

Pedoman untuk industri tentang Perlindungan Online Anak 2020





Penerjemahan ini didukung pendanaannya oleh UK Aid dari pemerintah Kerajaan Inggris.

This translation was funded by UK Aid from the UK government.

Terjemahan ini tidak dibuat oleh International Telecommunication Union (ITU) dan tidak dapat diperlakukan sebagai terjemahan resmi ITU.

This translation was not created by the International Telecommunication Union (ITU) and should not be considered an official ITU translation.

ITU tidak bertanggung jawab atas isi atau sembarang kesalahan dalam terjemahan ini.

The ITU shall not be liable for any content or error in this translation.

Kata Pengantar

Pedoman Perlindungan Online Anak



Puji dan syukur kepada Tuhan Yang Maha Esa atas berkatNYA maka telah diterbitkan suatu rangkaian panduan tentang perlindungan anak online yang khusus menyorot pengambil kebijakan, pelaku industri, guru dan orang tua, dan untuk anak-anak sendiri. Panduan ini ikut memperkaya proses penyusunan kebijakan tentang perlindungan anak di ranah daring.

Kemajuan teknologi saat ini membuat dunia sudah tanpa batas dan berpengaruh besar pada masyarakat termasuk anak. Bersama dengan potensi manfaatnya, akses konektivitas juga membawa peluang timbulnya pengaruh yang buruk terhadap anak. Maka diperlukan upaya-upaya untuk mengantisipasi dan melaksanakan perlindungan anak di ranah daring.

Kementerian Pemberdayaan Perempuan dan Perlindungan Anak (PPPA) saat ini tengah menyusun peta jalan perlindungan anak di ranah daring yang penting untuk segera diselesaikan demi mendorong terbentuknya regulasi untuk dipatuhi, dipedomani, dan dijadikan acuan oleh semua pihak dalam pencegahan dan penanganan akses konektivitas ke ranah daring. Ini termasuk kekerasan siber, screentime berlebihan yang tidak berimbang, dan perundungan siber.

Terima kasih saya sampaikan kepada International Telecommunication Union (ITU) yang membantu mendapatkan akses, dan Foreign and Commonwealth Development Organization dari Pemerintah Kerajaan Inggris (FCDO) atas dukungan pendanaan untuk penerbitan panduan-panduan yang penting ini. Penghargaan juga kepada Kementerian Komunikasi dan Informatika serta ID-COP dan lembaga-lembaga jejaringnya yang telah melaksanakan berbagai kegiatan untuk mengawal dan mengkoordinasi upaya berbagai pihak dalam penerbitan panduan-panduan ini.

Semoga panduan-panduan ini dapat memberikan manfaat dalam mewujudkan Pemenuhan Hak dan Perlindungan Anak di Indonesia.

Deputi Bidang Perlindungan Khusus Anak
Kementerian Pemberdayaan Perempuan
dan Perlindungan Anak (Kemen PPPA)

Nahar, SH, MSI

Kata Pengantar Kementerian Komunikasi dan Informatika



Pandemi Covid-19 telah mendorong seluruh kalangan untuk bermigrasi, berinteraksi, juga melakukan berbagai aktivitas di ruang digital secara aktif, termasuk pula anak-anak. Tidak dapat dipungkiri juga, teknologi digital telah menghadirkan banyak solusi baru di tengah keterbatasan sumber belajar dan fasilitas pembelajaran khususnya di era post-COVID-19. Hadirnya produk-produk pembelajaran yang dikemas secara digital membuka pintu-pintu terhadap berbagai ilmu dan pustaka yang lebih luas dan juga gratis untuk diakses oleh anak-anak kita.

Namun, layaknya pisau bermata dua, penggunaan teknologi yang tidak dibarengi dengan etika dan pemahaman yang komprehensif tentang ruang digital akan menimbulkan dampak buruk bagi anak-anak. Oleh sebab itu, Kementerian Komunikasi dan Informatika RI terus berupaya memasifkan edukasi literasi digital yang mencakup pada empat pilar literasi digital, yakni digital skills, digital ethics, digital culture, dan digital safety kepada seluruh lapisan masyarakat, khususnya kepada anak-anak hingga remaja.

Terbitnya serial buku ini tidak lain merupakan salah satu wujud nyata upaya kita dalam memberikan perlindungan anak di ranah daring, serta menjadi "amunisi baru" pada Program Nasional Literasi Digital. Apresiasi yang setinggi-tingginya kami sampaikan kepada International Telecommunication Union (ITU), Kementerian Pemberdayaan Perempuan dan Perlindungan Anak (Kemen PPPA), Foreign and Commonwealth Development Office dari Pemerintah Kerajaan Inggris (FCDO), ID-COP, GNLD Siberkreasi, dan seluruh pihak yang terlibat dalam penyusunan pedoman ini. Semoga serial buku ini dapat menjadi pedoman bagi kita semua dalam mengedukasi anak tentang perkembangan teknologi digital, sekaligus menjadi perisai yang selalu siap melindungi mereka dari kejahatan siber.

Salam literasi digital.

Jakarta, Oktober 2022

Semuel Abrijani Pangerapan
Direktur Jenderal Aplikasi Informatika, Kominfo

Kata Pengantar

Indonesia Child Online Protection (ID-COP)



Internet saat ini sudah digunakan oleh hampir seluruh lapisan masyarakat di dunia, tidak terkecuali di Indonesia. Bahkan sebagian besar anak-anak di Indonesia sudah mengenal dengan baik internet dan menjadi pengguna aktif. Internet merupakan dunia tersendiri bagi aktifitas online anak-anak untuk bermain, belajar, berkreaitifitas, berbagi dan berinteraksi satu sama lain. Apa yang ada di internet seakan merupakan dunia baru yang menarik untuk di eksplorasi oleh anak-anak kita. Dunia yang penuh tantangan dan peluang dalam tumbuh kembang anak-anak kita.

Apa yang ditawarkan di internet sejatinya adalah dunia tanpa batas, dimana kreatifitas, pengetahuan bisa diraih dengan kesungguhan anak untuk belajar dan mengembangkan diri. Sayangnya dunia online ini juga memiliki sisi rentan yang sering disalah gunakan oleh pihak-pihak yang tidak bertanggung jawab. Dan menjadi perangkap bagi anak-anak yang tidak memiliki pengetahuan memadai dalam beraktifitas di online dengan baik.

Sering kali kita menunjuk satu pihak sebagai pihak yang paling berperan dan bertanggung jawab memiliki kewajiban dalam melakukan perlindungan online anak. Namun sejatinya hal ini merupakan kewajiban semua pihak, tidak hanya di bebankan kepada orang tua sebagai pengasuh utama anak, pemerintah sebagai institusi yang memiliki kewenangan dan bertanggung jawab, industry digital yang memfasilitasi aktifitas anak dengan produk digital online nya ataupun tenaga pendidik yang setiap hari berinteraksi mengedukasi anak anak di sekolah, namun menjadi kewajiban seluruh komponen masyarakat.

Memahami kompleksitas dari upaya perlindungan anak online akan membangun kepekaan kita untuk mengupayakan yang terbaik dalam melindungi anak, mendorong peran industri, menggerakkan tenaga pendidik dan mengkapasitasi orang tua dalam mencari formula terbaiknya dalam melindungi anak saat online. Ditengah kekhawatiran orang tua, masyarakat, aparaturnegara dan juga industry IT, serial buku ini mengingatkan akan peran apa yang semestinya kita lakukan dalam melindungi anak kita agar tetap aman saat online.

Kami menyambut baik dan berterima kasih atas dedikasi International Telecommunication Union (ITU) dalam menerbitkan serial buku pedoman ataupun panduan mengenai perlindungan online anak yang ditujukan ke berbagai kalangan dalam versi bahasa indonesia. Semoga dapat menambah khasanah pengetahuan seluruh komponen masyarakat akan pentingnya upaya perlindungan online anak di Indonesia.

Terakhir, ID-COP sebagai sebuah wadah dari multi stakeholder dalam mengarus utamakan agenda perlindungan anak di dunia siber percaya bahwa membangun kolaborasi dengan semua pihak, menyediakan sumber daya dan literatur untuk perlindungan online anak, dan upaya edukasi serta advokasi akan mampu mewujudkan masyarakat Indonesia yang berdaya secara informasi sehingga mandiri dalam membangun dunia internet ramah anak. Kami berharap apa yang telah di lakukan ITU dapat memberikan dorongan dan menginspirasi pihak lain untuk melanjutkan dan meningkatkan upaya perlindungan online anak di Indonesia.

Jakarta, September 2022

Andy Ardian
Koordinator ID-COP

**Pedoman untuk industri
tentang Perlindungan Online
Anak**

Daftar Isi

Daftar Isi	v
1. Ikhtisar	1
2. Apa itu perlindungan online anak?	3
2.1 Informasi latar belakang	6
2.2 Model nasional dan transnasional yang ada untuk Perlindungan Online Anak	14
3. Bidang-bidang utama untuk melindungi dan mempromosikan hak-hak anak	17
3.1 Mengintegrasikan pertimbangan hak anak ke dalam semua kebijakan perusahaan dan proses manajemen yang tepat	17
3.2 Mengembangkan proses standar untuk menangani CSAM	19
3.4 Menciptakan lingkungan online yang lebih aman dan sesuai usia	22
3.5 Mendidik anak-anak, pengasuh dan pendidik tentang keselamatan anak-anak dan penggunaan TIK yang bertanggung jawab	24
3.6 Mempromosikan teknologi digital sebagai cara untuk meningkatkan keterlibatan masyarakat	27
4. Pedoman umum untuk industri	29
5. Daftar periksa terkait fitur	38
5.1 Fitur A: Menyediakan konektivitas, penyimpanan data, dan layanan hosting	39
5.2 Fitur B: Menawarkan konten digital yang dikurasi	42
5.3 Fitur C: Menghosting konten buatan pengguna dan hubungkan pengguna	47
5.4 Fitur D: Sistem berbasis kecerdasan buatan	52
Referensi	57
Glosarium	58

Meja

Tabel 1: Pedoman umum untuk industri	29
Tabel 2: Daftar periksa COP untuk Fitur A: Menyediakan konektivitas, data, dan hosting perangkat	40
Tabel 3: Daftar periksa COP untuk Fitur B: Menawarkan konten digital yang dikurasi	43
Tabel 4: Daftar periksa COP untuk Fitur C: Menghosting konten buatan pengguna dan menghubungkan pengguna	48
Tabel 5: Daftar periksa COP untuk Fitur D: Sistem berbasis AI	55

1. Ikhtisar

Tujuan dari dokumen ini adalah untuk memberikan arahan bagi para pemangku kepentingan industri TIK untuk membangun sumber daya perlindungan online anak (child online protection / COP) mereka sendiri. Tujuan dari panduan untuk industri tentang perlindungan online anak ini adalah untuk menyediakan kerangka kerja yang berguna, fleksibel, dan ramah pengguna untuk visi perusahaan dan tanggung jawab mereka untuk melindungi pengguna. Mereka juga bertujuan untuk membangun landasan bagi penggunaan layanan berbasis Internet dan teknologi terkait yang lebih aman dan terjamin bagi anak-anak saat ini, dan generasi mendatang.

Sebagai *toolkit*, pedoman ini juga bertujuan untuk meningkatkan kesuksesan bisnis dengan membantu operasi besar dan kecil serta pemangku kepentingan untuk mengembangkan dan mempertahankan model bisnis yang menarik dan berkelanjutan, sambil memahami tanggung jawab hukum dan moral terhadap anak-anak dan masyarakat.

Menanggapi kemajuan substansial dalam teknologi dan konvergensi, ITU, UNICEF dan mitra perlindungan online anak telah mengembangkan dan memperbarui pedoman untuk berbagai perusahaan yang mengembangkan, menyediakan atau menggunakan telekomunikasi atau kegiatan terkait dalam penyampaian produk dan layanan mereka.

Pedoman baru untuk industri tentang perlindungan online anak adalah hasil konsultasi dengan anggota COP Initiative, serta konsultasi yang lebih luas dengan anggota masyarakat sipil, bisnis, akademisi, pemerintah, media, organisasi internasional dan kaum muda.

Tujuan dari dokumen ini adalah untuk:

- menetapkan titik acuan dan panduan bersama untuk industri TIK dan online serta pemangku kepentingan terkait;
- memberikan panduan kepada perusahaan dalam mengidentifikasi, mencegah, dan mengurangi dampak merugikan dari produk dan layanan mereka terhadap hak-hak anak;
- memberikan panduan kepada perusahaan dalam mengidentifikasi cara-cara di mana mereka dapat mempromosikan hak-hak anak dan kewarganegaraan digital yang bertanggung jawab di antara anak-anak;
- menyarankan prinsip-prinsip umum untuk membentuk dasar komitmen nasional atau regional di semua industri terkait, sambil mengakui bahwa berbagai jenis bisnis akan menggunakan model implementasi yang beragam.

Ruang lingkup

Perlindungan online anak merupakan tantangan kompleks yang mencakup berbagai aspek tata kelola, kebijakan, operasional, teknis, dan hukum yang berbeda. Pedoman ini berusaha untuk mengatasi, mengatur dan memprioritaskan banyak bidang ini, berdasarkan model, kerangka kerja, dan referensi lain yang ada dan dikenal dengan baik.

Pedoman tersebut berfokus pada perlindungan anak-anak di semua bidang dan terhadap semua risiko dunia digital dan, dengan demikian, menyoroti praktik yang baik dari pemangku kepentingan industri yang dapat dipertimbangkan dalam proses penyusunan, pengembangan, dan pengelolaan kebijakan COP perusahaan.

Mereka memberikan panduan kepada pelaku industri tidak hanya tentang bagaimana mengelola dan menahan aktivitas online ilegal yang menjadi kewajiban mereka untuk bertindak (seperti CSAM online) melalui layanan mereka, tetapi juga fokus pada masalah lain yang mungkin tidak didefinisikan sebagai kejahatan di semua yurisdiksi. Ini termasuk kekerasan peer-to-peer, cyberbullying dan pelecehan online, serta masalah yang berkaitan dengan privasi atau kesejahteraan umum, penipuan atau ancaman lain, yang mungkin hanya berbahaya bagi anak-anak dalam konteks tertentu.

Untuk tujuan ini, pedoman ini mencakup rekomendasi tentang praktik yang baik dalam menghadapi risiko yang dihadapi anak-anak di dunia digital dan bagaimana bertindak untuk membangun lingkungan yang aman bagi anak-anak secara online. Panduan ini memberikan saran tentang bagaimana industri dapat bekerja untuk membantu memastikan keselamatan anak-anak saat menggunakan TIK, Internet, atau teknologi atau perangkat terkait apa pun yang dapat terhubung dengannya, termasuk ponsel, konsol game, mainan yang terhubung, jam tangan, Internet of Things. dan sistem berbasis AI. Oleh karena itu, mereka memberikan gambaran umum tentang masalah dan tantangan utama terkait perlindungan online anak dan mengusulkan tindakan untuk bisnis dan pemangku kepentingan untuk pengembangan kebijakan COP lokal dan internal. Pedoman ini tidak mencakup aspek-aspek seperti proses pengembangan aktual atau teks yang dapat disertakan dalam kebijakan COP untuk industri.

Struktur

Bagian 1 – Ikhtisar: Bagian ini menyoroti tujuan, ruang lingkup, dan target audiens dari pedoman ini.

Bagian 2 – Pengantar perlindungan online anak: Bagian ini menetapkan gambaran umum tentang masalah perlindungan online anak, menguraikan beberapa informasi latar belakang, termasuk situasi khusus anak penyandang disabilitas. Selain itu, ini memberikan contoh model internasional dan nasional yang ada untuk menjaga anak-anak tetap aman saat online sebagai bidang intervensi yang memungkinkan bagi pemangku kepentingan industri.

Bagian 3 – Bidang-bidang utama untuk melindungi dan mempromosikan hak-hak anak: Bagian ini menguraikan lima bidang utama di mana perusahaan dapat mengambil tindakan untuk memastikan penggunaan TIK yang aman dan positif bagi anak-anak.

Bagian 4 – Pedoman umum: Bagian ini memberikan rekomendasi untuk semua pemangku kepentingan industri tentang melindungi keselamatan anak-anak saat menggunakan TIK dan mempromosikan penggunaan TIK yang positif, termasuk kewarganegaraan digital yang bertanggung jawab di antara anak-anak.

Bagian 5 – Daftar periksa terkait fitur: Bagian ini menyoroti rekomendasi khusus bagi pemangku kepentingan tentang tindakan nyata untuk menghormati dan mendukung hak anak, dengan fitur berikut:

- Fitur A: Menyediakan konektivitas, penyimpanan data, dan layanan hosting
- Fitur B: Menawarkan konten digital yang dikurasi
- Fitur C: Menghosting konten buatan pengguna dan menghubungkan pengguna
- Fitur D: Sistem berbasis kecerdasan buatan

Target audiens

Berdasarkan Prinsip-Prinsip Panduan PBB tentang Bisnis dan Hak Asasi Manusia,¹ Hak Anak dan Prinsip Bisnis menyerukan kepada bisnis untuk memenuhi tanggung jawab mereka untuk menghormati hak-hak anak dengan menghindari dampak buruk apa pun yang terkait dengan operasi, produk, atau layanan mereka. Prinsip-prinsip ini juga mengartikulasikan perbedaan antara rasa hormat (minimum yang diperlukan bisnis untuk menghindari menyakiti anak-anak) dan dukungan (misalnya, dengan mengambil tindakan sukarela yang berusaha untuk memajukan realisasi hak-hak anak). Bisnis perlu memastikan hak anak-anak baik untuk perlindungan online maupun akses ke informasi dan kebebasan berekspresi, sambil mempromosikan penggunaan TIK yang positif bagi anak-anak.

Perbedaan tradisional antara bagian yang berbeda dari industri telekomunikasi dan telepon seluler, dan antara perusahaan Internet dan penyiar, dengan cepat rusak dan menjadi kabur. Konvergensi menarik aliran digital yang sebelumnya berbeda ini menjadi satu arus yang menjangkau miliaran orang di semua bagian dunia. Kerjasama dan kemitraan adalah kunci untuk membangun fondasi untuk penggunaan Internet dan teknologi terkait yang lebih aman dan terjamin. Pemerintah, sektor swasta, pembuat kebijakan, pendidik, masyarakat sipil, orang tua dan pengasuh semua memiliki peran penting dalam mencapai tujuan ini. Industri dapat bertindak dalam lima bidang utama, seperti yang dijelaskan di bagian 3.

2. Apa itu perlindungan online anak?

Selama 10 tahun terakhir, penggunaan dan peran Internet dalam kehidupan masyarakat telah banyak berubah. Dengan prevalensi smartphone dan tablet, aksesibilitas Wi-Fi dan teknologi 4G, dan perkembangan platform dan aplikasi media sosial, semakin banyak orang mengakses Internet untuk alasan yang terus meningkat.

Pada tahun 2019, lebih dari setengah populasi dunia menggunakan Internet. Proporsi terbesar pengguna Internet adalah orang-orang di bawah 44 tahun, dengan penggunaan Internet yang sama tinggi antara usia 16-24 tahun dan 35-44 tahun. Di tingkat global, satu dari tiga pengguna Internet adalah anak-anak (0–18 tahun) dan UNICEF memperkirakan bahwa 71 persen anak muda sudah online.² Proliferasi titik akses Internet, teknologi seluler, dan semakin banyaknya perangkat Internet yang diaktifkan, dikombinasikan dengan sumber daya besar yang dapat ditemukan di dunia maya, memberikan peluang yang belum pernah terjadi sebelumnya untuk belajar, berbagi, dan berkomunikasi.

Manfaat penggunaan TIK mencakup akses yang lebih luas ke informasi tentang layanan sosial, sumber daya pendidikan, dan saran kesehatan. Karena anak-anak dan remaja serta keluarga menggunakan Internet dan telepon seluler untuk mencari informasi dan bantuan, dan untuk melaporkan insiden pelecehan, teknologi ini dapat membantu melindungi anak-anak dan remaja dari kekerasan dan eksploitasi.

¹ United Nations Guiding Principles on Business and Human Rights.

² OECD, "New Technologies and 21st Century Children: Recent Trends and Outcomes", Education Working Paper No. 179

Penyedia layanan perlindungan anak juga menggunakan TIK untuk mengumpulkan dan mengirimkan data, sehingga memfasilitasi pencatatan kelahiran, manajemen kasus, penelusuran keluarga, pengumpulan data dan pemetaan kekerasan, antara lain.

Selain itu, Internet telah meningkatkan akses ke informasi di seluruh penjuru dunia, memungkinkan anak-anak dan remaja untuk meneliti hampir semua subjek yang diminati, mengakses media di seluruh dunia, mengejar prospek kejuruan, dan memanfaatkan ide untuk masa depan. Penggunaan TIK memberdayakan anak-anak dan remaja untuk menegaskan hak-hak mereka dan mengekspresikan pendapat mereka, dan juga memungkinkan mereka untuk terhubung dan berkomunikasi dengan keluarga dan teman-teman mereka. TIK juga berfungsi sebagai mode terpenting dari pertukaran budaya dan sumber hiburan.

Terlepas dari manfaat besar Internet, anak-anak dan remaja juga dapat menghadapi sejumlah risiko saat menggunakan TIK. Mereka dapat terpapar konten yang tidak sesuai usia atau kontak yang tidak pantas, termasuk dari calon pelaku pelecehan seksual. Mereka dapat mengalami kerusakan reputasi karena mempublikasikan informasi pribadi yang sensitif baik secara online atau melalui "sexting", seringkali gagal memahami implikasi dari tindakan mereka pada diri mereka sendiri dan

orang lain dan "jejak digital" jangka panjang mereka. Mereka juga menghadapi risiko terkait privasi online yang berasal dari pengumpulan data, serta pengumpulan dan penggunaan informasi lokasi.

Konvensi Hak Anak, yang merupakan perjanjian hak asasi manusia internasional yang paling banyak diratifikasi,³ mengatur tentang hak-hak sipil, politik, ekonomi, sosial, dan budaya anak. Ini menetapkan bahwa semua anak dan orang muda memiliki hak atas pendidikan; rekreasi, bermain dan budaya; informasi yang sesuai; kebebasan berpikir dan berekspresi; dan privasi, dan untuk mengekspresikan pandangan mereka tentang hal-hal yang mempengaruhi mereka sesuai dengan kapasitas mereka yang berkembang. Konvensi juga melindungi anak-anak dan remaja dari segala bentuk kekerasan, eksploitasi, penyalahgunaan dan diskriminasi dalam bentuk apapun, dan menetapkan bahwa kepentingan terbaik anak harus menjadi pertimbangan utama dalam segala hal yang mempengaruhi mereka. Orang tua, pengasuh, pendidik dan anggota masyarakat, termasuk tokoh masyarakat dan aktor masyarakat sipil, memiliki tanggung jawab untuk mengasuh dan mendukung anak-anak dan remaja dalam perjalanan mereka menuju kedewasaan. Pemerintah memiliki peran penting dalam memastikan bahwa semua pemangku kepentingan tersebut memenuhi peran ini.

