menyediakan jalur pelaporan eksploitasi yang cepat dan menjaga bukti sesuai hukum. Pendamping profesional membantu menentukan kebutuhan perlindungan, kesehatan, serta dukungan psikologis. Dalam kedua contoh, keselamatan tidak menghapus hak

anak untuk berbicara; ia memastikan partisipasi berlangsung tanpa ancaman dan memungkinkan anak tetap belajar menggunakan teknologi secara bertanggung jawab.

Agenda kebijakan dan prioritas pelaksanaan

Prioritas pertama ialah memastikan kewajiban platform diterapkan secara terukur: penilaian risiko yang substantif, desain aman, pengaturan privasi default, pembatasan kontak yang berisiko, dan pengaduan yang efektif. Prioritas kedua ialah membangun layanan pemulihan lintas sektor agar anak yang mengalami bahaya segera memperoleh dukungan. Prioritas ketiga ialah memperkuat literasi digital dan kewargaan di sekolah serta keluarga, dengan materi yang sesuai usia dan konteks lokal. Prioritas keempat ialah memastikan verifikasi usia meminimalkan data dan memiliki mekanisme koreksi. Prioritas kelima ialah menyertakan suara anak dalam perumusan kebijakan, evaluasi fitur, dan penilaian pengalaman. Semua prioritas memerlukan anggaran, petugas, koordinasi, dan publikasi kemajuan.

Kebijakan juga perlu ditinjau berkala karena platform, fitur, dan pola risiko berubah. Pemerintah dapat menerbitkan laporan tahunan tentang kepatuhan platform, insiden, hasil pengaduan, kesenjangan wilayah, serta dampak terhadap hak partisipasi dan informasi. Peninjauan perlu melibatkan kelompok anak yang beragam, termasuk anak penyandang disabilitas dan anak dari daerah dengan akses terbatas. Jika suatu langkah mengurangi satu risiko tetapi menciptakan hambatan serius lainnya, kebijakan perlu diubah berdasarkan bukti. Regulasi yang responsif tidak berarti berubah tanpa arah; ia menjaga prinsip hak anak sambil menyesuaikan instrumen terhadap perubahan teknologi dan pengalaman nyata pengguna.

Anak sebagai pencipta konten dan hak atas citra

Anak bukan hanya konsumen konten; banyak yang membuat video, siaran, musik, ulasan, tutorial, atau dokumentasi kegiatan sehari-hari. Produksi kreatif dapat mengembangkan kemampuan komunikasi, literasi media, dan peluang ekonomi. Namun publikasi anak juga membawa konsekuensi privasi, persetujuan, reputasi, dan keselamatan jangka panjang. Konten yang dibuat pada usia muda dapat disalin atau ditempatkan ulang tanpa konteks, kemudian ditemukan kembali pada masa dewasa. Karena itu anak perlu memperoleh penjelasan yang sesuai usia tentang audiens, pengaturan visibilitas, komentar, lokasi, dan permanensi konten. Platform harus memberi pilihan untuk menghapus, membatasi, atau meninjau ulang unggahan dan data yang melibatkan anak, dengan proses yang tidak berbelit.

Hak anak atas citra dan privasi juga berlaku dalam praktik berbagi oleh orang dewasa. Orang tua, sekolah, lembaga sosial, bahkan organisasi publik dapat mengunggah foto anak untuk dokumentasi atau promosi tanpa benar-benar mempertimbangkan persetujuan dan jangkauan publikasi. Praktik sharenting dapat membuka informasi tentang lokasi, kebiasaan, kondisi kesehatan, atau rutinitas anak. Sebelum mengunggah, orang dewasa perlu mempertimbangkan apakah publikasi diperlukan, siapa yang dapat melihatnya, dan apakah anak dapat menyampaikan keberatan. Untuk konten promosi atau kegiatan komersial, persetujuan harus jelas dan penggunaan gambar tidak boleh menjadi syarat anak memperoleh layanan. Kebijakan perlindungan perlu mencakup tanggung jawab lembaga dan orang dewasa, bukan hanya perilaku anak.

Komersialisasi perhatian dan anak sebagai influencer

Ekonomi kreator membuat sebagian anak memperoleh penghasilan atau hadiah dari konten dan kerja sama merek. Aktivitas tersebut dapat menjadi bentuk ekspresi dan keterampilan, tetapi juga menimbulkan risiko eksploitasi

kerja, tekanan untuk selalu tampil, pengawasan berlebihan oleh pengelola, dan ketidakjelasan kepemilikan pendapatan. Anak mungkin tidak mempunyai kuasa menentukan jadwal produksi, jenis konten, atau apakah informasi pribadi mereka akan dibagikan. Penonton dapat mendorong anak membagikan cerita yang semakin intim demi keterlibatan. Orang dewasa yang mengelola akun perlu mengutamakan kepentingan anak, waktu sekolah dan istirahat, persetujuan yang dapat ditarik, dan penyimpanan hasil ekonomi bagi anak sesuai hukum yang berlaku.