Berkenaan dengan perlindungan hak anak secara online, industri perlu bekerja sama untuk mencapai keseimbangan yang cermat antara hak anak atas perlindungan dan hak mereka atas akses informasi dan kebebasan berekspresi. Oleh karena itu, perusahaan harus memprioritaskan langkah-langkah untuk melindungi anak-anak dan remaja secara online yang ditargetkan dan tidak terlalu membatasi, baik untuk anak atau pengguna lain.

³ United Nations Convention on the Rights of the Child. All but three countries (Somalia, South Sudan and the United States) have ratified the Convention on the Rights of the Child

Selain itu, ada konsensus yang berkembang bahwa mempromosikan kewarganegaraan digital di antara anak-anak dan remaja, dan mengembangkan produk dan platform yang memfasilitasi penggunaan TIK secara positif bagi anak-anak, harus menjadi prioritas bagi sektor swasta.

Sementara teknologi online memberikan banyak kesempatan bagi anak-anak dan remaja untuk berkomunikasi, mempelajari keterampilan baru, menjadi kreatif dan berkontribusi untuk meningkatkan masyarakat untuk semua, mereka juga dapat menimbulkan risiko baru bagi keselamatan anak-anak dan remaja. Mereka dapat mengekspos anak-anak dan remaja pada potensi risiko dan bahaya yang terkait dengan masalah privasi, konten ilegal, pelecehan, cyberbullying, penyalahgunaan data pribadi atau grooming untuk tujuan seksual dan bahkan pelecehan dan eksploitasi seksual anak. Mereka juga dapat terkena kerusakan reputasi termasuk "revenge porn" terkait dengan penerbitan informasi pribadi yang sensitif baik secara online atau melalui "sexting", cara bagi pengguna untuk mengirim pesan seksual eksplisit, foto atau gambar antara ponsel. Mereka juga menghadapi risiko terkait privasi online saat menggunakan Internet. Anak-anak, berdasarkan usia dan perkembangan kedewasaan mereka, seringkali tidak dapat sepenuhnya memahami risiko yang terkait dengan dunia online dan kemungkinan dampak negatif dari perilaku mereka yang tidak pantas terhadap orang lain dan diri mereka sendiri.

Terlepas dari kelebihanannya, ada juga kerugian dari penggunaan teknologi yang muncul dan lebih maju. Perkembangan dalam AI dan pembelajaran mesin, virtual dan augmented reality, big data, robotika, dan Internet of Things akan mengubah praktik media anak-anak dan remaja lebih jauh lagi. Sementara teknologi ini sebagian besar sedang dikembangkan untuk memperluas cakupan pemberian layanan dan meningkatkan kenyamanan (melalui, misalnya, bantuan suara, aksesibilitas dan bentuk-bentuk baru *digital immersion*), beberapa teknologi tersebut dapat memiliki dampak yang tidak disengaja dan bahkan disalahgunakan oleh pelaku kejahatan seks anak untuk melayani kebutuhan mereka. Menciptakan lingkungan online yang aman dan terjamin untuk anak-anak dan remaja membutuhkan partisipasi efektif dari pemerintah, sektor swasta, dan semua pemangku kepentingan. Fokus pada keterampilan digital dan literasi orang tua dan pendidik juga harus menjadi salah satu target pertama, yang dalam pencapaiannya industri dapat memainkan peran vital dan berkelanjutan.

Beberapa anak mungkin memiliki pemahaman yang baik tentang risiko online dan bagaimana menanggapi. Namun, hal ini tidak berlaku untuk semua anak di mana pun, terutama di antara kelompok rentan. Di bawah target 16.2 Tujuan Pembangunan Berkelanjutan Perserikatan Bangsa-Bangsa, yang bertujuan untuk mengakhiri pelecehan, eksploitasi, perdagangan manusia dan segala bentuk kekerasan dan penyiksaan terhadap anak, perlindungan anak secara online sangat penting.

Sejak 2009, COP Initiative, sebuah upaya multi-stakeholder internasional yang didirikan oleh ITU, telah bertujuan untuk meningkatkan kesadaran akan risiko terhadap anak-anak secara online dan tanggapan terhadap risiko tersebut. Inisiatif ini menyatukan mitra dari semua sektor komunitas global untuk memastikan pengalaman online yang aman dan terjamin bagi anak-anak di mana pun. Sebagai bagian dari Inisiatif, pada tahun 2009 ITU menerbitkan pedoman seperangkat COP untuk empat kelompok: anak-anak; orang tua, wali dan pendidik; industri; dan pembuat kebijakan.

Perlindungan online anak dipahami dalam pedoman ini sebagai pendekatan menyeluruh untuk menanggapi semua potensi ancaman dan bahaya yang mungkin dihadapi anak-anak dan remaja baik secara online atau yang difasilitasi oleh teknologi online. Dalam dokumen ini, perlindungan online anak juga mencakup bahaya terhadap anak yang terjadi secara offline tetapi terkait dengan bukti kekerasan dan pelecehan online. Selain mempertimbangkan perilaku dan aktivitas online anak, perlindungan online anak juga mengacu pada penyalahgunaan teknologi oleh orang selain anak itu sendiri untuk mengeksploitasi anak.

Semua pemangku kepentingan yang relevan memiliki peran dalam membantu anak-anak dan remaja mendapatkan manfaat dari peluang yang dapat ditawarkan Internet, sambil memperoleh literasi dan ketahanan digital terkait dengan kesejahteraan dan perlindungan online mereka.

Melindungi anak dan remaja adalah tanggung jawab bersama semua pemangku kepentingan. Agar itu terjadi, pembuat kebijakan, industri, orang tua, pengasuh, pendidik, dan pemangku kepentingan lainnya, harus memastikan bahwa anak-anak dan remaja dapat memenuhi potensi mereka – online dan offline.

Meskipun tidak ada definisi universal, perlindungan online anak mengambil pendekatan holistik untuk membangun ruang digital yang aman, sesuai usia, inklusif dan partisipatif untuk anak-anak dan remaja, yang ditandai dengan:

- respon, dukungan dan swadaya dalam menghadapi ancaman;
- pencegahan bahaya;
- keseimbangan dinamis antara memastikan perlindungan dan memberikan kesempatan bagi anak-anak untuk menjadi warga digital;
- menjunjung tinggi hak dan tanggung jawab anak dan masyarakat.

Selain itu, karena kemajuan pesat dalam teknologi dan masyarakat serta sifat Internet yang tanpa batas, perlindungan online anak harus gesit dan adaptif agar efektif. Tantangan baru akan muncul seiring seiring perkembangan inovasi teknologi dan akan bervariasi dari satu daerah ke daerah lainnya. Ini akan paling baik ditangani dengan bekerja sama sebagai komunitas global, karena solusi baru untuk tantangan ini perlu ditemukan.

2.1 Informasi latar belakang

Karena Internet terintegrasi penuh ke dalam kehidupan anak-anak dan remaja, tidak mungkin untuk mempertimbangkan dunia digital dan fisik secara terpisah.

Konektivitas semacam itu telah sangat memberdayakan. Dunia online memungkinkan anak-anak dan remaja untuk mengatasi kekurangan dan disabilitas, dan telah menyediakan arena baru untuk hiburan, pendidikan, partisipasi dan pembangunan hubungan. Platform digital saat ini digunakan untuk berbagai aktivitas dan seringkali merupakan pengalaman multi-media.

Memiliki akses dan belajar untuk menggunakan dan menavigasi teknologi ini dipandang sebagai hal yang penting bagi perkembangan kaum muda dan TIK pertama kali digunakan pada usia dini.

Oleh karena itu, sangat penting bagi semua pelaku untuk menyadari bahwa anak-anak dan remaja sering kali mulai menggunakan platform dan layanan sebelum mereka mencapai usia minimum yang ditentukan yang harus dipatuhi oleh industri teknologi dan, oleh karena itu, pendidikan harus diintegrasikan ke dalam semua layanan online yang digunakan oleh anak-anak di samping langkah-langkah perlindungan.

2.1.1 Anak-anak di dunia digital

Akses internet

Pada tahun 2019, lebih dari setengah populasi dunia menggunakan Internet (53,6 persen), dengan perkiraan 4,1 miliar pengguna. Di tingkat global, satu dari tiga pengguna Internet adalah anak-anak di bawah usia 18 tahun¹. Menurut UNICEF, di seluruh dunia, 71 persen anak muda sudah online². Terlepas dari persyaratan usia minimum, Ofcom (pengatur komunikasi Inggris) memperkirakan bahwa hampir 50 persen anak-anak berusia antara 10 dan 12 tahun sudah memiliki akun media sosial.³ Anak-anak dan remaja sekarang merupakan kehadiran yang substansial, permanen, dan terus-menerus di Internet. Internet melayani tujuan sosial, ekonomi dan politik lainnya dan telah menjadi produk atau layanan keluarga atau konsumen, integral dengan cara keluarga, anak-anak dan remaja menjalani kehidupan mereka.

Pada tahun 2017, di tingkat daerah, akses internet anak-anak dan remaja sangat terkait dengan tingkat pendapatan nasional. Negara-negara berpenghasilan rendah cenderung memiliki tingkat pengguna Internet anak yang lebih rendah daripada negara-negara berpenghasilan tinggi. Anak-anak dan remaja di sebagian besar negara menghabiskan lebih banyak waktu online di akhir pekan daripada hari kerja, dengan remaja berusia 15-17 tahun menghabiskan waktu online terlama, antara 2,5 dan 5,3 jam, tergantung pada negara.

¹ Livingstone, S., Carr, J., and Byrne, J. (2015) One in three: The task for global internet governance in addressing children's rights. Global Commission on Internet Governance: Paper Series. London: CIGI and Chatham House, <https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights>.

² Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)," *Broadband Commission for Sustainable Development*, October 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

³ BBC, "Under-age social media use 'on the rise', says Ofcom".

Penggunaan internet

Di kalangan anak-anak dan remaja, perangkat yang paling populer untuk mengakses Internet adalah ponsel, diikuti oleh komputer desktop dan laptop. Anak-anak dan remaja menghabiskan rata-rata dua jam sehari online selama seminggu dan empat jam setiap hari di akhir pekan. Sementara beberapa merasa terhubung secara permanen, banyak yang lain masih tidak memiliki akses ke Internet di rumah. Dalam praktiknya, sebagian besar anak-anak dan remaja yang menggunakan Internet memperoleh akses melalui lebih dari satu perangkat, dengan mereka yang terhubung setidaknya setiap minggu terkadang menggunakan hingga tiga perangkat berbeda. Anak-anak yang lebih besar dan mereka yang berada di negara kaya umumnya menggunakan lebih banyak perangkat, dan anak laki-laki menggunakan perangkat sedikit lebih banyak daripada anak perempuan di setiap negara yang disurvei.

Aktivitas paling populer di kalangan anak perempuan dan laki-laki adalah menonton klip video. Lebih dari tiga perempat anak-anak dan remaja yang menggunakan Internet melaporkan menonton video online setidaknya setiap minggu, baik sendiri atau dengan anggota lain dari keluarga mereka. Banyak anak-anak dan remaja dapat dianggap sebagai "pesosialisasi aktif", menggunakan beberapa platform media sosial seperti Facebook, Twitter, Tiktok atau Instagram. Anak-anak dan remaja juga terlibat dalam politik online dan menyuarakan pendapat mereka melalui blog.

Tingkat keseluruhan partisipasi dalam permainan online bervariasi menurut negara, kira-kira sejalan dengan kemudahan akses ke Internet untuk anak-anak dan remaja. Namun, ketersediaan dan keterjangkauan game online berubah dengan cepat dan usia anak-anak dan remaja yang pertama kali mengakses game online semakin berkurang.

Setiap minggu, 10-30 persen anak-anak dan remaja yang menggunakan Internet – diambil dari di beberapa negara tertentu – terlibat dalam aktivitas online yang kreatif.¹ Untuk tujuan pendidikan, banyak anak dan remaja dari segala usia menggunakan Internet untuk pekerjaan rumah, atau bahkan untuk mengejar ketinggalan kelas atau mencari informasi kesehatan secara online, setiap minggu. Anak-anak yang lebih besar tampaknya memiliki selera informasi yang lebih besar daripada anak-anak yang lebih muda.

¹ Livingstone, S., Kardefelt Winther, D., and Hussein, M. (2019). *Global Kids Online Comparative Report, Innocenti Research Report*. UNICEF Office of Research - Innocenti, Florence, <https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html>

Eksplorasi dan pelecehan seksual anak secara online

Eksplorasi dan pelecehan seksual anak online (CSEA) meningkat pada tingkat yang mengejutkan. Satu dekade yang lalu ada kurang dari satu juta file materi pelecehan anak yang dilaporkan. Pada 2019, jumlah itu naik menjadi 70 juta, meningkat hampir 50 persen dari angka 2018. Selain itu, untuk pertama kalinya video pelecehan melebihi jumlah foto dalam laporan kepada pihak berwenang, menunjukkan perlunya alat baru untuk mengatasi tren ini. Korban CSEA online jatuh ke semua kelompok umur tetapi semakin muda. Pada tahun 2018, jaringan hotline INHOPE mencatat perubahan profil korban dari puber menjadi praremaja. Selain itu, penelitian oleh ECPAT International dan INTERPOL pada tahun 2018 menemukan bahwa anak-anak yang lebih kecil lebih mungkin mengalami pelecehan yang parah, termasuk penyiksaan, pemerkosaan dengan kekerasan, atau sadisme. Ini termasuk bayi yang baru berumur beberapa hari, minggu atau bulan. Sementara anak perempuan lebih terpengaruh, pelecehan anak laki-laki mungkin terjadi lebih parah. Laporan yang sama menunjukkan bahwa 80 persen korban yang dirujuk dalam laporan adalah anak perempuan dan 17 persen adalah anak laki-laki. Anak-anak dari kedua jenis kelamin disebutkan dalam 3 persen dari laporan yang dinilai.¹

Snapshot Data²

- Satu dari tiga pengguna internet di seluruh dunia adalah anak-anak.
- Setiap setengah detik, seorang anak online untuk pertama kalinya.
- 800 juta anak menggunakan media sosial.
- Pada suatu waktu, 750.000 orang yang online diperkirakan mencari hubungan dengan anak-anak untuk tujuan seksual.
- Ada lebih dari 46 juta gambar atau video unik CSAM di repository EUROPOL.
- Lebih dari 89 persen korban berusia antara 3 dan 13 tahun.

Untuk informasi lebih lanjut tentang skala dan respons terhadap CSEA online, lihat: [WePROTECT Global Alliance](#).

¹ ECPAT and Interpol, "Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: summary report", 2018.

² End Violence Against Children, "Safe Online".

2.1.2 Dampak platform yang berbeda pada pengalaman digital anak-anak

Internet dan teknologi digital menghadirkan peluang dan risiko bagi anak-anak dan remaja. Beberapa di antaranya diuraikan di bawah ini.

Ketika anak-anak menggunakan media sosial, mereka mendapat manfaat dari banyak kesempatan untuk mengeksplorasi, belajar, berkomunikasi, dan mengembangkan keterampilan utama.

Jejaring sosial dilihat oleh anak-anak sebagai platform yang memungkinkan mereka untuk mengeksplorasi identitas pribadi mereka di lingkungan yang aman. Memiliki keterampilan yang relevan dan mengetahui cara mengatasi masalah yang berkaitan dengan privasi dan reputasi penting bagi kaum muda.

"Saya tahu semua yang Anda posting di Internet tetap ada di sana selamanya dan itu dapat memengaruhi hidup Anda di masa depan", anak lelaki berusia 14 tahun, Chili.

Namun, dengan survei yang menunjukkan bahwa sebagian besar anak menggunakan media sosial sebelum usia minimum 13 tahun dan layanan verifikasi usia umumnya lemah atau kurang, risiko yang dihadapi anak-anak bisa serius. Selain itu, ketika anak-anak ingin mempelajari keterampilan digital, menjadi warga digital dan mengontrol pengaturan privasi, mereka cenderung mempertimbangkan privasi dalam hubungannya dengan teman dan kenalan mereka – "Apa yang bisa dilihat teman saya?" - dan kurang dari itu dalam hubungannya dengan orang asing dan pihak ketiga. Ini, dikombinasikan dengan keingintahuan alami anak-anak dan ambang batas risiko yang umumnya lebih rendah, dapat membuat mereka rentan terhadap grooming, eksploitasi, intimidasi, atau jenis konten atau kontak berbahaya lainnya.

Popularitas yang meluas dari berbagi gambar dan video melalui aplikasi seluler, dan khususnya penggunaan platform streaming langsung oleh anak-anak, menghadirkan kekhawatiran dan risiko privasi lebih lanjut. Beberapa anak memproduksi gambar seksual diri mereka sendiri, teman dan saudara kandung dan membagikannya secara online. Pada tahun 2019, hampir sepertiga (29 persen) dari semua halaman web yang diberi teks oleh IWF berisi citra yang dibuat sendiri. Dari jumlah tersebut, 76 persen menunjukkan anak perempuan berusia 11-13 tahun, dengan sebagian besar di kamar tidur mereka atau ruangan lain di lingkungan rumah. Bagi beberapa orang, terutama anak-anak yang lebih besar, hal ini dapat dilihat sebagai eksplorasi alami seksualitas dan identitas seksual, sementara bagi yang lain, terutama anak-anak yang lebih muda, seringkali ada paksaan oleh orang dewasa atau anak lain. Apa pun masalahnya, konten yang dihasilkan di banyak negara ilegal dan dapat membuat anak-anak menghadapi risiko penuntutan atau digunakan untuk mengeksploitasi, merawat, atau memeras anak lebih lanjut.

Demikian pula, game online memungkinkan anak-anak memenuhi hak dasar mereka untuk bermain, serta membangun jaringan, menghabiskan waktu bersama teman dan bertemu teman baru, serta mengembangkan keterampilan penting. Meskipun ini bisa sangat positif, dalam beberapa kasus, dibiarkan tanpa pengawasan dan tidak didukung oleh orang dewasa yang bertanggung jawab, platform game juga dapat menimbulkan risiko bagi anak-anak. Ini termasuk bermain secara berlebihan, risiko keuangan terkait dengan pembelian dalam game yang berlebihan, pengumpulan dan monetisasi data pribadi anak-anak oleh pelaku industri, cyberbullying, ujaran kebencian, kekerasan dan paparan terhadap perilaku atau konten yang tidak pantas, *grooming*, penggunaan nyata, yang dihasilkan komputer atau bahkan gambar virtual realitas, dan video yang menggambarkan dan menormalkan CSEA. Risiko-risiko ini tidak hanya berlaku untuk lingkungan game tetapi juga berlaku untuk lingkungan digital lain tempat anak-anak menghabiskan waktu.

Selanjutnya, perkembangan teknologi telah menyebabkan munculnya "Internet of Things", di mana semakin banyak dan beragam perangkat yang terhubung ke Internet dapat berkomunikasi dan berjejaring melalui Internet. Ini termasuk mainan, monitor bayi, dan perangkat yang didukung oleh AI yang dapat menimbulkan risiko dalam hal privasi dan kontak yang tidak diinginkan.

Praktik yang baik: Penelitian

Dalam konteks online atau cyberbullying, Microsoft telah melakukan penelitian keamanan digital dan cyberbullying. Pada tahun 2012, lembaga tersebut mensurvei anak-anak berusia 8-17 tahun di 25 negara tentang perilaku negatif secara online. Hasilnya menunjukkan bahwa, rata-rata, 54 persen peserta menunjukkan bahwa mereka khawatir akan ditindas secara online; 37 persen menunjukkan bahwa mereka telah ditindas di dunia maya; dan 24 persen mengungkapkan bahwa mereka telah menindas seseorang. Survei yang sama menunjukkan bahwa kurang dari tiga dari 10 orang tua telah membahas intimidasi online dengan anak-anak mereka. Sejak 2016, Microsoft telah melakukan penelitian rutin terhadap risiko online yang menyediakan laporan Indeks Peradaban Digital tahunan.

FACES adalah program multimedia yang diproduksi oleh NHK Jepang dan oleh konsorsium berbagai penyiar layanan publik dengan kisah-kisah korban perundungan online dan offline di seluruh dunia. Serangkaian potret remaja di mana protagonis menjelaskan kepada kamera bagaimana mereka bereaksi terhadap serangan melalui Internet. Serial ini, yang juga diproduksi dalam klip dua menit, telah diadopsi oleh Facebook, UNESCO, dan Council of Europe, dan tersedia dalam banyak bahasa.

Pada tahun 2019, UNICEF menerbitkan makalah diskusi tentang Hak Anak dan Permainan Online: Peluang & Tantangan untuk Anak-Anak dan Industri untuk mengatasi peluang dan tantangan bagi anak-anak di salah satu industri hiburan yang tumbuh paling cepat. Makalah ini mengeksplorasi topik-topik berikut::

- Hak anak untuk bermain dan kebebasan berekspresi (waktu bermain game dan hasil kesehatan);
- Non-diskriminasi, partisipasi dan perlindungan dari pelecehan (interaksi sosial dan inklusi, lingkungan beracun, batas usia dan verifikasi, perlindungan dari grooming dan pelecehan seksual);
- Hak atas privasi dan kebebasan dari eksploitasi ekonomi (model bisnis akses data, permainan dan monetisasi gratis, kurangnya transparansi dalam konten komersial).

Praktik yang baik: Teknologi

The Google Virtual Reality Action Lab meneliti bagaimana realitas virtual dapat membantu mendorong kaum muda untuk menjadi lebih tangguh melawan intimidasi offline dan online.¹

Pada September 2019, BBC meluncurkan aplikasi seluler bernama Own IT, aplikasi kesejahteraan yang ditujukan untuk anak-anak berusia 8–13 tahun yang menerima ponsel cerdas pertama mereka. Aplikasi ini merupakan bagian dari komitmen BBC untuk mendukung kaum muda di lingkungan media yang berubah saat ini dan mengikuti keberhasilan peluncuran situs web Own IT pada tahun 2018. Aplikasi ini menggabungkan teknologi pembelajaran mesin canggih untuk melacak aktivitas anak-anak di smartphone dengan pilihan bagi anak-anak untuk melaporkan sendiri keadaan emosional mereka. Ini menggunakan informasi ini untuk memberikan konten dan intervensi yang disesuaikan untuk membantu anak-anak tetap bahagia dan sehat secara online, menawarkan dorongan yang ramah dan mendukung ketika perilaku mereka menyimpang di luar norma. Pengguna dapat mengakses aplikasi saat mereka mencari bantuan tetapi juga siap memberikan saran dan dukungan instan di layar saat mereka membutuhkannya, melalui keyboard yang dikembangkan secara khusus. Fitur termasuk:

- Mengingatkan pengguna untuk berpikir dua kali sebelum membagikan detail pribadi seperti nomor ponsel di media sosial.
- Membantu mereka memahami bagaimana pesan dapat dirasakan oleh orang lain, sebelum mereka menekan tombol kirim.
- Melacak suasana hati mereka dari waktu ke waktu dan menawarkan panduan tentang cara memperbaiki situasi jika diperlukan.
- Memberikan informasi tentang topik seperti menggunakan ponsel larut malam dan dampaknya terhadap kesejahteraan pengguna.

Aplikasi ini menampilkan konten yang dipesan khusus dari seluruh BBC. Ini menyediakan materi dan sumber daya yang berguna untuk membantu kaum muda mendapatkan hasil maksimal dari waktu online mereka dan membangun perilaku dan kebiasaan online yang sehat. Ini membantu kaum muda dan orang tua memiliki percakapan yang lebih konstruktif tentang pengalaman mereka secara online tetapi tidak akan memberikan laporan atau umpan balik kepada orang tua dan tidak ada data yang akan meninggalkan perangkat pengguna. Aplikasi tidak mengumpulkan data atau konten pribadi apa pun yang dihasilkan oleh pengguna, karena seluruh pembelajaran mesin berjalan di dalam aplikasi dan di dalam perangkat pengguna. Mesin dilatih secara terpisah pada data pelatihan untuk memastikan bahwa tidak ada pelanggaran privasi.

¹ Untuk informasi lebih lanjut lihat, Alexa Hasse et al., "Youth and Cyberbullying: Another Look", Berkman Klein Center for Internet & Society, 2019.

2.1.3 Situasi khusus anak-anak penyandang disabilitas⁴

Anak-anak dan remaja penyandang disabilitas menghadapi risiko secara online serupa dengan mereka yang tidak disabilitas, tetapi selain itu, mereka mungkin menghadapi risiko khusus terkait disabilitas mereka. Anak-anak dan remaja penyandang disabilitas sering menghadapi pengucilan, stigmatisasi dan hambatan (fisik, ekonomi, sosial dan sikap) untuk berpartisipasi dalam komunitas mereka. Pengalaman-pengalaman ini dapat berdampak negatif pada anak penyandang disabilitas dan menuntunnya untuk mencari bantuan

interaksi sosial dan persahabatan di ruang online. Meskipun interaksi semacam itu dapat menjadi positif dengan membantu membangun harga diri dan menciptakan jaringan dukungan, interaksi tersebut juga dapat menempatkan anak-anak tersebut pada risiko yang lebih tinggi terhadap insiden grooming, ajakan online, dan/atau pelecehan seksual. Penelitian menunjukkan bahwa anak-anak dan remaja yang mengalami kesulitan offline dan mereka yang terpengaruh oleh kesulitan psikososial berada pada risiko tinggi untuk insiden tersebut.⁵

Secara keseluruhan, anak-anak yang menjadi korban offline kemungkinan besar akan menjadi korban online. Ini menempatkan anak-anak penyandang disabilitas pada risiko yang lebih tinggi saat online, namun mereka memiliki kebutuhan yang lebih besar untuk online. Penelitian menunjukkan bahwa anak-anak penyandang disabilitas lebih mungkin mengalami pelecehan dalam bentuk apa pun,⁶ khususnya viktimisasi seksual.⁷ Korban dapat mencakup intimidasi, pelecehan, pengucilan dan diskriminasi berdasarkan disabilitas aktual atau yang dirasakan anak atau pada aspek yang terkait dengan disabilitas mereka, seperti cara mereka berperilaku atau berbicara, atau peralatan atau layanan yang mereka gunakan.

Pelaku grooming, ajakan online dan/atau pelecehan seksual terhadap anak-anak dan remaja penyandang disabilitas dapat mencakup tidak hanya pelaku preferensial yang menargetkan anak-anak dan remaja, tetapi juga mereka yang menargetkan anak-anak dan remaja penyandang disabilitas. Pelanggar tersebut mungkin termasuk "pemuja" – orang non-disabilitas yang tertarik secara seksual kepada penyandang disabilitas (paling sering diamputasi dan orang yang menggunakan alat bantu mobilitas), beberapa di antaranya bahkan berpura-pura menjadi disabilitas sendiri.⁸ Tindakan oleh orang-orang tersebut dapat mencakup mengunduh foto dan video anak-anak dan remaja penyandang disabilitas (yang sifatnya tidak berbahaya) dan/atau membagikannya melalui forum khusus atau akun media sosial. Alat pelaporan di forum dan media sosial seringkali tidak memiliki jalur yang tepat untuk menangani tindakan tersebut.

⁴ Lihat Council of Europe, "Two clicks forward and one click back: report on children with disabilities in the digital environment", 2019.

⁵ Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content", Berkman Center for Internet & Society, 2008.

⁶ UNICEF, "State of the World's Children Report: Children with Disabilities," 2013.

⁷ Katrin Mueller-Johnson et al., "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors", Journal of Interpersonal Violence, 2014.

⁸ Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder", Sexuality and Disability, 1997.

Ada kekhawatiran bahwa "berbagi" (orang tua berbagi informasi dan foto anak-anak dan remaja mereka secara online) dapat melanggar privasi anak, menyebabkan intimidasi, dan rasa malu, atau memiliki konsekuensi negatif di kemudian hari.⁹ Beberapa orang tua dari anak-anak penyandang disabilitas mungkin membagikan informasi atau media anak mereka untuk mendapatkan dukungan atau nasihat, akibatnya, menempatkan anak mereka pada risiko pelanggaran privasi baik sekarang maupun di masa depan. Orang tua seperti itu juga berisiko menjadi sasaran oleh orang-orang yang tidak tahu informasi atau tidak bermoral yang menawarkan grooming, terapi, atau "penyembuhan" untuk disabilitas anak. Demikian pula, beberapa orang tua dari anak-anak dan remaja penyandang disabilitas mungkin terlalu protektif karena kurangnya pengetahuan mereka tentang cara terbaik untuk memandu penggunaan Internet oleh anak mereka atau melindungi mereka dari perundungan atau pelecehan.¹⁰

Beberapa anak dan remaja penyandang disabilitas mungkin menghadapi kesulitan dalam menggunakan, atau bahkan dikucilkan dari, lingkungan online karena desain yang tidak dapat diakses (misalnya aplikasi yang tidak memungkinkan ukuran teks ditingkatkan), penolakan akomodasi yang diminta (misalnya perangkat lunak pembaca atau adaptif kontrol komputer), atau kebutuhan akan dukungan yang sesuai (misalnya pelatihan tentang cara menggunakan peralatan, dukungan satu lawan satu untuk menavigasi interaksi sosial).

¹¹

2.2 Model nasional dan transnasional yang ada untuk Perlindungan Online Anak

Di tingkat global, beberapa model diadopsi untuk menjaga anak-anak dan remaja tetap aman saat online. Pemangku kepentingan industri harus mempertimbangkan ini sebagai panduan untuk inisiatif internasional dan sebagai kerangka kerja untuk memastikan mereka tidak menyia-nyaiakan upaya untuk melindungi anak-anak dan remaja secara online. Industri Internet adalah arena yang beragam dan rumit, terdiri dari perusahaan dengan ukuran dan fungsi yang berbeda. Perlindungan anak harus ditangani tidak hanya oleh platform dan layanan berbasis konten, tetapi juga oleh mereka yang mendukung infrastruktur Internet.

Harus dicatat bahwa kapasitas industri untuk memperkenalkan kebijakan perlindungan anak yang komprehensif terbatas pada sumber daya yang tersedia. Oleh karena itu, pedoman ini merekomendasikan agar industri bekerja sama untuk menerapkan layanan guna melindungi pengguna. Dengan berbagi sumber daya dan keahlian teknik, industri akan dapat lebih efektif menciptakan "ruang aman" untuk mencegah penyalahgunaan.

Kerjasama industri

Koalisi Teknologi adalah contoh keberhasilan kerjasama antar pemangku kepentingan industri untuk melawan CSEA.

⁹ UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy", Innocenti Discussion Paper 2017-03.

¹⁰ UNICEF, "Is there a ladder of children's online participation?".

¹¹ Untuk panduan tentang hak-hak ini, lihat [Konvensi Perserikatan Bangsa-Bangsa tentang Hak-Hak Penyandang Disabilitas dan Protokol Opsional](#), terutama Pasal 9 tentang aksesibilitas dan Pasal 21 tentang kebebasan berekspresi dan berpendapat, dan akses ke informasi.

Model transnasional

Industri harus memasukkan pedoman internasional yang relevan dalam program struktural mereka serta mematuhi undang-undang nasional atau transnasional yang relevan yang berlaku di negara tempat mereka beroperasi. Industri seharusnya tidak hanya mempertimbangkan tindakan yang harus mereka ambil di tingkat hukum, tetapi juga aktivitas apa yang dapat mereka lakukan dan, jika memungkinkan, berupaya menerapkan inisiatif secara global. Beberapa model yang memberikan prinsip untuk inisiatif tersebut meliputi:

- Five Country Ministerial [Voluntary principles to counter online CSEA \(2020\)](#);
- Broadband Commission for Sustainable Development, [Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online \(2019\)](#);
- WePROTECT Global Alliance, [A Global Strategic Response to Online Child Sexual Exploitation and Abuse\(2019\)](#);
- Global Partnership to End Violence against Children, [Safe to Learn: Call toAction](#);
- Child Dignity in the Digital World, [Child Dignity Alliance: Technology Working Group Report \(2018\)](#);
- Directive (EU) 2018/1808 of the European Parliament and of the Council: [Audio Visual Media Services Directive](#);
- European Commission [General Data Protection Regulation \(2018\)](#);
- OECD [Recommendation on Protection of Children Online \(2012\)](#).

Model nasional

Ada sejumlah model nasional dan internasional yang menetapkan peran dan tanggung jawab yang jelas dari industri teknologi dalam menangani perlindungan online anak. Beberapa di antaranya tidak khusus untuk anak-anak tetapi dapat diterapkan pada mereka sebagai pengguna Internet. Mereka memberikan pedoman menyeluruh kepada industri mengenai kebijakan peraturan, standar dan kolaborasi dengan sektor lain. Untuk tujuan dokumen ini, prinsip-prinsip kunci dari model-model tersebut, sebagaimana diterapkan pada industri TIK, disorot.

Kode Desain Sesuai Usia, Inggris Raya

Pada awal 2019, Kantor Komisi Informasi menerbitkan proposal untuk kode desain yang sesuai dengan usianya tentang perlindungan data anak-anak. Kode yang diusulkan didasarkan pada kepentingan terbaik anak, sebagaimana tercantum dalam Konvensi PBB tentang Hak Anak, dan menetapkan beberapa harapan untuk industri. Kode tersebut terdiri dari lima belas standar termasuk, layanan lokasi yang dinonaktifkan secara default untuk anak-anak, agar industri mengumpulkan dan menyimpan hanya jumlah minimum data pribadi anak-anak, untuk produk yang dirancang untuk bersifat pribadi dan untuk penjelasan yang sesuai dengan usia dan dapat diakses.

Undang-Undang Komunikasi Digital yang Berbahaya, Selandia Baru

Undang-undang tahun 2015 menjadikan penyalahgunaan dunia maya sebagai kejahatan tertentu dan berfokus pada berbagai kerugian, mulai dari cyberbullying hingga revenge porn.

Ini bertujuan untuk mencegah dan mengurangi komunikasi digital yang berbahaya, menjadikannya ilegal untuk memposting komunikasi digital dengan tujuan menyebabkan tekanan emosional yang serius kepada orang lain, dan menetapkan serangkaian 10 prinsip komunikasi. Ini memberdayakan pengguna untuk mengeluh ke organisasi independen jika prinsip-prinsip ini dilanggar atau mengajukan perintah pengadilan terhadap penulis atau tuan rumah komunikasi jika masalah tidak diselesaikan.

eSafety Commissioner, Australia

Didirikan pada tahun 2015, Australia eSafety Commissioner adalah lembaga pemerintah pertama di dunia yang didedikasikan untuk menangani penyalahgunaan online dan menjaga warganya lebih aman saat online. Sebagai regulator independen nasional untuk keamanan online, eSafety memiliki kombinasi fungsi yang kuat. Mulai dari pencegahan melalui peningkatan kesadaran, pendidikan, penelitian, dan panduan praktik terbaik, hingga intervensi dini dan pemulihan kerugian melalui berbagai skema peraturan perundang-undangan yang memberi eSafety kekuatan untuk menghapus cyberbullying, penyalahgunaan berbasis gambar, dan konten online ilegal dengan cepat. Pengiriman luas ini memungkinkan eSafety untuk menangani keamanan online dengan cara yang beragam, holistik, dan proaktif.

Pada tahun 2018, eSafety mengembangkan Safety by Design (SbD), sebuah inisiatif yang menempatkan keselamatan dan hak-hak pengguna sebagai pusat desain, pengembangan, dan penerapan produk dan layanan online. Serangkaian prinsip keselamatan dengan desain berada di jantung inisiatif ini, yang menetapkan langkah-langkah realistis, dapat ditindaklanjuti, dan dapat dicapai bagi industri untuk dilakukan guna melindungi dan melindungi warga secara online dengan lebih baik. Tiga prinsip utama adalah:

- 1) Tanggung jawab penyedia layanan: beban keselamatan tidak boleh hanya dibebankan pada pengguna akhir. Langkah-langkah pencegahan dapat diambil untuk memastikan bahwa bahaya yang diketahui dan diantisipasi telah dievaluasi dalam desain dan penyediaan layanan online, bersama dengan langkah-langkah untuk membuat layanan cenderung tidak memfasilitasi, mengobarkan atau mendorong perilaku ilegal dan tidak pantas.
- 2) Pemberdayaan dan otonomi pengguna: martabat pengguna dan kepentingan terbaik mereka adalah sangat penting. Badan manusia dan otonomi harus didukung, diperkuat, dan diperkuat dalam desain layanan yang memungkinkan pengguna memiliki kontrol, tata kelola, dan regulasi yang lebih besar atas pengalaman mereka sendiri.
- 3) Transparansi dan akuntabilitas: ini adalah ciri dari pendekatan yang kuat terhadap keselamatan, yang memberikan jaminan bahwa layanan beroperasi sesuai dengan tujuan keselamatan yang dipublikasikan, serta mendidik dan memberdayakan masyarakat tentang langkah-langkah yang dapat diambil untuk mengatasi masalah keselamatan.

Aliansi Global WePROTECT

Inti dari strategi Aliansi Global WePROTECT adalah mendukung negara-negara untuk mengembangkan tanggapan multi-stakeholder yang terkoordinasi untuk mengatasi eksploitasi seksual anak secara online, yang dipandu oleh Model National Response-nya, yang bertindak

sebagai cetak biru untuk aksi nasional. Ini memberikan kerangka kerja bagi negara-negara untuk mengatasi eksploitasi seksual anak secara online. Dalam Respon Nasional Model WePROTECT, ada serangkaian komitmen yang jelas dari perusahaan TIK terkait dengan:

- prosedur pemberitahuan dan penghapusan;
- melaporkan eksploitasi dan pelecehan seksual anak secara online (CSEA);
- mengembangkan solusi teknologi; dan
- berinvestasi dalam program pencegahan COP dan layanan tanggap darurat.

Kemitraan Global dan Dana untuk Mengakhiri Kekerasan terhadap Anak

[Kemitraan Global dan Dana untuk Mengakhiri Kekerasan terhadap Anak](#) diluncurkan oleh Sekretaris Jenderal Perserikatan Bangsa-Bangsa pada tahun 2016 dengan satu tujuan: untuk mengkatalisasi dan mendukung tindakan untuk mengakhiri segala bentuk kekerasan terhadap anak pada tahun 2030 melalui kolaborasi unik lebih dari 400 mitra dari semua sektor.

Fokus pekerjaan adalah pada penyelamatan dan dukungan korban, solusi teknologi untuk mendeteksi dan mencegah pelanggaran, dukungan penegakan hukum, reformasi legislatif dan kebijakan, dan pembuatan data dan bukti pada skala dan sifat CSEA online serta pemahaman anak-anak. *perspektif*.¹²

3. Bidang-bidang utama untuk melindungi dan mempromosikan hak-hak anak

Bagian ini menguraikan lima bidang utama di mana perusahaan dapat mengambil tindakan untuk melindungi keselamatan anak-anak dan remaja saat menggunakan TIK dan mempromosikan penggunaan TIK secara positif.

3.1 Mengintegrasikan pertimbangan hak anak ke dalam semua kebijakan perusahaan dan proses manajemen yang tepat

Mengintegrasikan pertimbangan hak-hak anak mengharuskan perusahaan mengambil langkah-langkah yang memadai untuk mengidentifikasi, mencegah, mengurangi dan, jika perlu memulihkan, potensi dan dampak merugikan aktual terhadap hak-hak anak. Prinsip-Prinsip Panduan PBB tentang Bisnis dan Hak Asasi Manusia menyerukan semua bisnis dan industri untuk menerapkan kebijakan dan proses yang sesuai untuk memenuhi tanggung jawab mereka untuk menghormati hak asasi manusia.

Industri harus memberikan perhatian khusus kepada anak-anak dan remaja sebagai kelompok rentan sehubungan dengan perlindungan data dan kebebasan berekspresi mereka. [Resolusi Majelis Umum Perserikatan Bangsa-Bangsa 68/167](#) tentang hak atas privasi di era digital menegaskan kembali hak atas privasi dan kebebasan berekspresi tanpa mengalami gangguan yang melanggar hukum. Selain itu, [Resolusi 32/13 Dewan Hak Asasi Manusia Perserikatan Bangsa-Bangsa](#) tentang pemajuan, perlindungan dan penikmatan hak asasi manusia di Internet, mengakui sifat Internet yang global dan terbuka sebagai kekuatan pendorong dalam mempercepat kemajuan menuju pembangunan dan menegaskan bahwa hak-hak yang sama orang yang offline juga harus dilindungi secara online.

¹² Untuk informasi lebih lanjut lihat End Violence Against Children, "[Grantees of the End Violence Fund](#)".

Di negara-negara di mana tidak ada kerangka hukum yang memadai untuk perlindungan hak anak-anak dan remaja atas privasi dan kebebasan berekspresi, perusahaan harus mengikuti uji tuntas yang ditingkatkan untuk memastikan kebijakan dan praktik sejalan dengan hukum internasional. Karena keterlibatan masyarakat muda terus meningkat melalui komunikasi online, perusahaan memiliki tanggung jawab yang lebih besar untuk menghormati hak-hak anak dan remaja, bahkan ketika undang-undang domestik belum memenuhi standar internasional.

Perusahaan harus memiliki mekanisme pengaduan tingkat operasional untuk menyediakan format bagi individu yang terkena dampak untuk menyampaikan kekhawatiran tentang potensi pelanggaran. Mekanisme tingkat operasional harus dapat diakses oleh anak-anak, keluarga mereka dan mereka yang mewakili kepentingan mereka. Prinsip 31 dari Prinsip Panduan Bisnis dan Hak Asasi Manusia menjelaskan bahwa mekanisme tersebut harus sah, dapat diakses, dapat diprediksi, adil, transparan, kompatibel dengan hak, sumber pembelajaran berkelanjutan, dan berdasarkan keterlibatan dan dialog. Bersama dengan proses internal untuk mengatasi dampak negatif, mekanisme pengaduan harus memastikan bahwa perusahaan memiliki kerangka kerja untuk memastikan anak-anak dan remaja mendapatkan bantuan yang sesuai ketika hak-hak mereka terancam.

Ketika perusahaan mengambil pendekatan berbasis kepatuhan terhadap keselamatan TIK yang berfokus pada pemenuhan undang-undang nasional, mengikuti panduan internasional ketika undang-undang nasional tidak ada, dan menghindari dampak buruk pada hak-hak anak dan remaja, perusahaan secara proaktif mempromosikan perkembangan dan kesejahteraan anak-anak dan remaja. melalui tindakan sukarela yang memajukan hak anak dan remaja untuk mengakses informasi, kebebasan berekspresi, partisipasi, pendidikan dan budaya.

Praktik yang baik: Kebijakan dan desain yang sesuai dengan usia

Pengembang aplikasi [Toca Boca](#) memproduksi mainan digital dari perspektif anak. [Kebijakan privasi](#) perusahaan dirancang untuk membagikan informasi apa yang dikumpulkan perusahaan dan bagaimana informasi itu digunakan. Toca Boca, Inc adalah anggota [Program Sertifikasi Safe Harbor COPPA Kids Privacy Assured PRIVO](#).

[LEGO® Life](#) adalah contoh platform media sosial yang aman untuk anak-anak di bawah usia 13 tahun untuk berbagi kreasi LEGO mereka, mendapatkan inspirasi, dan berinteraksi dengan aman. Anak-anak di sini tidak diminta informasi pribadi apa pun untuk membuat akun, yang hanya dimungkinkan dengan alamat email orang tua atau wali. App menciptakan kesempatan bagi anak-anak dan keluarga untuk mendiskusikan keamanan online dan privasi di lingkungan yang positif.

Contoh desain yang sesuai dengan usia mencakup penawaran khusus dari beberapa Penyiar Layanan Umum utama untuk kelompok usia tertentu: misalnya, target ARD Jerman ([Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland – Das Erste](#)) dan ZDF ([Zweites Deutsches Fernsehen](#)) pemirsa mereka mulai dari usia 14 tahun, menawarkan konten yang disesuaikan melalui saluran online [funk.net](#). BBC ([British Broadcasting Corporation](#)) meluncurkan [CBeebies](#), yang ditujukan untuk anak-anak di bawah 6 tahun. Konten situs web secara khusus dirancang untuk kelompok usia masing-masing.

Praktik yang baik: Kebijakan dan teknologi

Twitter terus berinvestasi dalam teknologi kepemilikan, yang telah berkontribusi untuk terus mengurangi beban orang untuk melaporkan.¹ Secara khusus, lebih dari 50 persen Tweet, dibandingkan dengan 20 persen pada tahun 2018, yang ditindaklanjuti oleh Twitter sebagai tanggapan atas sifat kasar mereka, saat ini secara proaktif muncul menggunakan teknologi, daripada mengandalkan laporan ke Twitter. Teknologi baru ini digunakan untuk menangani bidang konten kebijakan informasi pribadi, media sensitif, perilaku kebencian, penyalahgunaan, dan peniruan identitas.

¹ Twitter "[Laporan Transparansi ke-15: Peningkatan penegakan proaktif pada akun](#)".