Platform dan pengiklan juga berperan dalam membentuk dorongan komersial. Iklan terselubung, pembelian dalam aplikasi, hadiah virtual, dan rekomendasi yang memanfaatkan minat anak dapat membuat batas antara hiburan, persahabatan, dan transaksi menjadi kabur. Penjelasan iklan harus mudah dikenali oleh anak; desain tidak boleh menekan mereka untuk membeli atau meminta orang tua terus-menerus. Data anak tidak seharusnya digunakan untuk mengeksploitasi kerentanan emosional atau membuat profil komersial yang tidak diperlukan. Regulator perlu memastikan klasifikasi konten bersponsor, perlindungan konsumen anak, dan mekanisme pengaduan. Perlindungan anak dalam ekonomi kreator harus menjaga kesempatan berekspresi sambil mencegah keuntungan pihak dewasa dibangun dari paparan anak yang tidak terkendali.

Privasi dalam verifikasi usia dan tata kelola identitas

Penegakan batas usia menghadirkan dilema desain yang nyata. Platform perlu mencegah anak masuk ke fitur yang diklasifikasikan berisiko tinggi, tetapi cara memastikan usia dapat menciptakan kumpulan data baru. Penggunaan kartu identitas, biometrik wajah, atau informasi keluarga menimbulkan risiko kebocoran dan penyalahgunaan. Kesalahan juga mungkin terjadi, misalnya orang dewasa ditolak atau anak berhasil lolos dengan identitas orang lain. Sistem yang baik seharusnya hanya memberi sinyal minimum bahwa batas usia

tertentu terpenuhi, tidak menyimpan bukti lebih lama daripada yang diperlukan, dan menawarkan jalur peninjauan jika keputusan keliru. Proses ini harus diaudit oleh otoritas perlindungan data dan regulator digital.

Privasi dan keselamatan tidak selalu memiliki hubungan yang sederhana. Pengumpulan data lebih banyak tidak otomatis menghasilkan perlindungan lebih baik; data yang dikumpulkan dapat meningkatkan risiko anak. Sebaliknya, verifikasi yang terlalu lemah mungkin gagal mendeteksi risiko di layanan tertentu. Karena itu setiap sistem harus melewati penilaian dampak pelindungan data dan hak anak, serta diuji pada kelompok dengan beragam warna kulit, kemampuan, bahasa, dan kondisi perangkat. Alternatif seperti verifikasi di perangkat, token usia, atau pengesahan pihak tepercaya dapat dipertimbangkan jika memenuhi standar keamanan dan aksesibilitas. Anak serta wali harus diberi penjelasan tentang data yang diproses dan cara meminta koreksi tanpa kehilangan hak akses pada layanan yang sah.

Ekosistem media dan pengaruh algoritma pada opini anak

Media sosial bukan sekadar saluran netral yang menyampaikan semua informasi secara setara. Algoritma mengurutkan konten berdasarkan sinyal tertentu, seperti interaksi, waktu tonton, kedekatan jaringan, dan prediksi minat. Hasilnya dapat membuat sebagian pandangan lebih terlihat dan yang lain tenggelam. Bagi anak, paparan berulang dapat membentuk persepsi mengenai tubuh, kelompok sosial, kesehatan, politik, atau apa yang dianggap normal. Platform perlu menjelaskan dengan bahasa sederhana mengapa konten direkomendasikan dan menyediakan kontrol yang nyata untuk mengubah rekomendasi. Pengguna anak sebaiknya tidak didorong menuju kelompok atau materi berisiko melalui rangkaian rekomendasi otomatis yang tidak dapat mereka pahami atau hentikan.

Dalam demokrasi, algoritma dapat memperluas informasi dan mempertemukan anak dengan komunitas yang mendukung, tetapi juga

menguatkan misinformasi atau konflik. Pendidikan perlu menjelaskan bahwa hasil pencarian dan feed bukan cerminan lengkap dunia, melainkan hasil pemilihan sistem yang mempunyai tujuan dan keterbatasan. Anak dapat membandingkan sumber, mencari konteks, memeriksa tanggal, dan menilai bukti sebelum membagikan klaim. Regulator perlu meminta platform menguji risiko sistemik terhadap anak, termasuk dampak rekomendasi, iklan, dan fitur interaksi. Pengawasan harus menjaga rahasia dagang yang sah tanpa menjadikan algoritma kotak hitam yang tidak dapat diperiksa ketika ada dampak serius terhadap hak anak.