3.2 Mengembangkan proses standar untuk menangani CSAM

Pada tahun 2019, IWF menindak 132.676 halaman web yang mengandung dikonfirmasi pelecehan seksual terhadap anak.¹³ Setiap URL dapat berisi ratusan, bahkan ribuan, gambar dan video. Dari gambar yang diambil oleh IWF, 45 persen menunjukkan anak-anak berusia 10 tahun atau lebih muda; dan 1.609 halaman web mewakili anak-anak berusia 0–2 tahun, di mana 71 persennya berisi pelecehan seksual paling parah, seperti pemerkosaan penyiksaan dan seksual. Fakta-fakta yang mengganggu ini menggarisbawahi pentingnya tindakan kolaboratif antara industri, pemerintah, penegak hukum dan masyarakat sipil untuk memerangi CSAM.

¹³ IWF, "[The why. The how. The who. And the results. Annual Report 2019](#)"

Sementara banyak pemerintah menangani penyebaran dan distribusi CSAM dengan memberlakukan undang-undang, mengejar dan menuntut pelaku, meningkatkan kesadaran, dan mendukung anak-anak dan remaja dalam pemulihan dari pelecehan atau eksploitasi, ada banyak negara yang belum memiliki sistem yang memadai. Mekanisme diperlukan di setiap negara untuk memungkinkan masyarakat umum melaporkan konten yang kasar dan eksploitatif seperti ini. Industri, penegak hukum, pemerintah, dan masyarakat sipil harus bekerja sama untuk memastikan bahwa kerangka hukum yang memadai sesuai dengan standar internasional tersedia. Kerangka kerja tersebut harus mengkriminalisasi semua bentuk CSEA, termasuk melalui CSAM, dan melindungi anak-anak yang menjadi korban pelecehan atau eksploitasi tersebut. Kerangka kerja ini harus memastikan bahwa proses pelaporan, investigasi, dan penghapusan konten bekerja seefisien mungkin.

Industri harus menyediakan tautan ke hotline nasional atau hotline lain yang tersedia secara lokal, seperti portal IWF di beberapa negara dan, jika tidak ada peluang pelaporan lokal, berikan tautan ke hotline internasional lain yang relevan, seperti [National Center for Missing and Exploited Children \(NCMEC\)](#) atau [International Association of Internet Hotlines \(INHOPE\)](#), di mana salah satu hotline internasional dapat digunakan untuk mengajukan laporan.

Perusahaan yang bertanggung jawab mengambil sejumlah langkah untuk membantu mencegah jaringan dan layanan mereka digunakan untuk menyebarkan CSAM. Ini termasuk memperkenalkan bahasa ke dalam syarat dan ketentuan atau kode etik yang secara eksplisit melarang konten atau perilaku tersebut;¹⁴ mengembangkan proses pemberitahuan dan penghapusan yang kuat; dan bekerja dengan dan mendukung hotline nasional.

Selain itu, beberapa perusahaan menerapkan langkah-langkah teknis untuk mencegah penyalahgunaan layanan atau jaringan mereka untuk berbagi CSAM yang diketahui. Misalnya, beberapa penyedia layanan Internet memblokir akses ke URL yang dikonfirmasi oleh otoritas yang sesuai karena mengandung CSAM jika situs web dihosting di negara yang tidak memiliki proses untuk memastikannya akan dihapus dengan cepat. Yang lain menggunakan teknologi hashing untuk secara otomatis mendeteksi dan menghapus gambar pelecehan seksual anak yang sudah diketahui oleh penegak hukum atau hotline. Anggota industri harus mempertimbangkan dan menggabungkan semua layanan yang relevan untuk operasi mereka untuk mencegah penyebaran pelecehan seksual anak.

Pelaku industri harus berkomitmen untuk mengalokasikan sumber daya yang proporsional dan terus mengembangkan dan berbagi solusi teknologi sumber terbuka yang lebih disukai untuk mendeteksi dan menghapus CSAM.

¹⁴ Perlu dicatat bahwa perilaku pengguna yang tidak pantas tidak terbatas pada CSAM dan bahwa semua jenis perilaku atau konten yang tidak pantas harus ditangani dengan semestinya oleh perusahaan.

Praktik yang baik: Teknologi

Microsoft menggunakan pendekatan empat cabang untuk mendorong penggunaan teknologi yang bertanggung jawab dan aman, dengan fokus pada teknologi itu sendiri, tata kelola mandiri, kemitraan, serta pendidikan dan penjangkauan konsumen. Microsoft juga telah menyematkan fitur yang membantu memberdayakan individu untuk mengelola keamanan online mereka secara lebih efektif. "Keamanan Keluarga" adalah salah satu fitur tersebut, yang memungkinkan orang tua dan pengasuh untuk memantau penggunaan Internet anak-anak mereka.

Microsoft memberlakukan kebijakan terhadap pelecehan pada platformnya, dan pengguna yang menyalahgunakan peraturan ini akan dikenakan penghentian akun atau, jika terjadi pelanggaran yang lebih serius, tindakan penegakan hukum.

Microsoft PhotoDNA adalah alat yang membuat hash gambar dan membandingkannya dengan database hash yang telah diidentifikasi dan dikonfirmasi sebagai CSAM. Jika menemukan kecocokan, gambar diblokir. Alat ini telah memungkinkan penyedia konten untuk menghapus jutaan foto ilegal dari Internet; membantu menghukum predator seksual anak; dan dalam beberapa kasus, membantu penegak hukum menyelamatkan calon korban sebelum mereka terluka secara fisik. Microsoft telah lama berkomitmen untuk melindungi pelanggannya dari konten ilegal pada produk dan layanannya, dan menerapkan teknologi yang telah dibuat perusahaan untuk memerangi pertumbuhan video ilegal ini adalah langkah logis berikutnya. Namun, alat ini tidak menggunakan teknologi pengenalan wajah, juga tidak dapat mengidentifikasi seseorang atau objek dalam gambar. Namun, dengan penemuan PhotoDNA for Video, segalanya telah berubah. PhotoDNA untuk Video memecah video menjadi bingkai utama dan pada dasarnya membuat hash untuk tangkapan layar tersebut. Dengan cara yang sama seperti PhotoDNA dapat mencocokkan gambar yang telah diubah untuk menghindari deteksi, PhotoDNA untuk Video dapat menemukan konten eksploitasi seksual anak yang telah diedit atau digabungkan menjadi video yang mungkin tampak tidak berbahaya.

Selain itu, Microsoft baru-baru ini merilis alat baru untuk mengidentifikasi predator anak yang mempersiapkan anak-anak untuk dilecehkan dalam obrolan online. Project Artemis, yang dikembangkan bekerja sama dengan The Meet Group, Roblox, Kik, dan Thorn, dibangun di atas teknologi yang dipatenkan Microsoft dan akan tersedia secara gratis melalui Thorn untuk perusahaan layanan online yang memenuhi syarat yang menawarkan fungsi obrolan. Project Artemis adalah alat teknologi yang membantu memberi peringatan kepada administrator saat moderasi diperlukan di ruang obrolan. Dengan teknik deteksi grooming ini, akan memungkinkan untuk mengidentifikasi, menangani, dan melaporkan pemangsa yang mencoba memikat anak-anak untuk tujuan seksual.

IWF menyediakan berbagai layanan kepada anggota industri untuk melindungi penggunaannya agar tidak tersandung pada CSAM. Ini termasuk:

- Daftar pemblokiran URL yang dinamis dan terjamin kualitasnya dari materi langsung;
- Daftar hash dari konten kriminal yang diketahui terkait dengan CSAM;
- Daftar kata kunci unik dari istilah samar yang diketahui terkait dengan CSAM;
- Daftar detail nama domain yang dikenal sebagai hosting konten pelecehan seksual terhadap anak untuk memungkinkan penghapusan cepat domain yang menghosting konten ilegal.

3.3 Menciptakan lingkungan online yang lebih aman dan sesuai usia

Sangat sedikit hal dalam hidup yang dapat dianggap benar-benar aman dan bebas risiko sepanjang waktu. Bahkan di kota-kota di mana pergerakan lalu lintas sangat diatur dan dikontrol dengan ketat, kecelakaan masih terjadi. Demikian pula, dunia maya bukan tanpa risiko, terutama bagi anak-anak dan remaja. Anak-anak dan remaja dapat dianggap sebagai penerima, peserta, dan aktor dalam lingkungan online mereka. Risiko yang mereka hadapi dapat dikategorikan ke dalam empat bidang:¹⁵

- *Konten yang tidak pantas* – Anak-anak dan remaja mungkin menemukan konten yang tidak pantas dan ilegal saat mencari sesuatu yang lain dengan mengklik tautan yang mungkin tidak berbahaya dalam pesan instan, di blog, atau saat berbagi file. Mereka mungkin juga mencari dan membagikan materi yang tidak pantas atau peka usia. Apa yang dianggap sebagai konten berbahaya berbeda-beda di setiap negara; contohnya termasuk konten yang mempromosikan penyalahgunaan zat, kebencian rasial, perilaku berisiko, bunuh diri, anoreksia, atau kekerasan.
- *Perilaku yang tidak pantas* – Anak-anak dan orang dewasa dapat menggunakan Internet untuk melecehkan atau bahkan mengeksploitasi orang lain. Anak-anak terkadang dapat menyiarkan komentar yang menyakitkan atau gambar yang memalukan atau mungkin mencuri konten atau melanggar hak cipta.
- *Kontak yang tidak pantas* – Baik orang dewasa maupun remaja dapat menggunakan Internet untuk mencari anak-anak atau remaja lain yang rentan. Seringkali, tujuan mereka adalah untuk meyakinkan target bahwa mereka telah mengembangkan hubungan yang bermakna, tetapi tujuan yang mendasarinya adalah manipulatif. Mereka mungkin berusaha membujuk anak tersebut untuk melakukan tindakan seksual atau kekerasan lainnya secara online, menggunakan webcam atau alat perekam lainnya, atau mereka akan mencoba mengatur pertemuan langsung dan kontak fisik. Proses ini sering disebut sebagai "grooming".
- *Risiko komersial* – Kategori ini mengacu pada risiko privasi data yang terkait dengan pengumpulan dan penggunaan data anak-anak, serta pemasaran digital. Keamanan online merupakan tantangan komunitas dan peluang bagi industri, pemerintah, dan masyarakat sipil untuk bekerja sama dalam menetapkan prinsip dan praktik keselamatan. Industri dapat menawarkan serangkaian pendekatan teknis, alat dan layanan untuk orang tua, dan anak-anak dan remaja, dan pertama-tama dan terutama harus menciptakan produk yang mudah digunakan, aman dengan desain dan sesuai usia untuk berbagai pengguna mereka. Pendekatan tambahan termasuk menawarkan alat untuk mengembangkan sistem verifikasi usia yang sesuai yang menghormati hak anak atas privasi dan akses atau membatasi akses anak-anak dan remaja ke konten yang tidak sesuai usia, atau membatasi orang-orang yang mungkin berhubungan dengan anak-anak atau waktu di mana mereka mungkin online. Yang paling penting, kerangka kerja "keselamatan berdasarkan desain"¹⁶ termasuk privasi perlu dimasukkan ke dalam inovasi dan proses desain produk. Keselamatan anak-anak dan penggunaan teknologi yang bertanggung jawab harus dipertimbangkan dengan hati-hati dan tidak boleh dianggap remeh.

Beberapa program memungkinkan orang tua untuk memantau teks dan komunikasi lain yang dikirim dan diterima oleh anak-anak dan remaja mereka. Jika program jenis ini akan digunakan, penting bahwa hal ini didiskusikan secara terbuka dengan anak, jika tidak, perilaku tersebut dapat dianggap sebagai "mata-mata" dan dapat merusak kepercayaan dalam keluarga.

¹⁵ Sonia Livingstone et al., "EU Kids Online: Final Report", London School of Economics, 2009.

¹⁶ eSafety Commissioner, *Safety by Design Overview*, 2019.

Kebijakan penggunaan yang dapat diterima adalah salah satu cara agar perusahaan dapat menetapkan jenis perilaku apa yang dianjurkan oleh orang dewasa dan anak-anak, jenis aktivitas apa yang tidak dapat diterima, dan konsekuensi dari setiap pelanggaran terhadap kebijakan ini. Mekanisme pelaporan yang jelas dan transparan harus tersedia bagi pengguna yang memiliki kekhawatiran tentang konten dan perilaku. Selanjutnya, pelaporan perlu ditindaklanjuti secara tepat, dengan penyediaan informasi yang tepat waktu tentang status laporan. Meskipun perusahaan dapat memvariasikan implementasi mekanisme tindak lanjut mereka berdasarkan kasus per kasus, penting untuk menetapkan kerangka waktu yang jelas untuk tanggapan, mengkomunikasikan keputusan yang dibuat mengenai laporan, dan menawarkan metode untuk menindaklanjuti jika pengguna kurang puas dengan responnya

Praktik yang baik: Pelaporan

Facebook, dalam upaya untuk mengekang pelecehan seksual di platform digital, telah mendanai bersama Project deSHAME dengan Uni Eropa, sebuah kolaborasi antara Childnet, Save the Children, Kek Vonal, dan UCLan. Proyek ini bertujuan untuk meningkatkan pelaporan pelecehan seksual online di kalangan anak di bawah umur dan meningkatkan kerjasama multisektor dalam mencegah dan menanggapi perilaku ini.

Karena salah satu tujuan utama proyek ini adalah untuk mendorong pengguna melaporkan konten yang mengganggu atau tidak pantas, Standar Komunitas Facebook juga relevan sebagai pedoman tentang apa yang boleh dan tidak boleh di Facebook. Mereka juga menguraikan jenis pengguna yang tidak diizinkan untuk diposkan. Facebook juga telah menciptakan fitur keamanan seperti "Apakah Anda mengenal orang ini?" fitur; kotak masuk "lainnya" yang mengumpulkan pesan baru dari orang yang tidak dikenal pengguna; dan popup yang muncul di umpan berita jika terlihat seperti anak di bawah umur sedang dihubungi oleh orang dewasa yang tidak mereka kenal.

Penyedia konten dan layanan online juga dapat menjelaskan sifat konten atau layanan yang mereka sediakan dan rentang usia target yang dituju. Deskripsi ini harus selaras dengan standar nasional dan internasional yang sudah ada sebelumnya, peraturan yang relevan, dan saran tentang pemasaran dan periklanan untuk anak-anak yang disediakan oleh badan klasifikasi yang sesuai. Namun, proses ini menjadi lebih sulit, dengan semakin banyaknya layanan interaktif yang memungkinkan publikasi konten buatan pengguna, misalnya, melalui papan pesan, ruang obrolan, dan layanan jejaring sosial. Ketika perusahaan secara khusus menargetkan anak-anak dan remaja, dan ketika layanan sangat ditujukan untuk audiens yang lebih muda, harapan dalam hal konten dan keamanan yang ramah pengguna, mudah dimengerti dan dapat diakses akan jauh lebih tinggi.

Perusahaan juga didorong untuk mengadopsi standar privasi tertinggi dalam hal pengumpulan, pemrosesan, dan penyimpanan data dari atau tentang anak-anak dan remaja, karena anak-anak dan remaja mungkin kurang matang untuk menghargai konsekuensi sosial dan pribadi yang lebih luas dari mengungkapkan atau menyetujui membagikan informasi pribadi mereka secara online, atau penggunaan informasi pribadi mereka untuk tujuan komersial. Layanan yang ditujukan pada atau mungkin menarik audiens utama anak-anak dan remaja harus mempertimbangkan risiko yang ditimbulkan

kepada mereka dengan akses ke, atau pengumpulan dan penggunaan, informasi pribadi (termasuk informasi lokasi), dan memastikan risiko tersebut ditangani dengan benar, dan pengguna diberitahukan. Secara khusus, perusahaan harus memastikan bahasa dan gaya materi atau komunikasi apa pun yang digunakan untuk mempromosikan layanan, menyediakan akses ke layanan, atau dengan mana informasi pribadi diakses, dikumpulkan, dan digunakan, membantu memahami dan membantu pengguna dalam mengelola privasi mereka secara jelas dan sederhana. cara, dan menjelaskan apa yang mereka setujui dalam bahasa yang jelas dan dapat diakses.

Praktik yang baik: Inovasi

Pada 2018 –2019 Kantor Regional UNICEF Asia Timur dan Pasifik menyelenggarakan lima meja bundar multi-stakeholder untuk berbagi praktik industri yang menjanjikan untuk menangani CSEA online. Peserta meja bundar adalah perusahaan sektor swasta terkemuka, seperti Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Mongolia) Mobifone+ (Vietnam), Globe Telecom (Filipina), True (Thailand), GSMA dan mitra masyarakat sipil, termasuk INHOPE, ECPAT Internasional dan Child Helpline International.

Sebagai bagian dari proyek yang sama, pada Februari 2020, UNICEF meluncurkan Think Tank untuk mempercepat kepemimpinan industri di kawasan Asia Timur dan Pasifik untuk mencegah kekerasan terhadap anak di dunia online. Think Tank adalah inkubator untuk ide dan inovasi, memanfaatkan perspektif unik pelaku industri (kreasi produk, pemasaran, dll.) untuk pengembangan materi pendidikan yang berdampak dan identifikasi platform penyampaian yang paling efektif, serta untuk pengembangan kerangka evaluasi yang dapat mengukur dampak materi dan pesan pendidikan ini yang ditargetkan pada anak-anak. Think Tank terdiri dari Facebook, Telenor, pakar akademis, badan-badan PBB, seperti ITU, UNESCO dan UNODC, dan lainnya, seperti Australia eSafety Commissioner, ECPAT International, ICMEC, INTERPOL, dan End Violence Global Fund. Pertemuan perdana Think Tank, yang diadakan bersamaan dengan Konferensi Regional ASEAN tentang Perlindungan Online Anak, mengumpulkan para ahli, termasuk Microsoft, untuk mengeksplorasi kemungkinan teknologi dan penelitian untuk melacak perubahan perilaku online dengan lebih baik, berdasarkan penggunaan materi dan pesan keamanan online.

3.4 Mendidik anak-anak, pengasuh dan pendidik tentang keselamatan anak-anak dan penggunaan TIK yang bertanggung jawab

Langkah-langkah teknis dapat menjadi bagian penting untuk memastikan bahwa anak-anak dan remaja dilindungi dari potensi risiko online, tetapi ini hanya persamaan satu elemen. Alat kontrol orang tua, peningkatan kesadaran dan pendidikan juga merupakan komponen kunci yang akan membantu memberdayakan dan menginformasikan anak-anak dan remaja dari segala usia, serta orang tua, pengasuh dan pendidik. Meskipun perusahaan memiliki peran penting dalam mendorong anak-anak dan remaja untuk menggunakan TIK dengan cara yang bertanggung jawab dan aman, tanggung jawab ini dibagi dengan orang tua, sekolah, dan anak-anak serta remaja.

Banyak perusahaan berinvestasi dalam program pendidikan yang dirancang untuk memungkinkan pengguna membuat keputusan berdasarkan informasi tentang konten dan layanan.

Perusahaan membantu orang tua, pengasuh, dan pendidik dalam membimbing anak-anak dan remaja menuju pengalaman online dan ponsel yang lebih aman, lebih bertanggung jawab, dan sesuai. Ini termasuk pengeposan konten yang peka terhadap usia dan memastikan bahwa informasi tentang item seperti harga konten, persyaratan berlangganan, dan cara membatalkan langganan, dikomunikasikan dengan jelas. Mempromosikan penghormatan terhadap persyaratan usia minimum oleh media sosial di semua negara di mana verifikasi usia dimungkinkan juga akan membantu melindungi anak-anak dengan mengizinkan mereka mengakses layanan pada usia yang sesuai. Pertimbangan penting yang harus sejalan dengan rekomendasi ini adalah pengumpulan data pribadi tambahan yang mungkin diperlukan dan kebutuhan untuk membatasi pengumpulan dan penyimpanan informasi ini dan pemrosesannya. Penting juga untuk memberikan informasi langsung kepada anak-anak dan remaja tentang penggunaan TIK yang lebih aman dan perilaku positif dan bertanggung jawab. Selain meningkatkan kesadaran tentang keselamatan, perusahaan dapat memfasilitasi pengalaman positif dengan mengembangkan konten untuk anak-anak dan remaja tentang bersikap hormat, baik hati, dan berpikiran terbuka saat menggunakan TIK dan menjaga teman. Mereka dapat memberikan informasi tentang tindakan yang harus diambil jika mereka memiliki pengalaman negatif seperti penindasan atau grooming online, sehingga memudahkan untuk melaporkan insiden tersebut dan menyediakan fungsi untuk tidak menerima pesan anonim.

Orang tua terkadang memiliki pemahaman dan pengetahuan yang kurang tentang Internet dan perangkat seluler dibandingkan anak-anak dan remaja. Selain itu, konvergensi perangkat seluler dan layanan Internet membuat pengawasan orang tua menjadi lebih sulit. Industri dapat bekerja sama dengan pemerintah dan pendidik untuk memperkuat kapasitas orang tua untuk mendukung anak-anak mereka dalam membangun ketahanan digital mereka dan bertindak sebagai warga digital yang bertanggung jawab. Tujuannya bukan untuk mengalihkan tanggung jawab penggunaan TIK anak-anak dan remaja kepada orang tua saja, tetapi lebih untuk mengakui bahwa orang tua berada dalam posisi yang lebih baik untuk memutuskan apa yang sesuai untuk anak-anak mereka dan bahwa mereka harus disadarkan akan semua risiko untuk lebih baik melindungi anak-anak mereka dan memberdayakan mereka untuk mengambil tindakan.

Informasi dapat ditransmisikan secara online dan offline melalui berbagai saluran media, dengan pertimbangan bahwa beberapa orang tua tidak menggunakan layanan Internet. Penting untuk berkolaborasi dengan distrik sekolah untuk menyediakan kurikulum tentang keamanan online dan penggunaan TIK yang bertanggung jawab untuk anak-anak dan remaja, dan materi pendidikan untuk orang tua. Contohnya termasuk menjelaskan jenis layanan dan opsi yang tersedia untuk memantau aktivitas, tindakan yang harus diambil jika seorang anak mengalami perundungan atau grooming online, cara menghindari spam dan mengelola pengaturan privasi, dan cara berbicara dengan anak laki-laki dan perempuan dari kelompok usia yang berbeda tentang hal sensitif. masalah. Komunikasi adalah proses dua arah dan banyak perusahaan memberikan pilihan bagi pelanggan untuk menghubungi mereka untuk melaporkan masalah atau mendiskusikan masalah.

Ketika konten dan layanan semakin tumbuh, semua pengguna akan terus mendapat manfaat dari saran dan peringatan tentang sifat layanan tertentu dan cara menikmatinya dengan aman. Meskipun penting untuk mengajari anak-anak tentang penggunaan Internet yang bertanggung jawab, kami tahu anak-anak suka bereksperimen, mengambil risiko, memiliki rasa ingin tahu yang tinggi, dan mungkin tidak selalu membuat keputusan terbaik.

Memberi mereka kesempatan untuk menggunakan hak pilihan mereka berkontribusi pada pertumbuhan mereka dan merupakan cara yang sehat untuk membantu mereka mengembangkan otonomi dan ketahanan, selama pukulan baliknya tidak terlalu keras. Sementara anak-anak harus diizinkan untuk mengambil beberapa risiko di lingkungan online, sangat penting bahwa orang tua dan perusahaan dapat mendukung mereka ketika terjadi kesalahan, karena dapat mengimbangi dampak negatif dari pengalaman yang tidak nyaman dan mengubahnya menjadi pelajaran yang berguna bagi mereka. masa depan.

Praktik yang baik: Pendidikan

NHK Jepang menjalankan [kampanye pencegahan bunuh diri](#) untuk kaum muda di Twitter: Di Jepang, bunuh diri di kalangan remaja memuncak ketika mereka kembali ke sekolah setelah liburan musim panas. Kembalinya ke kenyataan dikatakan sebagai alasan puncaknya. Tim produksi NHK Heart Net TV (NHK Japan) memproduksi program multimedia [#On the Night of August](#). Menghubungkan televisi, live streaming, dan media sosial, NKH berhasil menciptakan "tempat" di mana remaja dapat berbagi perasaan tanpa rasa takut.

Praktik yang baik: Pendidikan

Twitter juga telah menerbitkan [panduan untuk pendidik tentang literasi media](#). Disusun bersama UNESCO, buku pegangan ini terutama bertujuan untuk membantu para pendidik membekali generasi muda dengan keterampilan literasi media. Aspek lain dari pekerjaan keselamatan Twitter berkaitan dengan [pengungkapan operasi informasi](#) mereka. Ini adalah arsip operasi informasi yang didukung Negara, yang dibagikan Twitter secara publik. Inisiatif ini diluncurkan untuk memberdayakan pemahaman akademis dan publik tentang kampanye yang terkait dengan masalah ini di seluruh dunia, dan untuk memberdayakan pengawasan pihak ketiga yang independen terhadap taktik ini di platform Twitter.

Project deSHAME, yang dibiayai bersama oleh Facebook dan Uni Eropa, juga memfasilitasi pembuatan sumber daya untuk berbagai kelompok usia, dengan fokus khusus pada anak-anak berusia 9–13 tahun. Sebagai bagian dari proyek, sebuah toolkit yang disebut "[Step Up, Speak Up!](#)" telah dikembangkan, menyediakan berbagai materi pendidikan, pelatihan dan peningkatan kesadaran, serta perangkat praktis untuk strategi pencegahan dan penanggulangan multisektor. Proyek ini akan mentransfer materi pembelajaran ini ke negara dan mitra Eropa lainnya di seluruh dunia untuk mempromosikan hak digital kaum muda.

Google telah mengembangkan serangkaian inisiatif, sumber daya, dan alat pendidikan untuk membantu mempromosikan keamanan online bagi kaum muda. Salah satunya adalah kampanye [Be Internet Awesome](#) seputar kewarganegaraan digital, yang dibuat bekerja sama dengan organisasi seperti ConnectSafely, Family Online Safety Institute, dan Internet Keep Safe Coalition. Kampanye ini menasar anak muda usia 8-11 tahun. Ini menampilkan permainan berbasis web untuk pemuda (Interland) yang mengajarkan dasar-dasar keamanan digital dan sumber daya untuk pendidik, seperti Kewarganegaraan Digital dan Kurikulum Keselamatan. Kurikulum Keselamatan menawarkan rencana pelajaran untuk lima bidang tematik utama kampanye, salah satunya berfokus pada cyberbullying. Selain itu, Google telah membuat kursus keamanan dan kewarganegaraan digital online untuk pendidik siswa dari segala usia, memberikan dukungan lebih lanjut untuk mengintegrasikan kewarganegaraan digital dan kegiatan tentang keselamatan di kelas. Google juga menawarkan beberapa program untuk membantu melibatkan kaum muda secara langsung dalam upaya keamanan online dan kewarganegaraan digital. Inisiatif global Web Rangers adalah salah satu program yang mengajarkan kaum muda tentang keamanan online dan mendorong mereka untuk merancang kampanye mereka sendiri seputar penggunaan Internet yang positif dan aman. Ada juga program khusus negara untuk kaum muda, seperti program Warga Internet dan Legenda Internet di Inggris, yang diluncurkan oleh Google.

Di Eurovision Youth News Exchange, European Broadcasting Union mengumpulkan 15 penyiar televisi Eropa untuk berbagi program, format, dan solusi secara online dan offline. Dalam beberapa tahun terakhir, mengajarkan literasi digital dan memperingatkan anak-anak tentang risiko di Internet telah menjadi pusat program mereka. Di antara inisiatif paling sukses dalam beberapa tahun terakhir adalah iklan media sosial dan program berita yang cocok untuk anak-anak yang diproduksi oleh Super dan Ultra nytt di bawah NRK, penyiar publik Norwegia. .

Praktik yang baik: Kemitraan strategis

Sebagai bagian dari proyek yang didukung oleh [End Violence Against Children Fund](#), pada tahun 2018 [Capital Humano y Social Alternativo](#) menjalin kemitraan dengan Telefónica, penyedia layanan Internet, kabel, dan telepon terbesar di Peru, dengan 14,4 juta pelanggan, termasuk lebih dari 8 juta Pengguna seluler Movistar.

Beberapa kegiatan dilakukan di bawah kemitraan yang bermanfaat ini:

- Kursus virtual tentang perlindungan online anak dikembangkan oleh Telefónica dengan dukungan teknis dari Capital Humano y Social Alternativo. Kursus ini sekarang tersedia secara terbuka di situs web Telefónica dan perusahaan melacak jumlah orang yang mendaftar dan berhasil menyelesaikan kursus. Kementerian Pendidikan Peru setuju untuk memasukkan akses ke kursus virtual ini melalui situs resminya.
- Sebuah buklet tentang keamanan Internet dibuat oleh Capital Humano y Social Alternativo dan didistribusikan oleh Telefónica di lebih dari 300 pusat penjualan selulernya. Tujuannya adalah untuk meningkatkan kesadaran di antara pelanggan Telefónica tentang keamanan online dan risiko yang terkait dengan CSEA online.
- Sebuah game interaktif di CSEA online dikembangkan oleh Telefónica dengan dukungan teknis dari Capital Humano y Social Alternativo, yang dapat dimainkan pelanggannya sambil menunggu giliran di toko Telefónica.

Membangun kesuksesan dengan Telefónica, Capital Humano y Social Alternativo bermitra dengan Econocable, penyedia layanan Internet dan kabel yang bekerja di daerah terpencil dan berpenghasilan rendah di Peru.

3.5 Mempromosikan teknologi digital sebagai cara untuk meningkatkan keterlibatan masyarakat

Pasal 13 Konvensi PBB tentang Hak Anak menyatakan bahwa "anak berhak atas kebebasan berekspresi; hak ini harus mencakup kebebasan untuk mencari, menerima, dan memberikan informasi dan gagasan dalam segala jenis, tanpa memandang batas-batas, baik secara lisan, tertulis atau tercetak, dalam bentuk karya seni, atau melalui media lain apa pun yang dipilih anak." Perusahaan dapat memenuhi kewajiban mereka untuk menghormati hak-hak sipil dan politik anak-anak dan remaja dengan memastikan bahwa teknologi, dan penerapan undang-undang dan kebijakan yang dikembangkan untuk melindungi anak-anak dan remaja dari bahaya online tidak memiliki konsekuensi yang tidak diinginkan berupa penekanan hak mereka untuk berpartisipasi dan berekspresi atau mencegah mereka mengakses informasi yang penting untuk kesejahteraan mereka. Sangat penting untuk memastikan bahwa sistem verifikasi usia tidak membahayakan kebutuhan asli kelompok usia tertentu untuk mengakses konten yang relevan untuk perkembangan mereka.

Pada saat yang sama, bisnis dan industri juga dapat mendukung hak-hak anak dan remaja dengan menyediakan mekanisme dan alat untuk memfasilitasi partisipasi pemuda.

Mereka dapat menekankan kapasitas Internet untuk memfasilitasi keterlibatan positif dalam kehidupan sipil yang lebih luas, mendorong kemajuan sosial, dan mempengaruhi keberlanjutan dan ketahanan masyarakat, misalnya, dengan berpartisipasi dalam kampanye sosial dan lingkungan dan meminta pertanggungjawaban mereka yang bertanggung jawab. Dengan alat dan informasi yang tepat, anak-anak dan remaja ditempatkan dengan lebih baik untuk mengakses peluang grooming kesehatan, pendidikan dan pekerjaan, dan untuk menyuarakan pendapat dan kebutuhan mereka di sekolah, masyarakat, dan negara. Mereka diberdayakan untuk mengakses informasi tentang hak-hak mereka dan mencari informasi tentang hal-hal yang mempengaruhi mereka secara pribadi, seperti kesehatan seksual mereka, dan tentang akuntabilitas politik dan pemerintah.

Perusahaan juga dapat berinvestasi dalam penciptaan pengalaman online yang sesuai untuk anak-anak dan remaja serta keluarga. Mereka dapat mendukung pengembangan teknologi dan konten yang mendorong dan memungkinkan anak-anak dan remaja untuk belajar, berinovasi, dan menciptakan solusi. Mereka harus selalu mempertimbangkan keselamatan dengan desain dalam produk mereka.

Selain itu, perusahaan dapat secara proaktif mendukung hak-hak anak dan remaja dengan berupaya menutup kesenjangan digital. Partisipasi anak-anak dan remaja membutuhkan literasi digital – kemampuan untuk memahami dan berinteraksi di dunia digital. Tanpa kemampuan ini, warga tidak dapat berpartisipasi dalam banyak fungsi sosial yang telah didigitalkan, termasuk mengajukan pajak, mendukung kandidat politik, menandatangani petisi online, mendaftarkan kelahiran, atau sekadar mengakses informasi komersial, kesehatan, pendidikan, atau budaya. Tanpa tindakan, kesenjangan antara warga yang dapat mengakses forum-forum ini dan mereka yang tidak, karena kurangnya akses Internet atau literasi digital, akan terus melebar, menempatkan yang terakhir pada kerugian yang signifikan. Perusahaan dapat mendukung inisiatif multimedia untuk mengembangkan keterampilan digital yang dibutuhkan anak-anak dan remaja untuk menjadi warga negara yang percaya diri, terhubung, dan terlibat secara aktif.¹⁷ Di banyak negara, literasi digital dan media, serta upaya untuk menutup kesenjangan digital telah menjadi bagian dari misi media layanan publik selama beberapa tahun terakhir. Parlemen Italia, misalnya, telah mengusulkan agar prioritas lembaga penyiaran nasional termasuk menutup kesenjangan digital dan memastikan perlindungan anak baik offline maupun online, sebuah contoh yang bisa diikuti oleh negara lain.

Praktik yang baik: Kolaborasi multi-agensi

Baru-baru ini, Microsoft bergabung dengan kampanye global **Power of ZERO**, yang dipimpin oleh organisasi No Bully, yang bertujuan untuk membantu anak kecil, dan orang dewasa yang mengasuh mereka, belajar menggunakan teknologi digital dengan baik dan mengembangkan suara, kasih sayang, dan inklusivitas yang merupakan jantung kewarganegaraan digital. Inisiatif ini menawarkan pendidik awal (kampanye ini ditargetkan untuk anak-anak usia 8 tahun ke bawah) dan keluarga dengan materi pembelajaran gratis untuk membantu anak-anak mengembangkan "12 kekuatan untuk kebaikan" (Keterampilan hidup 12 Power of Zero atau "kekuatan," untuk anak-anak untuk berhasil menavigasi dunia online dan offline, termasuk ketahanan, rasa hormat, inklusivitas, dan kreativitas) dan meletakkan fondasi yang kuat bagi mereka sejak usia dini.

¹⁷ Untuk contoh partisipasi pemuda dari komunitas keliling lihat [here](#).

4. Pedoman umum untuk industri

Tabel 1 menguraikan pedoman luas untuk industri untuk mengidentifikasi, mencegah dan mengurangi dampak buruk produk dan layanan terhadap hak-hak anak dan remaja, dan untuk mempromosikan penggunaan TIK secara positif bagi anak-anak dan remaja.

Perhatikan bahwa tidak semua langkah yang tercantum dalam Tabel 1 akan sesuai di semua perusahaan dan layanan, dan juga tidak semua langkah yang diperlukan untuk setiap layanan ditemukan dalam Tabel ini. Pedoman umum untuk industri dilengkapi dengan daftar periksa terkait fitur (lihat bagian 5) dan sebaliknya. Daftar periksa terkait fitur di Tabel 2–5 menyoroti langkah-langkah tambahan yang paling relevan untuk layanan individual. Perhatikan bahwa daftar periksa khusus fitur mungkin tumpang tindih, dan lebih dari satu daftar periksa dapat relevan untuk layanan yang sama.

Tabel 1: Pedoman umum untuk industri

<p>Mengintegrasikan pertimbangan hak anak ke dalam semua kebijakan perusahaan dan proses manajemen yang tepat</p>	<p>Industri dapat mengidentifikasi, mencegah dan mengurangi dampak buruk TIK terhadap hak anak dan remaja, dan mengidentifikasi peluang untuk mendukung pemajuan hak anak dan remaja dengan mengambil tindakan berikut:</p>
	<p>Pastikan bahwa individu dan/atau tim tertentu ditunjuk dengan tanggung jawab untuk proses ini dan memiliki akses ke pemangku kepentingan internal dan eksternal yang diperlukan. Beri wewenang kepada orang atau tim ini untuk memimpin dalam meningkatkan profil perlindungan online anak di seluruh perusahaan.</p>
	<p>Kembangkan kebijakan perlindungan dan perlindungan anak dan/atau integrasikan risiko dan peluang khusus yang berkaitan dengan hak anak dan remaja ke dalam komitmen kebijakan di seluruh perusahaan (misalnya hak asasi manusia, privasi, pemasaran, dan kode etik yang relevan).</p>
	<p>Mengintegrasikan uji tuntas pada isu-isu COP ke dalam kerangka penilaian risiko atau hak asasi manusia yang ada (di tingkat perusahaan, produk atau teknologi dan/atau negara) untuk menentukan apakah bisnis atau industri dapat menyebabkan atau berkontribusi terhadap dampak yang merugikan melalui kegiatannya, atau apakah dampak merugikan dapat secara langsung dikaitkan dengan operasi, produk atau layanan, atau hubungan bisnisnya.</p>
	<p>Identifikasi dampak hak anak pada kelompok usia yang berbeda sebagai akibat dari operasi perusahaan dan desain, pengembangan dan pengenalan produk dan layanan, serta peluang untuk mendukung hak anak dan remaja.</p>
<p>Mengembangkan standar industri untuk melindungi anak-anak secara online</p>	<p>Membuat dan menerapkan standar perusahaan dan industri untuk perlindungan anak-anak dan remaja, dengan memperhatikan industri dan fitur spesifik.</p>

<p>Mengintegrasikan pertimbangan hak anak ke dalam semua kebijakan perusahaan dan proses manajemen yang tepat <i>(lanjutan)</i></p>	<p>Mengadopsi pendekatan berbasis pemberdayaan dan pendidikan untuk perlindungan anak. Pertimbangkan hak perlindungan data anak-anak, hak mereka atas privasi dan kebebasan berbicara, sambil menawarkan pendidikan dan bimbingan melalui layanan perusahaan.</p> <p>Manfaatkan keahlian internal dan eksternal dan konsultasikan dengan pemangku kepentingan utama, termasuk anak-anak dan remaja, tentang mekanisme keamanan online anak untuk mendapatkan umpan balik dan panduan berkelanjutan tentang pendekatan perusahaan.</p> <p>Di Negara-negara yang tidak memiliki kerangka hukum yang memadai untuk perlindungan hak anak-anak dan remaja atas privasi dan kebebasan berekspresi, perusahaan harus memastikan kebijakan dan praktik sejalan dengan standar internasional. Lihat Resolusi Majelis Umum PBB 68/167 tentang hak privasi di era digital</p> <p>Pastikan akses untuk pemulihan dengan menetapkan mekanisme pengaduan dan pelaporan tingkat operasional untuk setiap pelanggaran hak anak (misalnya CSAM, konten atau kontak yang tidak pantas atau pelanggaran privasi).</p> <p>Nominasikan manajer kebijakan perlindungan anak atau orang lain yang ditunjuk yang dapat dihubungi untuk masalah COP. Jika seorang anak berada dalam risiko bahaya, manajer kebijakan perlindungan anak harus segera memberi tahu pihak yang berwenang.</p> <p>Pedoman editorial BBC (2019), misalnya, menetapkan penunjukan manajer kebijakan perlindungan anak, yang dianggap wajib dalam media layanan publik.</p>
<p>Mengembangkan proses standar ke CSAM</p>	<p>Bekerja sama dengan pemerintah, penegak hukum, masyarakat sipil dan organisasi hotline, industri memiliki peran penting dalam memerangi CSAM dengan mengambil tindakan berikut:</p> <p>Melarang mengunggah, memposting, mentransmisikan, membagikan, atau menyediakan konten yang melanggar hak pihak mana pun atau melanggar hukum lokal, negara bagian, nasional, atau internasional.</p> <p>Berkomunikasi dengan lembaga penegak hukum nasional atau hotline nasional untuk menyampaikan laporan CSAM segera setelah diketahui oleh penyedia.</p> <p>Pastikan bahwa prosedur internal tersedia untuk mematuhi tanggung jawab pelaporan berdasarkan hukum lokal dan internasional.</p> <p>Jika perusahaan beroperasi di pasar dengan pengawasan peraturan dan penegakan hukum yang kurang berkembang atas masalah ini, perusahaan dapat merujuk mereka yang ingin mengajukan laporan ke International Association of Internet Hotlines (INHOPE), di mana laporan dapat diajukan dengan hotline internasional mana pun.</p>

Mengembangkan proses standar ke CSAM
(lanjutan)

Menetapkan prosedur internal untuk memastikan kepatuhan di bawah hukum lokal dan internasional tentang memerangi CSAM.

Menetapkan posisi senior atau tim yang didedikasikan untuk mengintegrasikan prosedur ini ke dalam organisasi. Anggota industri kemudian harus melaporkan tindakan yang diambil dan hasil yang dicapai oleh tim ini dalam laporan tahunan perusahaan dan keberlanjutan mereka.

Ketika peraturan nasional tidak memberikan perlindungan yang memadai, perusahaan harus menghormati tetapi melampaui undang-undang nasional dan menggunakan pengaruh mereka untuk melobi perubahan legislatif untuk memungkinkan industri memerangi CSAM.

Posisi senior atau tim harus dibuat dalam organisasi, yang didedikasikan untuk mengintegrasikan prosedur ini dan memantau operasi. Ini harus tercermin secara transparan dalam laporan tahunan perusahaan dan keberlanjutan dan tersedia untuk publik.

Tentukan bahwa bisnis akan bekerja sama sepenuhnya dengan investigasi penegakan hukum jika konten ilegal dilaporkan atau ditemukan dan catat detail mengenai hukuman seperti denda atau pembatalan hak penagihan.

Menggunakan syarat dan ketentuan pelanggan dan/atau kebijakan penggunaan yang dapat diterima untuk secara eksplisit menyatakan posisi perusahaan atas penyalahgunaan layanannya untuk menyimpan atau membagikan CSAM dan konsekuensi dari penyalahgunaan apa pun.

Kembangkan proses pemberitahuan dan penghapusan serta pelaporan yang memungkinkan pengguna untuk melaporkan CSAM atau kontak yang tidak pantas dan profil/lokasi spesifik tempat terdeteksinya.

Tetapkan proses tindak lanjut laporan, setuju prosedur untuk menangkap bukti dan segera hapus atau blokir akses ke CSAM.

Pastikan bahwa, jika diperlukan, penyedia layanan meminta pendapat para ahli (misalnya badan COP nasional) sebelum menghancurkan konten ilegal.

Pastikan bahwa pihak ketiga yang relevan dengan siapa perusahaan memiliki hubungan kontraktual memiliki pemberitahuan yang kuat dan proses penghapusan yang sama.

Bersiaplah untuk menangani CSAM dan melaporkan kasus ke pihak yang berwenang. Jika hubungan dengan penegak hukum dan hotline nasional belum terjalin, libatkan mereka untuk mengembangkan proses bersama.

Bekerja dengan fungsi internal, seperti layanan pelanggan, pencegahan penipuan dan keamanan untuk memastikan bahwa bisnis dapat mengirimkan laporan dugaan konten ilegal langsung ke penegak hukum dan hotline.

Idealnya, ini harus dilakukan dengan cara yang tidak membuat staf garis depan terpapar konten berbahaya atau membuat korban kembali anak-anak dan remaja yang terkena dampak. Untuk mengatasi situasi di mana staf dapat terpapar materi yang kasar, terapkan kebijakan atau program untuk mendukung ketahanan, keselamatan, dan kesejahteraan staf.