Rancangan layanan publik yang ramah anak

Layanan publik digital semakin sering digunakan anak untuk belajar, mengakses bantuan, berkomunikasi dengan sekolah, atau melaporkan kekerasan. Karena layanan tersebut dapat mengumpulkan data sensitif, standar perlindungan perlu berlaku juga pada aplikasi pendidikan, kesehatan, dan administrasi publik. Anak harus mengetahui data apa yang dikumpulkan dan untuk tujuan apa, sedangkan orang tua atau wali perlu memperoleh informasi yang memadai tanpa menghapus ruang privasi anak sesuai tahap perkembangannya. Sistem tidak seharusnya menampilkan iklan atau menggunakan aktivitas anak untuk pelatihan produk komersial tanpa dasar hukum dan perlindungan yang kuat. Pengadaan aplikasi publik perlu mensyaratkan keamanan, aksesibilitas, minimisasi data, dan audit yang independen.

Kanal pelaporan daring untuk anak harus dirancang agar tidak menambah hambatan. Formulir panjang, istilah hukum, keharusan menyertakan banyak bukti, atau kewajiban memiliki akun dapat membuat anak berhenti meminta bantuan. Layanan perlu menyediakan pilihan berbicara langsung dengan petugas terlatih, mode komunikasi yang aman, informasi mengenai kerahasiaan, dan rujukan yang jelas. Jika laporan menyangkut ancaman segera,

sistem harus membedakannya dari pengaduan rutin serta mengarahkan kepada layanan darurat. Pemerintah daerah perlu menguji alur layanan dengan anak sebelum peluncuran. Pengalaman pengguna anak, bukan hanya kepatuhan teknis, harus menjadi ukuran apakah layanan publik digital benar-benar mudah diakses.

Kapasitas anak dan pengambilan keputusan sesuai usia

Pengakuan terhadap kapasitas anak yang berkembang berarti keputusan perlindungan perlu disesuaikan dengan usia dan kemampuan memahami konsekuensi. Anak kecil mungkin memerlukan pembatasan lebih besar terhadap kontak dan pengumpulan data; remaja membutuhkan ruang privat, akses informasi yang lebih luas, dan kesempatan berlatih mengambil keputusan. Tidak ada satu tingkat pengawasan yang tepat bagi semua keluarga atau semua anak. Kebijakan dapat menetapkan batas perlindungan dasar, sementara fitur dan pendampingan disesuaikan melalui penilaian risiko dan percakapan. Anak perlu memahami alasan pembatasan dan dapat menyampaikan keberatan. Pendekatan ini membangun kemampuan mengelola risiko secara bertahap, bukan menciptakan ketergantungan permanen pada pengawasan orang dewasa.

Kapasitas berkembang tidak berarti anak harus dibiarkan menanggung bahaya sendiri. Platform tetap memiliki kewajiban desain dan negara tetap bertanggung jawab mengatur penyedia layanan. Namun anak perlu mendapatkan alat yang membuatnya mampu bertindak: mengubah pengaturan privasi, memblokir, melaporkan, meminta bantuan, menyimpan bukti dengan aman, dan mengenali manipulasi. Kemampuan ini harus diajarkan tanpa menyalahkan korban atas pilihan yang dibuatnya. Ketika terjadi insiden, pertanyaan utamanya bukan mengapa anak tidak lebih berhati-hati, melainkan bagaimana sistem dapat mencegah, mempercepat pertolongan, dan mengurangi pengulangan. Pendidikan berbasis hak membuat anak lebih siap

dan tetap menempatkan tanggung jawab utama pada pihak yang mengendalikan produk dan lingkungan.

Kerja sama lintas sektor dan pembelajaran kebijakan

Perlindungan di media sosial melibatkan lembaga yang memiliki fungsi berbeda. Regulator digital mengawasi platform dan tata kelola sistem; lembaga perlindungan anak menangani hak serta layanan korban; sekolah membangun literasi dan merespons dampak pada pembelajaran; aparat menangani dugaan tindak pidana; layanan kesehatan membantu kebutuhan fisik dan mental; organisasi masyarakat mendampingi anak dan keluarga. Agar kerja sama tidak berhenti pada nota kesepahaman, perlu ada protokol pembagian kasus, pertukaran informasi yang terbatas, mekanisme eskalasi, dan standar kerahasiaan. Anak dan keluarga harus diberi satu titik kontak yang jelas agar tidak harus memahami struktur birokrasi sebelum menerima bantuan.