<p>Mengembangkan proses standar ke CSAM (cont.)</p>	<p>Sertakan kebijakan penyimpanan dan pelestarian data untuk mendukung penegakan hukum jika terjadi penyelidikan kriminal melalui kegiatan seperti menangkap bukti. Dokumentasikan praktik perusahaan untuk menangani CSAM, dimulai dengan pemantauan dan perluasan hingga transfer akhir dan penghancuran konten. Sertakan daftar semua personel yang bertanggung jawab untuk menangani materi dalam dokumentasi.</p>
	<p>Mempromosikan mekanisme pelaporan untuk CSAM dan memastikan bahwa pelanggan tahu cara mengajukan laporan jika mereka menemukan konten tersebut. Jika hotline nasional tersedia, tawarkan tautan ke hotline tersebut dari situs web perusahaan dan dari layanan konten relevan apa pun yang dipromosikan oleh perusahaan.</p>
	<p>Gunakan semua layanan/kumpulan data yang relevan untuk mencegah penyebaran konten pelecehan seksual terhadap anak yang diketahui di layanan atau platform mereka.</p>
	<p>Secara aktif menilai semua konten yang dihosting di server perusahaan, termasuk komersial (bermerek atau dikontrak dari penyedia konten pihak ketiga) secara teratur. Pertimbangkan untuk menggunakan alat seperti pemindaian hash gambar pelecehan seksual anak yang diketahui, perangkat lunak pengenalan gambar, atau pemblokiran URL untuk menangani CSAM.</p>
<p>Menciptakan lingkungan online yang lebih aman dan sesuai usia</p>	<p>Industri dapat membantu menciptakan lingkungan digital yang lebih aman dan lebih menyenangkan bagi anak-anak dan remaja dari segala usia dengan mengambil tindakan berikut:</p>
	<p>Mengadopsi prinsip-prinsip keamanan dan privasi-by-design dalam teknologi dan layanan perusahaan dan memprioritaskan solusi yang mengurangi volume data yang berkaitan dengan anak-anak seminimal mungkin.</p>
	<p>Terapkan desain yang sesuai dengan usia dalam layanan yang ditawarkan.</p>
	<p>Menyajikan informasi kepada anak-anak mengenai aturan situs dengan cara yang dapat diakses dan sesuai usia, memberikan jumlah detail yang sesuai.</p>
	<p>Selain syarat dan ketentuan yang sesuai dengan usia dan dapat diakses, industri harus mengkomunikasikan informasi yang sama, dan dengan jelas, seperti aturan dan kebijakan utama. Ini harus menekankan perilaku yang dapat diterima dan tidak dapat diterima pada layanan, konsekuensi dari melanggar aturan apa pun, spesifikasi layanan dan apa yang disetujui pengguna melalui pendaftaran. Informasi semacam itu harus secara khusus ditujukan untuk pengguna muda dan orang tua serta pengasuh mereka.</p>
	<p>Menggunakan syarat layanan atau syarat dan ketentuan untuk menarik perhatian pengguna pada konten dalam layanan online perusahaan yang mungkin tidak sesuai untuk segala usia. Syarat dan ketentuan juga harus mencakup mekanisme yang jelas untuk melaporkan dan menangani pelanggaran aturan tersebut.</p>
	<p>Pertimbangkan untuk menyediakan mekanisme seperti perangkat lunak kontrol orang tua dan alat lain yang memungkinkan orang tua dan pengasuh untuk mengelola akses anak-anak mereka ke sumber daya Internet sambil memberikan panduan kepada mereka tentang penggunaan yang sesuai sehingga hak-hak anak-anak tidak dilanggar. Ini termasuk daftar blokir/izinkan, filter konten, pemantauan penggunaan, manajemen kontak, dan batas waktu/program.</p>

Menciptakan lingkungan online yang lebih aman dan sesuai usia (*lanjutan*)

Menawarkan opsi kontrol orang tua yang mudah digunakan yang memungkinkan orang tua dan pengasuh membatasi layanan dan konten tertentu yang dapat diakses anak-anak saat menggunakan perangkat elektronik. Pembatasan ini dapat mencakup kontrol tingkat jaringan dan perangkat, serta kontrol aplikasi. Mempertimbangkan bahwa ini memiliki implikasi besar pada kemampuan anak untuk meningkatkan keterampilan digital mereka dan mengganggu peluang mereka secara online, kontrol ini harus dirancang untuk anak-anak yang sangat muda sejalan dengan konteks perkembangan mereka dan dengan bimbingan yang tepat untuk orang tua.

Jika memungkinkan, promosikan layanan dukungan nasional yang dapat digunakan orang tua dan pengasuh untuk melaporkan pelanggaran dan mencari dukungan jika terjadi pelecehan atau eksploitasi.

Hindari konten iklan online yang berbahaya atau tidak pantas dan tetapkan kewajiban pengungkapan pelanggan untuk penyedia layanan dengan konten yang ditujukan untuk audiens dewasa dan dapat berbahaya bagi anak-anak dan remaja. Iklan berbahaya juga dapat mencakup iklan makanan dan minuman yang tinggi lemak, gula, atau garam.

Sejajarkan praktik bisnis dengan peraturan dan saran tentang pemasaran dan periklanan kepada anak-anak dan remaja. Pantau di mana, kapan, dan bagaimana anak-anak dan remaja mungkin menemukan pesan iklan yang berpotensi berbahaya yang ditujukan untuk segmen pasar lain.

Pastikan bahwa kebijakan pengumpulan data mematuhi undang-undang yang relevan mengenai privasi anak-anak dan remaja, termasuk mempertimbangkan apakah persetujuan orang tua diperlukan sebelum perusahaan komersial dapat mengumpulkan informasi pribadi dari atau tentang seorang anak.

Menyesuaikan dan menerapkan pengaturan privasi default yang ditingkatkan untuk pengumpulan, pemrosesan, penyimpanan, penjualan, dan penerbitan data pribadi, termasuk informasi terkait lokasi dan kebiasaan menjelajah, yang dikumpulkan dari orang-orang di bawah 18 tahun. Pengaturan privasi default dan informasi tentang pentingnya privasi harus sesuai dengan usia pengguna dan sifat layanan.

Menerapkan langkah-langkah teknis, seperti alat kontrol orang tua yang sesuai, keamanan berdasarkan desain, pengalaman yang dibedakan berdasarkan usia, konten yang dilindungi kata sandi, daftar blokir/izinkan, kontrol pembelian/waktu, fungsi penolakan, pemfilteran dan pemerataan, untuk mencegah akses di bawah umur dan paparan hingga konten atau layanan yang tidak pantas.

Menerapkan teknologi yang dapat mengidentifikasi usia pengguna dan menyajikannya dengan versi aplikasi yang sesuai dengan usia.

Untuk konten atau layanan yang sensitif terhadap usia, industri pemangku kepentingan harus mengambil langkah-langkah untuk memverifikasi usia pengguna. Jika memungkinkan, gunakan verifikasi usia untuk membatasi akses ke konten atau materi yang, baik menurut hukum atau kebijakan, hanya ditujukan untuk orang di atas usia tertentu.

Perusahaan juga harus menyadari potensi penyalahgunaan teknologi tersebut untuk membatasi hak anak-anak dan remaja atas kebebasan berekspresi dan akses ke informasi atau membahayakan privasi mereka.

Menciptakan lingkungan online yang lebih aman dan sesuai usia (*lanjutan*)

Memastikan bahwa konten dan layanan yang tidak sesuai untuk pengguna dari segala usia adalah:

- diklasifikasikan sejalan dengan standar nasional dan norma budaya;
- konsisten dengan standar yang ada di media yang setara;
- diidentifikasi dengan opsi tampilan yang menonjol untuk mengontrol akses;
- ditawarkan bersama dengan verifikasi usia, jika memungkinkan sesuai dan dengan persyaratan yang jelas terkait dengan penghapusan data identitas pribadi yang diperoleh melalui proses verifikasi.

Misalnya, sehubungan dengan standar media, semua otoritas pengatur media menyediakan serangkaian persyaratan untuk konten terkait usia dan penyedia Internet diharuskan untuk mengadaptasi repositori dan menerapkan pedoman pada penawaran konten mereka. Lihat, [Ofcom di Inggris Raya](#), [CSA di Prancis](#) dan [AGCOM di Italia](#).

Tawarkan alat pelaporan yang jelas dan kembangkan proses tindak lanjut untuk melaporkan konten yang tidak pantas, kontak dan penyalahgunaan, serta berikan umpan balik terperinci kepada pengguna layanan tentang proses pelaporan.

Pastikan pra-moderasi ruang interaktif yang dirancang untuk anak-anak dan remaja dengan cara yang sejalan dengan hak anak-anak atas privasi dan kapasitas mereka yang terus berkembang. Moderasi aktif dapat mendorong suasana di mana perundungan dan pelecehan tidak dapat diterima. Perilaku yang tidak dapat diterima meliputi:

- memposting komentar yang tidak menyenangkan atau mengancam di profil seseorang;
- menyiapkan profil palsu atau situs kebencian untuk mempermalukan korban;
- mengirim pesan berantai dan lampiran dengan maksud berbahaya;
- meretas akun seseorang untuk mengirim pesan ofensif kepada orang lain.

Lakukan tindakan pencegahan khusus dengan anggota staf atau kolaborator yang bekerja dengan anak-anak dan remaja, yang mungkin diperlukan pemeriksaan catatan kriminal awal dengan otoritas polisi.

Rujuk setiap insiden dugaan grooming segera ke tim manajemen eksekutif online atau interaktif yang bertanggung jawab untuk melaporkannya kepada pihak berwenang yang sesuai:

- melaporkan grooming kepada tim manajemen eksekutif dan kepada manajer kebijakan perlindungan anak yang dinominasikan, jika memungkinkan;
- memungkinkan pengguna untuk melaporkan dugaan insiden grooming langsung ke pihak berwenang;
- menetapkan kemungkinan kontak langsung melalui alamat email untuk memberi tahu dan melaporkan.

Prioritaskan keselamatan dan kesejahteraan anak setiap saat. Selalu bertindak dalam batas-batas profesional dan memastikan semua kontak dengan anak-anak sangat penting untuk layanan, program, acara, kegiatan atau proyek. Jangan pernah bertanggung jawab penuh atas seorang anak. Jika seorang anak membutuhkan grooming, beri tahu orang tua, wali, atau pendamping. Dengarkan dan hormati anak-anak setiap saat.

Jika ada yang berperilaku tidak pantas di sekitar anak-anak, laporkan perilaku tersebut ke kontak perlindungan anak setempat.

<p>Menciptakan lingkungan online yang lebih aman dan sesuai usia (<i>lanjutan</i>)</p>	<p>Tetapkan seperangkat aturan yang jelas yang ditempatkan dengan jelas dan gaungkan poin-poin penting dari persyaratan layanan dan pedoman penggunaan yang dapat diterima. Bahasa yang mudah digunakan untuk aturan ini harus mendefinisikan:</p> <ul style="list-style-type: none">• sifat layanan dan apa yang diharapkan dari penggunanya;• apa yang dapat dan tidak dapat diterima dalam hal konten, perilaku dan bahasa, serta melarang penggunaan ilegal;• konsekuensinya sebanding dengan pelanggaran, misalnya, pelaporan ke penegak hukum atau penangguhan akun pengguna. <p>Permudah pelanggan untuk melaporkan kekhawatiran tentang penyalahgunaan ke layanan pelanggan, dengan proses standar dan dapat diakses untuk menangani berbagai masalah, seperti menerima komunikasi yang tidak diinginkan (misalnya SMS spam).</p> <p>Bersikaplah transparan dan berikan informasi yang jelas kepada pelanggan tentang sifat layanan yang ditawarkan, misalnya:</p> <ul style="list-style-type: none">• jenis konten/layanan dan biaya;• usia minimum yang diperlukan untuk akses;• ketersediaan kontrol orang tua, termasuk apa yang dicakup oleh kontrol (misalnya jaringan) atau tidak tercakup (misalnya Wi-Fi) dan pelatihan tentang cara menggunakannya;• jenis informasi pengguna yang dikumpulkan dan bagaimana informasi tersebut digunakan. <p>Mempromosikan layanan dukungan nasional yang memungkinkan anak-anak dan remaja untuk melaporkan dan mencari dukungan dalam kasus pelecehan atau eksploitasi (lihat, misalnya, Child Helpline International).</p>
<p>Mendidik anak-anak, orang tua, dan pendidik tentang keselamatan anak-anak dan penggunaan TIK yang bertanggung jawab</p>	<p>Industri dapat melengkapi langkah-langkah teknis dengan kegiatan pendidikan dan pemberdayaan dengan mengambil tindakan berikut:</p> <p>Jelaskan dengan jelas konten yang tersedia dan kontrol orang tua yang sesuai atau setelan keamanan keluarga. Membuat bahasa dan terminologi dapat diakses, terlihat, jelas, dan relevan untuk semua pengguna, termasuk anak-anak, orang tua, dan pengasuh, terutama dalam kaitannya dengan syarat dan ketentuan, biaya yang terlibat dalam penggunaan konten atau layanan, kebijakan privasi, informasi keselamatan, dan mekanisme pelaporan.</p> <p>Edukasi pelanggan tentang cara mengelola masalah yang berkaitan dengan penggunaan internet, termasuk spam, pencurian data, dan kontak yang tidak pantas seperti penindasan dan grooming, serta jelaskan tindakan apa yang dapat diambil pelanggan dan bagaimana mereka dapat menyampaikan kekhawatiran tentang penggunaan yang tidak pantas.</p> <p>Menyiapkan mekanisme dan mengedukasi orang tua untuk terlibat dalam kegiatan TIK anak-anak dan remajanya, khususnya yang berasal dari anak-anak yang lebih kecil, dengan, misalnya, memungkinkan orang tua untuk meninjau pengaturan privasi anak-anak dan remaja.</p> <p>Berkolaborasi dengan pemerintah dan pendidik untuk membangun kapasitas orang tua untuk mendukung dan berbicara dengan anak-anak dan remaja mereka tentang menjadi warga negara digital dan pengguna TIK yang bertanggung jawab.</p>

<p>Mendidik anak-anak, orang tua, dan pendidik tentang keselamatan anak-anak dan penggunaan TIK yang bertanggung jawab (lanjutan)</p>	<p>Berdasarkan konteks lokal, menyediakan materi pendidikan untuk digunakan di sekolah dan rumah untuk meningkatkan penggunaan TIK oleh anak-anak dan remaja dan untuk mengembangkan pemikiran kritis untuk memungkinkan mereka berperilaku aman dan bertanggung jawab saat menggunakan layanan TIK.</p> <p>Dukung pelanggan dengan menyebarkan pedoman tentang keamanan online keluarga yang mendorong orang tua dan pengasuh untuk:</p> <ul style="list-style-type: none"> • membiasakan diri dengan produk dan layanan yang digunakan oleh anak-anak dan remaja; • memastikan penggunaan perangkat elektronik secara moderat oleh anak-anak dan remaja sebagai bagian dari gaya hidup sehat dan seimbang; • perhatikan baik-baik perilaku anak-anak dan remaja untuk mengidentifikasi perubahan yang dapat mengindikasikan cyberbullying atau pelecehan. <p>Berikan informasi yang diperlukan kepada orang tua untuk memahami bagaimana anak-anak dan remaja mereka menggunakan layanan TIK, menangani masalah yang berkaitan dengan konten dan perilaku berbahaya dan diperlengkapi untuk membimbing anak-anak dan remaja dalam penggunaan yang bertanggung jawab. Hal ini dapat difasilitasi melalui penggunaan alat dan interaksi dengan distrik sekolah untuk menyediakan kurikulum keamanan online untuk anak-anak dan materi pendidikan bagi orang tua.</p>
<p>Menggunakan kemajuan teknologi untuk melindungi dan mendidik anak-anak</p>	<p>AI yang menjaga privasi, yang memahami teks, gambar, percakapan, dan konteks, dapat mendeteksi dan mengatasi berbagai bahaya dan ancaman online, dan menggunakan informasi tersebut untuk memberdayakan dan mendidik anak-anak untuk menghadapinya. Ketika dilakukan dalam lingkungan perangkat pintar, ini dapat melindungi data dan privasi kaum muda sambil tetap mendukung mereka.</p> <p>Layanan publik dan media nasional dapat memainkan peran penting melalui penawaran program mereka (offline dan online) untuk mendidik orang tua dan anak-anak dan membuat mereka sadar akan risiko dan peluang dunia online</p>
<p>Mempromosikan teknologi digital sebagai mode untuk keterlibatan sipil lebih lanjut</p>	<p>Industri dapat mendorong dan memberdayakan anak-anak dan remaja dengan mendukung hak mereka untuk berpartisipasi melalui tindakan berikut:</p> <p>Berikan informasi tentang layanan untuk menyoroti manfaat yang diperoleh anak-anak dengan berperilaku baik dan bertanggung jawab, seperti menggunakan layanan untuk tujuan kreatif.</p> <p>Menetapkan prosedur tertulis yang memastikan implementasi kebijakan dan proses yang konsisten yang melindungi kebebasan berekspresi bagi semua pengguna, termasuk anak-anak dan remaja, serta dokumentasi kepatuhan terhadap kebijakan ini.</p>

<p>Mempromosikan teknologi digital sebagai mode untuk keterlibatan sipil lebih lanjut (lanjutan)</p>	<p>Hindari pemblokiran berlebihan terhadap konten yang sah dan sesuai dengan perkembangan. Untuk memastikan bahwa permintaan dan alat pemfilteran tidak disalahgunakan untuk membatasi akses anak-anak dan remaja ke informasi, memastikan transparansi tentang konten yang diblokir dan menetapkan proses bagi pengguna untuk melaporkan pemblokiran yang tidak disengaja. Proses ini harus tersedia untuk semua konsumen, termasuk webmaster. Setiap proses pelaporan harus memberikan persyaratan layanan yang jelas, bertanggung jawab, dan diadili.</p> <p>Mengembangkan platform online yang mempromosikan hak anak-anak dan remaja untuk mengekspresikan diri; memfasilitasi partisipasi mereka dalam kehidupan publik; dan mendorong kolaborasi, kewirausahaan, dan partisipasi sipil mereka.</p> <p>Mengembangkan konten pendidikan untuk anak-anak dan remaja yang mendorong pembelajaran, pemikiran kreatif dan pemecahan masalah.</p> <p>Mempromosikan literasi digital, peningkatan kapasitas, dan keterampilan TIK untuk membekali anak-anak dan remaja, terutama mereka yang berada di daerah pedesaan dan kurang terlayani, untuk memanfaatkan sumber daya TIK dan berpartisipasi penuh dengan aman di dunia digital.</p> <p>Berkolaborasi dengan masyarakat sipil dan pemerintah setempat dalam prioritas nasional dan lokal untuk memperluas akses universal dan adil ke TIK, platform dan perangkat, dan infrastruktur yang mendasarinya untuk mendukungnya.</p> <p>Informasikan dan libatkan pelanggan, termasuk orang tua, pengasuh, anak-anak dan kaum muda, tentang layanan yang ditawarkan, misalnya:</p> <ul style="list-style-type: none">• jenis konten dan kontrol orang tua yang sesuai;• mekanisme pelaporan untuk kasus penyalahgunaan, penyalahgunaan, dan konten yang tidak pantas atau ilegal;• prosedur tindak lanjut untuk laporan;• jenis layanan yang dibatasi usia;• penggunaan layanan interaktif "merek sendiri" yang aman dan bertanggung jawab. <p>Terlibat dengan masalah yang lebih luas seputar kewarganegaraan digital yang aman dan bertanggung jawab, misalnya reputasi online dan jejak digital, konten berbahaya, dan grooming. Pertimbangkan untuk bermitra dengan pakar lokal, seperti LSM anak-anak, badan amal dan kelompok pengasuhan anak-anak, untuk membantu membentuk pesan perusahaan dan menjangkau audiens yang dituju.</p> <p>Jika bisnis sudah bekerja dengan anak-anak atau sekolah, misalnya, through corporate social responsibility programmes, investigate the kemungkinan memperluas keterlibatan ini untuk mencakup mendidik dan terlibat dengan anak-anak dan remaja, dan pendidik pada pesan COP.</p>
<p>Berinvestasi dalam penelitian</p>	<p>Berinvestasi dalam penelitian berbasis bukti dan analisis mendalam tentang teknologi digital, dampak teknologi pada anak-anak, perlindungan anak dan pertimbangan hak-hak anak sehubungan dengan lingkungan digital, untuk mengintegrasikan sistem perlindungan online ke dalam layanan yang digunakan oleh anak-anak dan remaja dan lebih memahami jenis intervensi apa yang paling efektif dalam meningkatkan pengalaman online anak-anak.</p>

Tipologi perusahaan TIK

Meskipun pedoman ITU ini ditargetkan untuk industri TIK secara keseluruhan, penting untuk menyadari bahwa layanan yang ditawarkan perusahaan TIK, cara mereka beroperasi, skema peraturan di bawah yang mereka fungsikan, dan ruang lingkup serta skala penawaran mereka sangat berbeda. Setiap perusahaan teknologi yang produk dan layanannya ditargetkan secara langsung atau tidak langsung pada anak-anak dapat memperoleh manfaat dari prinsip-prinsip umum yang diuraikan sebelumnya dan dapat beradaptasi, berdasarkan mereka bidang operasi tertentu. Ide intinya adalah untuk mendukung dan memandu industri TIK dalam mengambil langkah-langkah yang tepat untuk melindungi anak-anak secara online dengan lebih baik dari risiko bahaya sambil memberdayakan mereka untuk menavigasi dunia online dengan cara terbaik. Tipologi di bawah ini akan membantu memberikan pemahaman yang lebih jelas tentang beberapa audiens target dan bagaimana mereka cocok dalam daftar periksa di bagian berikut. Perlu dicatat bahwa ini hanya beberapa kategori contoh spesifik dan tidak lengkap:

- (a) Penyedia layanan internet, termasuk melalui layanan broadband telepon rumah tetap atau layanan data seluler operator jaringan seluler: sementara ini biasanya mencerminkan layanan yang ditawarkan dalam jangka panjang untuk pelanggan berlangganan, itu juga dapat diperluas ke bisnis yang menyediakan hotspot WI-FI publik gratis atau berbayar.
- (b) Platform jejaring sosial/perpesanan dan platform game online.
- (c) Produsen perangkat keras dan perangkat lunak, seperti penyedia perangkat genggam termasuk ponsel, konsol game, perangkat rumah berbasis bantuan suara, Internet of Things, dan mainan pintar yang terhubung ke Internet untuk anak-anak.
- (d) Perusahaan yang menyediakan media digital (pembuat konten, menyediakan akses ke atau hosting konten).
- (e) Perusahaan yang menyediakan layanan streaming, termasuk streaming langsung.
- (f) Perusahaan yang menawarkan layanan penyimpanan file digital, penyedia layanan berbasis cloud.

5. Daftar periksa terkait fitur

Bab ini melengkapi daftar periksa umum sebelumnya untuk industri dengan menawarkan rekomendasi untuk bisnis yang menyediakan layanan dengan fitur khusus untuk menghormati dan mendukung hak-hak anak secara online. Daftar periksa khusus fitur berikut menguraikan cara-cara untuk melengkapi prinsip-prinsip dan pendekatan umum yang disajikan dalam Tabel 1, karena berlaku untuk layanan yang berbeda, dan oleh karena itu harus dipertimbangkan selain langkah-langkah dalam Tabel 1.

Fitur-fitur yang disorot di sini adalah crosscutting dan beberapa daftar periksa khusus fitur mungkin relevan untuk perusahaan yang sama.

Daftar periksa fitur berikut diatur oleh dan merujuk kembali ke area utama yang sama dengan pedoman umum dalam Tabel 1. Setiap daftar periksa fitur telah dikembangkan bekerja sama dengan kontributor utama dan, sebagai hasilnya, ada variasi kecil dalam tabel.

5.1 Fitur A: Menyediakan konektivitas, penyimpanan data, dan layanan hosting

Akses internet sangat penting untuk realisasi hak-hak anak, dan konektivitas dapat membuka seluruh dunia bagi anak-anak. Penyedia layanan konektivitas, penyimpanan data, dan hosting memiliki peluang luar biasa untuk membangun keamanan dan privasi ke dalam penawaran mereka untuk anak-anak dan remaja. Layanan ini memiliki alamat antara lain operator seluler, penyedia layanan Internet, sistem penyimpanan data, dan layanan hosting.