Kebijakan sebaiknya diperlakukan sebagai proses belajar. Pemerintah dapat menguji prosedur pada beberapa jenis layanan, mengevaluasi pengalaman anak, lalu memperbaiki standar sebelum perluasan. Evaluasi harus mencakup kelompok yang sering tak terlihat, termasuk anak di daerah tertinggal, anak penyandang disabilitas, anak dalam pengasuhan alternatif, dan anak yang mengalami kekerasan. Temuan perlu diumumkan dengan bahasa yang dapat dipahami publik, sementara identitas dan detail sensitif tetap dilindungi. Mekanisme koreksi harus memungkinkan anak, orang tua, guru, dan organisasi menyampaikan kegagalan sistem. Dengan siklus pembelajaran yang terbuka, aturan dapat menyesuaikan perubahan teknologi tanpa mengorbankan prinsip dasar hak dan keselamatan.

Penutup: perlindungan yang memungkinkan anak bersuara

Demokrasi digital memberi anak peluang untuk belajar, berjejaring, berkarya, dan menyampaikan pandangan tentang dunia yang mereka hidupi. Kesempatan tersebut berjalan beriringan dengan risiko eksploitasi, perundungan, manipulasi, pelanggaran privasi, paparan konten berbahaya, dan dampak terhadap kesejahteraan. Bukti penelitian menunjukkan perlunya kewaspadaan, tetapi juga mengingatkan bahwa dampak media sosial tidak seragam dan tidak dapat disimpulkan hanya dari durasi layar. Perlindungan yang adil menggabungkan keselamatan, privasi, akses informasi, kebebasan berekspresi, dan partisipasi yang sesuai dengan kapasitas anak.

Indonesia telah memiliki PP TUNAS dan Permenkomdigi Nomor 9 Tahun 2026 sebagai dasar tata kelola platform dan pendekatan berbasis risiko, termasuk aturan usia untuk layanan berisiko tinggi. Tahap berikutnya adalah memastikan kewajiban tersebut benar-benar mengurangi risiko melalui desain aman, pengawasan independen, layanan pemulihan, literasi, dan akuntabilitas yang transparan. Keluarga dan sekolah perlu mendampingi tanpa meniadakan kepercayaan; pemerintah harus menegakkan aturan tanpa membatasi kritik yang sah; platform harus bertanggung jawab atas desain dan dampak layanannya; anak harus dilibatkan dalam keputusan yang memengaruhi mereka. Demokrasi digital yang matang bukan ruang tanpa risiko, melainkan ruang yang mengelola risiko sehingga anak dapat aman sekaligus tetap memiliki suara.

Glossarium

Age assurance — Metode untuk memperkirakan atau memverifikasi usia pengguna; harus akurat, proporsional, dan meminimalkan pengumpulan data.

Child rights by design — Penerapan hak dan kepentingan anak sejak tahap perancangan produk, fitur, algoritma, dan tata kelola.

Demokrasi digital — Pemanfaatan teknologi digital untuk komunikasi publik, akses informasi, deliberasi, advokasi, dan partisipasi warga.

Doxing — Pengungkapan data pribadi atau lokasi seseorang tanpa izin, sering kali untuk mengintimidasi atau mengundang serangan.

Jejak digital — Data dan rekaman aktivitas yang tertinggal ketika seseorang menggunakan layanan digital, baik dibuat sengaja maupun dikumpulkan otomatis.

Kepentingan terbaik anak — Prinsip bahwa keselamatan, perkembangan, hak, kebutuhan, dan pandangan anak harus menjadi pertimbangan utama dalam keputusan yang memengaruhinya.

Literasi digital — Kemampuan mengakses, memahami, mengevaluasi, membuat, dan membagikan informasi digital secara aman, kritis, etis, dan bertanggung jawab.

Moderasi konten — Proses menilai dan menangani konten atau perilaku yang melanggar aturan layanan atau hukum, dengan prosedur transparan dan mekanisme keberatan.

Partisipasi bermakna — Keterlibatan yang memberi anak ruang menyampaikan pandangan, audiens yang mendengar, serta pengaruh yang sesuai konteks dan usia.

Profil risiko PLF — Pengelompokan tingkat risiko produk, layanan, dan fitur digital untuk menentukan bentuk kewajiban perlindungan yang relevan.

Safety by design — Perancangan sistem yang mengantisipasi dan mengurangi risiko keselamatan sejak awal, bukan hanya menanggapi insiden setelah terjadi.