Operator seluler memungkinkan akses ke Internet dan menawarkan berbagai layanan data khusus seluler. Banyak operator telah mendaftar ke kode praktik COP dan menawarkan berbagai alat dan sumber daya informasi untuk mendukung komitmen mereka.

Sebagian besar penyedia layanan Internet bertindak sebagai saluran, menyediakan akses ke dan dari Internet, dan repositori untuk data melalui layanan hosting, caching, dan penyimpanan mereka. Akibatnya, mereka memiliki tanggung jawab utama untuk melindungi anak-anak secara online.

Akses internet di ruang publik

Menjadi semakin umum bagi kotamadya, pengecer, perusahaan transportasi, jaringan hotel, serta bisnis dan organisasi lain untuk menyediakan akses Internet melalui hotspot Wi-Fi. Akses semacam itu biasanya gratis atau disediakan dengan biaya minimal, dan kadang-kadang dengan formalitas masuk minimal sebagai layanan publik, atau oleh perusahaan untuk menarik pelanggan ke sana tempat atau membujuk lebih banyak orang untuk menggunakan layanannya.

Mempromosikan Wi-Fi adalah cara yang efektif untuk memastikan ketersediaan Internet di area tertentu. Namun, penjagaan perlu dilakukan ketika akses tersebut disediakan di ruang publik di mana anak-anak cenderung hadir secara teratur. Pengguna perlu memperhatikan fakta bahwa sinyal Wi-Fi mungkin tersedia untuk orang yang lewat dan data pengguna yang disusupi. Oleh karena itu, penyedia Wi-Fi tidak akan selalu dapat mendukung atau mengawasi penggunaan koneksi Internet yang telah disediakan dan oleh karena itu pengguna perlu mengambil tindakan pencegahan agar tidak untuk berbagi informasi sensitif melalui Wi-Fi yang tersedia untuk umum.

Di ruang publik, penyedia Wi-Fi mungkin ingin mempertimbangkan langkah-langkah tambahan untuk melindungi anak-anak dan remaja, seperti:

- Secara proaktif memblokir akses ke alamat web yang diketahui berisi konten yang tidak pantas untuk khalayak luas, di samping upaya mereka untuk memblokir akses ke CSAM.
- Termasuk klausul dalam syarat dan ketentuan penggunaan yang melarang penggunaan layanan Wi-Fi untuk mengakses atau menampilkan materi apa pun yang mungkin tidak cocok di lingkungan tempat anak-anak hadir. Syarat dan ketentuan juga harus mencakup mekanisme yang jelas mengenai konsekuensi dari pelanggaran aturan tersebut.
- Mengambil semua tindakan untuk melindungi dari akses yang tidak sah, yang dapat mengakibatkan manipulasi atau kehilangan data pribadi.
- Memasang filter pada sistem Wi-Fi untuk memperkuat kebijakan tentang materi yang tidak pantas.
- Menyediakan prosedur dan perangkat lunak untuk signpost dan menawarkan kontrol orang tua opsional yang terkait dengan akses anak-anak dan remaja ke konten Internet

Praktik yang baik: Peraturan telekomunikasi di sebagian besar negara anggota Uni Eropa, misalnya, menetapkan bahwa akses ke jaringan harus diidentifikasi, melalui kartu SIM individu atau lainnya alat identifikasi.

Tabel 2 memberikan panduan bagi penyedia layanan konektivitas, penyimpanan data, dan hosting tentang tindakan yang dapat mereka ambil untuk meningkatkan perlindungan online anak dan partisipasi anak-anak.

Tabel 2: Daftar periksa COP untuk Fitur A: Menyediakan konektivitas, data, dan layanan hosting

Mengintegrasikan pertimbangan hak anak ke dalam semua kebijakan perusahaan dan proses manajemen yang sesuai	<p>Penyedia layanan konektivitas, penyimpanan data, dan hosting dapat mengidentifikasi, mencegah, dan mengurangi dampak buruk TIK terhadap hak-hak anak dan remaja, dan mengidentifikasi peluang untuk mendukung kemajuan hak-hak anak dan remaja.</p> <p><i>Lihat pedoman umum pada Tabel 1.</i></p>
Mengembangkan proses standar untuk menangani CSAM	<p>Bekerja sama dengan pemerintah, penegak hukum, masyarakat sipil, dan organisasi hotline, penyedia layanan konektivitas, penyimpanan data, dan hosting dapat memainkan peran kunci dalam memerangi CSAM dengan mengambil tindakan berikut:</p> <p>Berkolaborasi dengan pemerintah, penegak hukum, masyarakat sipil, dan organisasi hotline untuk menangani CSAM secara efektif dan melaporkan kasus kepada pihak berwenang yang sesuai. Jika hubungan dengan penegak hukum dan hotline belum terjalin, terlibatlah dengan mereka untuk mengembangkan proses bersama.</p> <p>Penyedia layanan konektivitas, penyimpanan data, atau hosting juga dapat memberikan pelatihan TIK untuk penegakan hukum.</p> <p>Jika sebuah perusahaan beroperasi di pasar dengan pengawasan hukum dan penegakan hukum yang kurang berkembang terhadap masalah ini, itu dapat merujuk mereka yang ingin mengajukan laporan ke Asosiasi Internasional Hotline Internet (INHOPE) di mana laporan dapat diajukan ke hotline internasional mana pun.</p> <p>Pertimbangkan untuk menyebarkan URL atau daftar pemblokiran situs web yang diakui secara internasional yang dibuat oleh otoritas yang sesuai (misalnya, penegak hukum atau hotline nasional, Cybertip Canada, Interpol, IWF), untuk mempersulit pengguna mengakses CSAM yang teridentifikasi.</p> <p>Mengembangkan proses pemberitahuan dan penghapusan dan pelaporan, dan menghubungkan laporan penyalahgunaan ke proses tersebut dengan perjanjian layanan publik tentang prosedur respons dan waktu penghapusan.</p> <p>Lihat, misalnya, Panduan UNICEF dan GSMA tentang kebijakan dan praktik pemberitahuan dan penghapusan.</p> <p>Siapkan mekanisme pelaporan dengan informasi yang jelas tentang penggunaannya dengan, misalnya, memberikan panduan tentang konten ilegal dan perilaku yang akan dilaporkan dan mengklarifikasi materi apa yang tidak dapat dilampirkan dengan laporan untuk menghindari distribusi lebih lanjut di web.</p>

<p>Mengembangkan proses standar untuk menangani CSAM (cont.)</p>	<p>Mendukung penegakan hukum jika terjadi investigasi kriminal melalui kegiatan seperti menangkap bukti.</p> <p>Menggunakan syarat layanan dan ketentuan untuk secara khusus melarang penggunaan layanan untuk menyimpan, berbagi, atau mendistribusikan CSAM. Pastikan persyaratan ini dengan jelas menyatakan bahwa CSAM tidak akan ditoleransi.</p> <p>Pastikan bahwa syarat layanan dan ketentuan menyatakan bahwa perusahaan akan bekerja sama sepenuhnya dengan penyelidikan <u>penegakan hukum jika CSAM ditemukan atau dilaporkan</u>.</p> <p>Saat ini ada dua solusi pelaporan untuk CSAM online di tingkat nasional: hotline dan portal pelaporan. Daftar lengkap terbaru dari semua hotline dan portal yang ada dapat ditemukan di INHOPE.</p> <p>Hotline: Jika hotline nasional tidak tersedia, jelajahi peluang untuk menyiapkannya (lihat Panduan Hotline GSMA INHOPE untuk berbagai opsi, termasuk bekerja sama dengan INHOPE dan INHOPE Foundation. Versi interaktif panduan GSMA INHOPE tersedia yang memberikan panduan tentang cara mengembangkan proses internal bagi staf layanan pelanggan untuk mengirimkan laporan konten yang dipertanyakan kepada penegak hukum dan INHOPE.</p> <p>Portal pelaporan: IWF menawarkan solusi portal pelaporan yang memungkinkan pengguna Internet di negara dan negara tanpa hotline, untuk melaporkan gambar dan video dugaan pelecehan seksual anak langsung ke IWF melalui halaman portal online yang dipesan lebih dahulu.</p> <p>Untuk penyedia konektivitas, penyimpanan data, dan layanan hosting yang layanannya melibatkan semacam hosting konten (banyak yang tidak), perhatikan dan hapus proses harus ada.</p>
<p>Menciptakan lingkungan digital yang lebih aman dan sesuai dengan usia</p>	<p>Penyedia layanan konektivitas, penyimpanan data, dan hosting, dapat membantu menciptakan lingkungan digital yang lebih aman dan menyenangkan bagi anak-anak dari segala usia dengan <u>mengambil tindakan berikut</u>:</p> <p>Penyedia layanan penyimpanan data / hosting harus mempertimbangkan untuk menyajikan fungsi pelaporan di semua halaman web dan layanan, dan mengembangkan dan mendokumentasikan proses yang jelas untuk mengelola laporan penyalahgunaan dengan cepat atau pelanggaran syarat dan ketentuan lainnya.</p> <p>Penyedia konektivitas harus menawarkan kontrol teknis merek sendiri atau rambu-rambu ketersediaan alat yang dibuat oleh penyedia spesialis yang sesuai untuk layanan yang ditawarkan dan mudah bagi pengguna akhir untuk menerapkan dan menawarkan kemungkinan memblokir atau memfilter akses ke Internet melalui jaringan perusahaan. Menyediakan mekanisme verifikasi usia yang sesuai jika perusahaan menawarkan konten atau layanan (termasuk merek sendiri atau layanan pihak ketiga yang dipromosikan oleh perusahaan), yang hanya legal atau sesuai untuk pengguna dewasa (misalnya game, lotere tertentu).</p>

<p>Mendidik anak-anak, orang tua, dan pendidik tentang keselamatan anak-anak dan penggunaan TIK yang bertanggung jawab</p>	<p>Penyedia layanan konektivitas, penyimpanan data, dan hosting harus menggemakan pesan utama dari syarat dan ketentuan dalam pedoman komunitas yang ditulis dalam bahasa yang mudah digunakan untuk mendukung anak-anak dan orang tua serta pengasuh mereka. Dalam layanan itu sendiri, pada titik mengunggah konten, sertakan pengingat tentang topik seperti jenis konten yang dianggap tidak pantas.</p>
	<p>Berikan informasi kepada anak-anak dan remaja tentang penggunaan Internet yang lebih aman. Pertimbangkan cara-cara kreatif untuk mempromosikan pesan-pesan utama seperti berikut ini:</p> <p>"Jangan pernah membagikan detail kontak apa pun, termasuk lokasi fisik dan nomor telepon Anda, dengan siapa pun yang tidak Anda kenal secara langsung."</p> <p>"Jangan pernah setuju untuk berkumpul dengan siapa pun yang Anda temui secara online sendiri tanpa berkonsultasi dengan orang dewasa terlebih dahulu. Selalu beri tahu teman tepercaya tentang keberadaanmu."</p> <p>"Jangan menanggapi pesan yang menindas, cabul, atau menyinggung. Tapi simpan buktinya - jangan hapus pesannya."</p> <p>"Beri tahu orang dewasa atau teman tepercaya jika Anda merasa tidak nyaman atau kesal tentang sesuatu atau seseorang."</p> <p>"Jangan pernah memberikan kata sandi atau nama pengguna akun Anda! Ketahuilah bahwa orang lain secara online dapat memberikan informasi palsu untuk meyakinkan Anda agar membagikan informasi pribadi Anda."</p>
	<p>Penyedia layanan dapat bermitra dengan organisasi yang berada di posisi yang baik untuk mendidik dan mendukung anak-anak tentang penggunaan internet yang lebih aman dan masalah terkait.</p> <p>Lihat Panduan praktis Child Helpline International dan GSMA untuk Saluran Bantuan Anak dan Operator Seluler: Bekerja sama untuk melindungi hak-hak anak sebagai contoh.</p>
<p>Mempromosikan teknologi digital sebagai mode untuk keterlibatan sipil lebih lanjut</p>	<p><i>Lihat pedoman umum pada Tabel 1.</i></p>

5.2 Fitur B: Menawarkan konten digital yang dikurasi

Internet menyediakan semua jenis konten dan kegiatan, banyak di antaranya ditujukan untuk anak-anak dan remaja. Layanan yang menawarkan konten yang dikurasi secara editorial memiliki peluang luar biasa untuk membangun keamanan dan privasi ke dalam penawaran mereka untuk anak-anak dan remaja.

Fitur layanan ini membahas bisnis yang membuat konten mereka sendiri, dan yang memungkinkan akses ke konten digital. Ini mengacu pada, antara lain, layanan streaming berita dan multimedia, penyiaran layanan nasional dan publik dan industri game.

Tabel 3 memberikan panduan bagi penyedia layanan yang menawarkan konten yang dikurasi secara editorial tentang kebijakan dan tindakan yang dapat mereka ambil untuk meningkatkan perlindungan dan partisipasi online anak

Tabel 3: Daftar periksa COP untuk Fitur B:
Menawarkan konten digital yang dikurasi

<p>Mengintegrasikan pertimbangan hak anak ke dalam semua kebijakan perusahaan dan proses manajemen yang sesuai</p>	<p>Layanan yang menyediakan konten digital yang dikurasi dapat membantu mengidentifikasi, mencegah, dan mengurangi dampak buruk TIK terhadap hak-hak anak dan remaja, dan mengidentifikasi peluang untuk mendukung kemajuan hak-hak anak dan remaja dengan mengambil tindakan berikut</p>
	<p>Mengembangkan kebijakan yang menjaga kesejahteraan anak-anak dan remaja yang menyumbangkan konten secara online untuk mempertimbangkan kesejahteraan fisik dan emosional serta martabat orang-orang di bawah 18 tahun yang terlibat dalam program, film, permainan, berita, dll. terlepas dari persetujuan yang mungkin telah diberikan oleh orang tua atau orang dewasa lainnya.</p>
<p>Mengembangkan proses standar untuk menangani CSAM</p>	<p>Bekerja sama dengan pemerintah, penegak hukum, masyarakat sipil, dan organisasi hotline, perusahaan yang menawarkan konten digital yang dikurasi dapat memainkan peran kunci dalam memerangi CSAM melalui tindakan berikut:</p> <p>Dalam kasus CSAM, misalnya melalui fitur "komentar" atau "ulasan" di mana pengguna memiliki kapasitas untuk mengunggah konten, staf harus menghubungi tim manajemen eksekutif yang bertanggung jawab untuk melaporkan materi tersebut kepada pihak berwenang yang sesuai. Selain itu, mereka harus:</p> <ul style="list-style-type: none">• segera menginformasikan aparat penegak hukum nasional;• memberi tahu manajer mereka dan melaporkan materi tersebut kepada manajer kebijakan perlindungan anak;• menghubungi layanan investigasi internal melalui telepon atau email dengan rincian insiden dan untuk meminta saran;• tunggu saran dari instansi terkait sebelum menghapus materi, menyimpannya ke ruang bersama atau meneruskannya.

<p>Mengembangkan proses standar untuk menangani CSAM</p>	<p>Jika materi diidentifikasi, itu harus dilaporkan langsung ke organisasi yang berspesialisasi dalam keamanan Internet yang mengoperasikan sistem pelaporan hotline untuk anggota masyarakat dan profesional teknologi informasi untuk melaporkan bentuk spesifik dari konten online yang berpotensi ilegal.</p> <p>Misalnya, berdasarkan Kebijakan Perlindungan dan Perlindungan Anak, BBC telah merilis panduan editorial tentang berinteraksi dengan anak-anak dan remaja secara online. Ini telah mengembangkan daftar periksa lebih lanjut dan kode etik untuk bekerja dengan anak-anak dan remaja secara online, yang juga meluas ke subkontraktor dan penyedia eksternal. Kebijakan Ofcom tentang perlindungan anak untuk Inggris Raya membahas konten online, perangkat seluler, dan konsol game secara terpisah.</p> <p>Terapkan strategi eskalasi yang cepat dan kuat jika CSAM diposting atau perilaku ilegal dicurigai. Untuk tujuan ini:</p> <ul style="list-style-type: none">• menawarkan kepada pengguna metode sederhana dan mudah diakses untuk memperingatkan produsen konten tentang pelanggaran aturan apa pun dari komunitas online;• menghapus konten yang melanggar aturan;• menawarkan kepada pengguna metode sederhana dan mudah diakses untuk memperingatkan produsen konten tentang pelanggaran aturan apa pun dari komunitas online;• menghapus konten yang melanggar aturan; <p>Sebelum mengunggah konten yang dikurasi secara editorial yang sensitif terhadap usia ke situs jejaring sosial, perhatikan syarat dan ketentuan situs tersebut. Peka terhadap persyaratan usia minimum di berbagai situs jejaring sosial.</p> <p>Syarat dan ketentuan setiap ruang online juga harus mencakup mekanisme pelaporan yang jelas untuk pelanggaran aturan tersebut.</p>
<p>Menciptakan lingkungan online yang lebih aman dan sesuai usia</p>	<p>Perusahaan yang menawarkan konten digital yang dikurasi dapat membantu menciptakan lingkungan digital yang lebih aman dan lebih menyenangkan bagi anak-anak dan remaja dari segala usia dengan mengambil tindakan berikut:</p> <p>Bekerja dengan orang lain di industri untuk mengembangkan klasifikasi konten / sistem peringkat usia yang didasarkan pada standar nasional atau internasional yang diterima dan konsisten dengan pendekatan yang diambil di media yang setara.</p> <p>Jika memungkinkan, klasifikasi konten harus konsisten di berbagai platform media, misalnya, trailer film di bioskop dan di smartphone akan menunjukkan kepada pelanggan klasifikasi yang sama.</p> <p>Mengembangkan produk yang ramah anak dan sesuai usia untuk anak-anak dan remaja yang aman secara desain dan dilengkapi dengan sistem verifikasi usia yang solid.</p>

Menciptakan lingkungan online yang lebih aman dan sesuai usia (*cont*)

Untuk membantu orang tua dan orang lain memutuskan apakah konten sesuai dengan usia untuk anak-anak dan remaja, bangun aplikasi dan layanan di semua media agar selaras dengan sistem rating konten.

Mengadopsi metode verifikasi usia yang sesuai untuk mencegah anak-anak dan remaja mengakses konten, situs, produk, atau layanan interaktif yang sensitif terhadap usia.

Berikan saran dan pengingat tentang sifat dan klasifikasi usia dari konten yang mereka gunakan.

Perusahaan yang menawarkan layanan audiovisual dan multimedia mungkin ingin memberikan nomor identifikasi pribadi kepada pengguna yang ingin mengakses konten yang dapat berbahaya bagi anak-anak dan remaja.

Pastikan transparansi harga untuk produk dan layanan, serta informasi yang dikumpulkan tentang pengguna. Pastikan bahwa kebijakan pengumpulan data mematuhi undang-undang yang relevan mengenai privasi anak-anak dan remaja, termasuk apakah persetujuan orang tua diperlukan sebelum perusahaan komersial dapat mengumpulkan informasi pribadi dari atau tentang seorang anak.

Pastikan bahwa iklan atau komunikasi komersial dapat dikenali dengan jelas seperti itu.

Awasi konten yang tersedia secara online dan sesuaikan dengan grup pengguna yang kemungkinan akan mengaksesnya dengan misalnya, menetapkan kebijakan yang sesuai untuk iklan online untuk anak-anak dan remaja. Jika penawaran konten mendukung elemen interaktif, seperti komentar, forum online, jejaring sosial, platform game, ruang obrolan, atau papan pesan, komunikasikan serangkaian "aturan rumah" yang jelas dalam bahasa yang ramah pelanggan dalam persyaratan layanan dan pedoman pengguna.

Putuskan tingkat keterlibatan apa yang diinginkan sebelum meluncurkan layanan online. Layanan yang ditujukan untuk menarik bagi anak-anak hanya boleh menyajikan konten yang cocok untuk audiens muda. Jika ragu, otoritas nasional yang bertanggung jawab atas perlindungan anak dapat dikonsultasikan.

Memberikan pelabelan konten yang jelas dan faktual. Perhatikan bahwa pengguna dapat menemukan konten yang tidak pantas dengan mengikuti tautan di situs pihak ketiga yang melewati halaman yang mengontekstualisasikan.

Mendidik anak-anak, orang tua, dan pendidik tentang keselamatan anak-anak dan penggunaan TIK yang bertanggung jawab

Perusahaan yang menawarkan konten digital yang dikurasi dapat melengkapi langkah-langkah teknis dengan kegiatan pendidikan yang memberdayakan anak-anak dengan mengambil tindakan berikut:

Memberi pelanggan informasi spesifik dan jelas tentang konten, seperti jenis konten, rating/pembatasan usia, bahasa atau kekerasan yang kuat, dan kontrol orang tua yang sesuai yang tersedia; dan tentang cara melaporkan penyalahgunaan dan konten yang tidak pantas atau ilegal, serta bagaimana laporan akan ditangani.

Di dunia interaktif, informasi ini harus disediakan dalam bentuk label konten untuk setiap program.

Dorong orang dewasa, terutama orang tua, pengasuh, dan pendidik, untuk terlibat dalam konsumsi konten online anak-anak dan remaja, sehingga mereka dapat membantu dan membimbing anak-anak dan remaja dalam memilih konten saat melakukan pembelian, dan membantu menetapkan aturan perilaku.

Bantu anak-anak (dan orang tua serta pengasuh) untuk belajar mengelola waktu layar mereka dan memahami cara menggunakan teknologi dengan cara yang terasa baik bagi mereka, termasuk kapan harus berhenti dan melakukan sesuatu yang lain.

Berikan aturan penggunaan dalam bahasa yang jelas dan dapat diakses yang mendorong anak-anak dan remaja untuk waspada dan bertanggung jawab ketika mereka menavigasi Internet.

Buat alat yang sesuai dengan usia, seperti tutorial dan pusat bantuan. Bekerja dengan program pencegahan online atau tatap muka dan klinik konseling bila perlu. Misalnya, jika ada risiko anak-anak dan remaja menjadi terlalu terlibat dengan teknologi, sehingga sulit bagi mereka untuk mengembangkan hubungan pribadi atau mengambil bagian dalam kegiatan fisik yang sehat, sebuah situs dapat menyediakan tautan kontak untuk saluran bantuan atau layanan konseling.

Buat informasi keselamatan, seperti tautan ke saran, menonjol, mudah diakses, dan jelas ketika konten online cenderung menarik bagi sebagian besar anak-anak dan remaja.