Verifikasi usia — Proses memeriksa apakah pengguna memenuhi batas usia tertentu; perlu menyediakan perlindungan privasi dan mekanisme koreksi kesalahan.

Daftar Pustaka

Disusun mengikuti APA edisi ke-7. DOI dicantumkan sebagai tautan doi.org; peraturan perundang-undangan dan dokumen kelembagaan dirujuk melalui sumber resmi.

Committee on the Rights of the Child. (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment (CRC/C/GC/25). United Nations. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

Indonesia. (1990). Keputusan Presiden Republik Indonesia Nomor 36 Tahun 1990 tentang Pengesahan Convention on the Rights of the Child (Konvensi tentang Hak-Hak Anak). https://peraturan.bpk.go.id/

Indonesia. (2002). Undang-Undang Republik Indonesia Nomor 23 Tahun 2002 tentang Perlindungan Anak. Lembaran Negara Republik Indonesia Tahun 2002 Nomor 109.

Indonesia. (2014). Undang-Undang Republik Indonesia Nomor 35 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 297.

Indonesia. (2022a). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Indonesia. (2024). Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1.

Indonesia. (2025). Peraturan Pemerintah Republik Indonesia Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik dalam Pelindungan Anak. Lembaran Negara Republik Indonesia Tahun 2025 Nomor 36. https://jdih.komdigi.go.id/produk_hukum/view/id/965/t/peraturan%20pemerintah%20nomor%2017%20tahun%202025

Indonesia. (2026). Peraturan Menteri Komunikasi dan Digital Republik Indonesia Nomor 9 Tahun 2026 tentang Peraturan Pelaksanaan Peraturan Pemerintah Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik dalam Pelindungan Anak. Berita Negara Republik Indonesia Tahun 2026 Nomor 163. https://jdih.komdigi.go.id/produk_hukum/view/id/1007/t/peraturan%2Bmenteri%2Bkomunikasi%2Bdan%2Bdigital%2Bnomor%2B9%2Btahun%2B2026

Kementerian Komunikasi dan Digital Republik Indonesia. (2026a, 6 Maret). Permen Komdigi terbit, pemerintah mulai implementasi perlindungan anak di platform digital. https://portal.komdigi.go.id/kanal-publik/berita-kini/10066

Kementerian Komunikasi dan Digital Republik Indonesia. (2026b, 6 Maret). Peraturan Menteri Komunikasi dan Digital Nomor 9 Tahun 2026 tentang peraturan pelaksanaan PP Nomor 17 Tahun 2025. JDIH Kemkomdigi. https://jdih.komdigi.go.id/produk_hukum/view/id/1007/t/peraturan%2Bm

enteri%2Bkomunikasi%2Bdan%2Bdigital%2Bnomor%2B9%2Btahun%2B2026

Kementerian Komunikasi dan Digital Republik Indonesia. (2026c, 15 September). Evaluasi 6 bulan PP TUNAS, 28 juta anak terlindungi, kepatuhan platform meningkat. InfoPublik. https://infopublik.id/kategori/siaran-pers/989065/index.html

Lundy, L. (2007). "Voice" is not enough: Conceptualising Article 12 of the United Nations Convention on the Rights of the Child. British Educational Research Journal, 33(6), 927–942. https://doi.org/10.1080/01411920701657033

Odgers, C. L., & Jensen, M. R. (2020). Annual research review: Adolescent mental health in the digital age: Facts, fears, and future directions. Journal of Child Psychology and Psychiatry, 61(3), 336–348. https://doi.org/10.1111/jcpp.13190

Orben, A. (2020). Teenagers, screens and social media: A narrative review of reviews and key studies. Social Psychiatry and Psychiatric Epidemiology, 55, 407–414. https://doi.org/10.1007/s00127-019-01825-4

Saleem, N., Young, P., & Yousuf, S. (2024). Exploring the relationship between social media use and symptoms of depression and anxiety among children and adolescents: A systematic narrative review. Cyberpsychology, Behavior, and Social Networking, 27(11), 767–778. https://doi.org/10.1089/cyber.2023.0456

UNICEF Indonesia. (2025, February). Online knowledge and practice of children in Indonesia: A baseline study 2023.

https://www.unicef.org/indonesia/child-protection/reports/online-knowledge-and-practice-children-indonesia-baseline-study-2023

United Nations. (1989). Convention on the Rights of the Child. Treaty Series, 1577, 3. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

Valkenburg, P. M., Meier, A., & Beyens, I. (2022). Social media use and its impact on adolescent mental health: An umbrella review of the evidence. Current Opinion in Psychology, 44, 58–68. https://doi.org/10.1016/j.copsyc.2021.08.017