Tawarkan alat panduan orang tua, seperti "kunci" untuk mengontrol konten yang dapat diakses melalui browser tertentu

Bekerja sama dengan orang tua untuk memastikan bahwa informasi yang diungkapkan di Internet tentang anak-anak tidak membahayakan mereka. Bagaimana anak-anak diidentifikasi dalam konten yang dikurasi secara editorial memerlukan pertimbangan yang cermat dan akan bervariasi sesuai dengan konteksnya. Dapatkan persetujuan berdasarkan informasi anak-anak saat menampilkan mereka dalam program, film, video, dll., Jika memungkinkan, dan hormati penolakan apa pun untuk ambil bagian.

Mempromosikan teknologi digital sebagai mode untuk keterlibatan sipil lebih lanjut	Perusahaan yang menawarkan konten digital yang dikurasi dapat mendorong dan memberdayakan anak-anak dan remaja dengan mendukung hak mereka untuk berpartisipasi melalui tindakan berikut:
	Mengembangkan dan / atau menawarkan berbagai konten berkualitas tinggi, menantang, mendidik, menyenangkan, dan menarik yang sesuai dengan usia dan membantu anak-anak dan remaja memahami dunia tempat mereka tinggal. Selain menarik dan dapat digunakan, dapat diandalkan dan aman, konten tersebut dapat berkontribusi untuk perkembangan fisik, mental, dan sosial anak-anak dan remaja dengan memberikan kesempatan baru untuk menghibur dan mendidik.
	Konten yang memberdayakan anak-anak untuk merangkul keragaman dan menjadi panutan positif harus sangat dianjurkan.

5.3 Fitur C: Menghosting konten buatan pengguna dan hubungan pengguna

Ada suatu masa ketika dunia online didominasi oleh orang dewasa tetapi sekarang jelas bahwa anak-anak dan remaja adalah peserta utama di berbagai platform dalam menciptakan dan berbagi dalam ledakan konten buatan pengguna. Fitur layanan ini membahas antara lain layanan media sosial, aplikasi dan website yang berkaitan dengan realisasi kreatif.

Layanan yang menghubungkan pengguna satu sama lain dapat dibagi dalam tiga kategori:

- Terutama aplikasi perpesanan (Facebook Messenger, Groupme, Line, Tinder, Telegram, Viber, WhatsApp).
- Terutama layanan jejaring sosial yang mencari dan menghosting konten buatan pengguna dan memungkinkan pengguna untuk berbagi konten dan terhubung di dalam dan di luar jaringan mereka (Instagram, Facebook, SnapChat, TikTok).
- Terutama aplikasi streaming langsung (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

Penyedia layanan meminta usia minimum untuk mendaftar ke platform tetapi ini sulit untuk ditegakkan karena verifikasi usia bergantung pada usia yang dilaporkan. Sebagian besar layanan yang menghubungkan pengguna baru satu sama lain juga memungkinkan fitur berbagi lokasi, yang membuat anak-anak dan remaja yang menggunakan layanan ini semakin rentan terhadap bahaya offline .

Tabel 4, yang telah diadaptasi dari aturan yang diterapkan oleh salah satu jejaring sosial terbesar, memberikan panduan bagi penyedia layanan yang menghosting konten buatan pengguna dan menghubungkan pengguna baru pada kebijakan dan tindakan yang dapat mereka ambil untuk meningkatkan perlindungan online anak dan partisipasi anak-anak.

Tabel 4: Daftar periksa COP untuk Fitur C: Menghosting konten buatan pengguna dan hubungkan pengguna

<p>Mengintegrasikan pertimbangan hak anak ke dalam semua kebijakan perusahaan dan proses manajemen yang sesuai</p>	<p>Layanan yang menghosting konten buatan pengguna dan menghubungkan pengguna dapat mengidentifikasi, mencegah, dan mengurangi dampak buruk TIK terhadap hak anak-anak dan remaja, dan mengidentifikasi peluang untuk mendukung kemajuan hak-hak anak dan remaja .</p>
	<p><i>Lihat pedoman umum pada Tabel 1.</i></p>
<p>Mengembangkan proses standar untuk menangani CSAM</p>	<p>Bekerja sama dengan pemerintah, penegak hukum, masyarakat sipil, dan organisasi hotline, perusahaan yang menghosting konten buatan pengguna dan menghubungkan pengguna dapat memainkan peran kunci dalam memerangi CSAM dengan mengambil tindakan berikut:</p>
	<p>Menetapkan prosedur bagi semua situs untuk memberikan bantuan segera kepada penegak hukum selama keadaan darurat dan untuk penyelidikan rutin.</p>
	<p>Tentukan bahwa bisnis akan bekerja sama sepenuhnya dengan penyelidikan penegakan hukum jika konten ilegal dilaporkan atau ditemukan dan catat detail mengenai hukuman seperti denda atau pembatalan hak istimewa penagihan.</p>
	<p>Bekerja dengan fungsi internal seperti layanan pelanggan, pencegahan penipuan, dan keamanan untuk memastikan bahwa bisnis dapat mengirimkan laporan dugaan konten ilegal langsung ke penegak hukum dan hotline. Idealnya, ini harus dilakukan dengan cara yang tidak mengekspos staf garis depan ke konten atau mereviktisasi anak/anak dan remaja yang terkena dampak. Untuk mengatasi situasi di mana staf mungkin terpapar materi yang kasar, terapkan kebijakan atau program untuk mendukung ketahanan, keselamatan, dan kesejahteraan staf.</p>
	<p>Menggunakan persyaratan layanan dan ketentuan untuk melarang konten dan perilaku ilegal, dengan alasan bahwa:</p>
	<ul style="list-style-type: none"> • konten berbahaya, termasuk dugaan grooming anak-anak dengan maksud penyalahgunaan kontak atau non-kontak, tidak akan ditoleransi;
	<ul style="list-style-type: none"> • konten ilegal, termasuk pengunggahan atau penyebaran CSAM lebih lanjut, tidak akan ditoleransi;
	<ul style="list-style-type: none"> • perusahaan akan merujuk dan berkolaborasi penuh dengan penyelidikan penegakan hukum jika konten ilegal, atau pelanggaran apa pun terhadap kebijakan perlindungan anak, dilaporkan atau ditemukan.
	<p>Dokumentasikan praktik perusahaan untuk menangani CSAM, dimulai dengan pemantauan dan perluasan hingga transfer akhir dan penghancuran konten. Sertakan daftar semua personel yang bertanggung jawab untuk menangani materi dalam dokumentasi.</p>
	<p>Mengadopsi kebijakan terkait kepemilikan konten buatan pengguna, termasuk opsi untuk menghapus konten buatan pengguna atas permintaan pengguna. Hapus konten yang melanggar kebijakan penyedia dan beri tahu pengguna yang telah mempostingnya tentang pelanggaran tersebut.</p>

<p>Mengembangkan proses standar untuk menangani CSAM (cont.)</p>	<p>Menunjukkan bahwa kegagalan pengguna untuk mematuhi kebijakan untuk penggunaan yang dapat diterima akan memiliki konsekuensi, termasuk:</p> <ul style="list-style-type: none">• penghapusan konten, penangguhan, atau penutupan akun mereka;• mencabut kemampuan mereka untuk berbagi jenis konten tertentu atau menggunakan fitur tertentu;• mencegah mereka menghubungi anak-anak;• merujuk masalah pada penegakan hukum .
<p>Mengembangkan proses standar untuk menangani materi pelecehan seksual terhadap anak di bawah umur</p>	<p>Mempromosikan mekanisme pelaporan untuk CSAM atau konten ilegal lainnya dan memastikan bahwa pelanggan mengetahui cara mengajukan laporan jika mereka menemukan konten tersebut.</p> <p>Membangun sistem dan menyediakan staf terlatih untuk menilai masalah berdasarkan kasus per kasus dan mengambil tindakan yang tepat. Membangun operasi dukungan pengguna yang komprehensif dan memiliki sumber daya yang baik</p> <p>Tim. Idealnya, tim-tim ini akan dilatih untuk menangani berbagai jenis insiden untuk memastikan bahwa respons yang memadai diberikan dan tindakan yang tepat diambil. Ketika pengguna mengajukan keluhan, tergantung pada jenis insiden, itu harus dialihkan ke staf yang sesuai.</p> <p>Perusahaan juga dapat membentuk tim khusus untuk menangani banding pengguna jika laporan mungkin telah diajukan karena kesalahan.</p>
	<p>Memiliki proses untuk segera menghapus atau memblokir akses ke CSAM, termasuk pemberitahuan dan proses penghapusan untuk menghapus konten ilegal segera setelah diidentifikasi. Pastikan bahwa pihak ketiga dengan siapa perusahaan memiliki hubungan kontraktual memiliki pemberitahuan yang sama kuatnya dan proses penghapusan.</p> <p>Jika undang-undang mengizinkan, materi tersebut dapat disimpan untuk bukti kejahatan jika terjadi penyelidikan.</p>
	<p>Mengembangkan sistem teknis yang dapat mendeteksi konten ilegal yang diketahui dan dapat mencegahnya diunggah, termasuk ke grup pribadi, atau menandainya untuk segera ditinjau oleh tim keamanan perusahaan. Ambil semua langkah yang relevan untuk melindungi layanan agar tidak disalahgunakan untuk menjadi tuan rumah, menyebarkan, atau membuat CSAM.</p> <p>Jika memungkinkan, buat langkah-langkah teknis proaktif untuk menganalisis objek dan metadata yang terkait dengan profil untuk mendeteksi perilaku atau pola kriminal, dan mengambil tindakan yang sesuai.</p>
	<p>Jika aplikasi atau layanan memungkinkan pelanggan untuk mengunggah dan menyimpan foto di server yang dimiliki atau dioperasikan oleh perusahaan, miliki proses dan alat untuk mengidentifikasi gambar yang kemungkinan besar berisi CSAM. Pertimbangkan teknik identifikasi proaktif seperti teknologi pemindaian atau tinjauan manusia.</p>

Pedoman untuk industri tentang Perlindungan Online Anak

Menciptakan lingkungan online yang lebih aman dan sesuai usia	Penyedia layanan yang menawarkan konten buatan pengguna dan menghubungkan pengguna dapat membantu menciptakan lingkungan digital yang lebih aman dan lebih menyenangkan bagi anak-anak dari segala usia dengan mengambil tindakan berikut:
	Berkomunikasi dalam bahasa yang ramah pelanggan dalam persyaratan layanan dan pedoman pengguna seperangkat "aturan rumah" yang jelas yang mendefinisikan: <ul data-bbox="630 470 1356 627" style="list-style-type: none">• sifat layanan dan apa yang diharapkan dari penggunanya;• apa yang dapat dan tidak dapat diterima dalam hal konten, perilaku dan bahasa serta melarang penggunaan ilegal;• konsekuensi dari setiap pelanggaran, misalnya, melaporkan ke penegak hukum dan penangguhan akun pengguna.
	Pesan keamanan dan hukum utama harus disajikan dalam format yang sesuai dengan usia (yaitu menggunakan ikon dan simbol intuitif) baik saat mendaftar maupun secara tepat waktu karena tindakan yang berbeda diambil di situs.
	Permudah pelanggan untuk melaporkan kekhawatiran tentang penyalahgunaan ke layanan pelanggan, dengan proses standar dan dapat diakses untuk menangani berbagai masalah, seperti menerima komunikasi yang tidak diinginkan (spam, penindasan) atau melihat konten yang tidak pantas.
	Berikan setelan berbagi konten dan visibilitas yang sesuai dengan usia. Misalnya, buat pengaturan privasi dan visibilitas untuk anak-anak dan remaja lebih ketat daripada pengaturan untuk orang dewasa secara default.
	Menegakkan persyaratan usia minimum dan mendukung penelitian dan pengembangan sistem verifikasi usia baru seperti biometrik, menggunakan standar internasional yang dikenal untuk pengembangan alat tersebut. Ambil langkah-langkah untuk mengidentifikasi dan menghapus pengguna di bawah umur yang telah salah mengartikan usia mereka untuk mendapatkan akses. Pertimbangan perlu diberikan pada pengumpulan data pribadi tambahan yang mungkin diperlukan dan kebutuhan untuk membatasi pengumpulan dan penyimpanan informasi ini dan pemrosesannya. Jika belum ada, siapkan proses masuk yang sesuai untuk menentukan apakah pengguna cukup umur untuk mengakses konten atau layanan tanpa mengorbankan identitas, lokasi, dan detail pribadi mereka. Gunakan sistem verifikasi usia fungsional yang ditetapkan secara nasional sebagaimana mestinya, jika ada langkah-langkah yang relevan untuk privasi data subjek anak. Fungsi pelaporan atau layanan/pusat bantuan yang dapat mendorong pengguna untuk melaporkan orang-orang yang telah memalsukan usia mereka.
	Lindungi pengguna yang lebih muda dari komunikasi yang tidak diundang dan pastikan bahwa pedoman privasi dan pengumpulan informasi sudah ada.

Menciptakan lingkungan online yang lebih aman dan sesuai usia
(lanjutan)

Temukan cara untuk meninjau gambar dan video yang dihosting dan menghapus gambar dan video yang tidak pantas jika terdeteksi. Alat seperti pemindaian hash gambar yang diketahui dan perangkat lunak pengenalan gambar tersedia untuk membantu dalam hal ini. Dalam layanan yang ditargetkan untuk anak-anak, foto dan video dapat diperiksa sebelumnya untuk memastikan bahwa anak-anak tidak mempublikasikan informasi pribadi yang sensitif tentang diri mereka sendiri atau orang lain.

Sejumlah tindakan dapat digunakan untuk mengontrol akses ke konten buatan pengguna dan melindungi anak-anak dan remaja secara online dari konten yang tidak pantas atau ilegal. Pastikan bahwa kata sandi yang aman digunakan sebagai langkah untuk melindungi anak-anak dan remaja dalam bermain game dan pengaturan media sosial lainnya. Teknik lain termasuk:

- meninjau grup diskusi untuk mengidentifikasi materi pelajaran berbahaya, ujaran kebencian, dan perilaku ilegal, serta menghapus konten tersebut jika ditemukan melanggar ketentuan penggunaan;
- mengembangkan alat untuk secara aktif mencari dan menghapus konten yang ilegal atau melanggar syarat dan layanan perusahaan, serta alat untuk mencegah pengunggahan konten ilegal yang diketahui ke situs;
- pra-moderator papan pesan dengan tim moderator anak-anak dan remaja khusus yang menyaring konten yang bertentangan dengan "aturan rumah" yang diterbitkan. Setiap pesan dapat diperiksa sebelum dipublikasikan, dan moderator juga dapat melihat dan menandai pengguna yang mencurigakan, serta pengguna yang dalam kesulitan;
- membentuk tim tuan rumah komunitas yang berfungsi sebagai titik kontak pertama bagi moderator ketika mereka memiliki kekhawatiran tentang pengguna.

Bertanggung jawab untuk meninjau konten komersial, termasuk di forum, jejaring sosial, dan situs game. Menerapkan standar dan aturan yang sesuai untuk melindungi anak-anak dari iklan yang tidak sesuai usia dan menetapkan batasan yang jelas untuk iklan online untuk anak-anak dan remaja.

Mendidik anak-anak, orang tua, dan pendidik tentang keselamatan anak-anak dan penggunaan TIK yang bertanggung jawab

Penyedia layanan yang menawarkan konten buatan pengguna dapat melengkapi langkah-langkah teknis dengan kegiatan pendidikan dan pemberdayaan dengan mengambil tindakan berikut:

Buat bagian yang didedikasikan untuk tips keselamatan, artikel, fitur, dan dialog tentang kewarganegaraan digital, serta tautan ke konten yang berguna dari pakar pihak ketiga. Saran keselamatan harus mudah dilihat dan diberikan dalam bahasa yang mudah dipahami. Penyedia platform juga didorong untuk memiliki antarmuka navigasi yang seragam di berbagai perangkat, seperti komputer, tablet, atau ponsel.

Tawarkan informasi yang jelas kepada orang tua tentang jenis konten dan layanan yang tersedia, termasuk, misalnya, penjelasan tentang situs jejaring sosial dan layanan berbasis lokasi, bagaimana Internet diakses melalui perangkat seluler, dan opsi yang tersedia bagi orang tua untuk menerapkan kontrol.

Mendidik anak-anak, orang tua, dan pendidik tentang keselamatan anak-anak dan penggunaan TIK yang bertanggung jawab (<i>cont</i>)	Beri tahu orang tua tentang cara melaporkan penyalahgunaan, penyalahgunaan, dan konten yang tidak pantas atau ilegal, serta cara menangani laporan tersebut. Beri tahu mereka layanan apa yang dikenai pembatasan usia dan cara lain untuk berperilaku aman dan bertanggung jawab saat menggunakan layanan interaktif.
	Membangun sistem berbasis "kepercayaan dan reputasi" untuk mendorong perilaku yang baik dan memungkinkan teman sebaya untuk mengajarkan praktik terbaik satu sama lain dengan memberi contoh. Mempromosikan pentingnya pelaporan sosial, yang memungkinkan orang untuk menjangkau pengguna lain atau teman tepercaya untuk membantu menyelesaikan konflik atau membuka percakapan tentang konten yang mengganggu.
	Berikan saran dan peringatan tentang sifat layanan atau konten tertentu dan cara menikmatinya dengan aman. Buat pedoman komunitas ke dalam layanan interaktif, misalnya, dengan popup keamanan yang mengingatkan pengguna tentang perilaku yang sesuai dan aman, seperti tidak memberikan detail kontak mereka .
	Bekerja sama dengan orang tua dan membimbing mereka untuk memastikan bahwa informasi yang diungkapkan di Internet tentang anak-anak tidak membahayakan mereka. Dapatkan persetujuan berdasarkan informasi anak-anak saat menampilkan mereka melalui konten buatan pengguna mereka sendiri, jika memungkinkan, dan hormati penolakan apa pun.
Mempromosikan teknologi digital sebagai mode untuk keterlibatan sipil lebih lanjut	Layanan yang menghosting konten buatan pengguna dapat mendorong dan memberdayakan anak-anak dan remaja dengan mendukung hak mereka untuk berpartisipasi.
<i>Lihat pedoman umum pada Tabel 1.</i>	

5.4 Fitur D: Sistem berbasis kecerdasan buatan

Dengan meningkatnya perhatian yang diberikan pada teknologi pembelajaran mendalam, istilah "kecerdasan buatan", "pembelajaran mesin", dan "pembelajaran mendalam" telah digunakan secara bergantian oleh masyarakat umum untuk mencerminkan konsep mereplikasi perilaku "cerdas" dalam mesin. Di bagian ini, kami fokus pada cara-cara pembelajaran mesin dan proses pembelajaran mendalam memengaruhi kehidupan anak-anak dan pada akhirnya, hak asasi manusia mereka.

"Karena kemajuan eksponensial teknologi berbasis kecerdasan buatan selama beberapa tahun terakhir, kerangka kerja internasional saat ini yang melindungi hak-hak anak tidak secara eksplisit membahas banyak hal isu-isu yang diangkat oleh pengembangan dan penggunaan kecerdasan buatan. Namun, itu mengidentifikasi beberapa hak yang mungkin terlibat oleh teknologi ini, dan dengan demikian memberikan tempat awal yang penting untuk setiap analisis tentang bagaimana hak-hak anak-anak mungkin secara positif atau negatif dipengaruhi oleh teknologi baru, seperti hak atas privasi, pendidikan, bermain, dan non-diskriminasi." ¹⁸

Penerapan AI dapat mempengaruhi dampak pada anak-anak dari berbagai layanan yang digunakan di jejaring sosial, seperti platform streaming video. Algoritme pembelajaran mesin, mesin rekomendasi yang terutama digunakan oleh platform berbagi video populer,

dioptimalkan untuk memastikan penayangan maksimum video tertentu dalam waktu tertentu.¹⁹ Teknologi layar sentuh dan desain platform ini memungkinkan anak-anak yang sangat muda untuk menelusuri dan menavigasi konten ini. Ada kekhawatiran khusus bahwa algoritme yang menggunakan video yang direkomendasikan dapat menjebak anak-anak dalam "gelembung filter" konten yang buruk atau tidak pantas. Karena anak-anak sangat rentan terhadap rekomendasi konten, "video terkait" yang mengejutkan dapat menarik perhatian mereka dan mengalihkan mereka dari program yang lebih ramah anak.²⁰

AI juga berdampak pada perlindungan online anak sehubungan dengan mainan pintar. Proses berbeda yang terlibat dalam pengoperasian mainan pintar datang dengan tantangan mereka sendiri, yaitu mainan (yang berinteraksi dengan anak), aplikasi seluler, bertindak sebagai titik akses untuk Wi-Fi koneksi, dan akun online mainan/konsumen yang dipersonalisasi, tempat data disimpan. Mainan semacam itu berkomunikasi dengan server berbasis cloud yang menyimpan dan memproses data yang disediakan oleh anak-anak yang berinteraksi dengan mainan tersebut. Model ini memiliki masalah privasi jika keamanan tidak diterapkan di setiap lapisan, yang telah ditunjukkan oleh banyak kasus peretasan di mana detail pribadi bocor. Selain itu, beberapa perangkat yang diretas (termasuk perangkat pintar yang mendukung web seperti monitor bayi, asisten suara, dll.) dapat digunakan untuk pengawasan pengguna tanpa sepengetahuan atau persetujuan mereka.

Saat mengintegrasikan mekanisme respons ke ancaman yang terdeteksi terhadap anak-anak yang menggunakan perangkat ini dengan, misalnya, memberikan tips dan rekomendasi berdasarkan perilaku yang terdeteksi (seperti yang disebutkan sebelumnya dengan aplikasi BBC Own It), sangat penting bahwa perusahaan yang merancang perangkat pintar mendasarkan rekomendasi ini pada bukti dan mengembangkannya dengan berkonsultasi dengan ahli perlindungan anak dan perlindungan anak.

Sementara beberapa perusahaan memajukan prinsip-prinsip untuk penggunaan Etis AI,²¹ tidak jelas apakah ada kebijakan publik yang ditujukan untuk AI dan anak-anak.²² Beberapa asosiasi teknologi dan perdagangan, dan kelompok ilmu komputer, telah menyusun prinsip-prinsip etika sehubungan dengan AI.²³ Namun, ini tidak secara eksplisit merujuk pada hak-hak anak, cara-cara di mana teknologi AI ini dapat menciptakan risiko bagi anak-anak, atau rencana proaktif untuk menguranginya.

"Seperti perusahaan, pemerintah di seluruh dunia telah mengadopsi strategi untuk menjadi pemimpin dalam pengembangan dan penggunaan AI, mendorong lingkungan yang menyenangkan bagi para inovator dan perusahaan."²⁴ Namun, tidak jelas bagaimana strategi nasional semacam itu secara langsung membahas hak-hak anak.

¹⁸ UNICEF and UC Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.

¹⁹ Ibid.

²⁰ Ibid.

²¹ See Microsoft, "Salient Human Rights Issues", Report - FY17; and Google, "Responsible Development of AI" (2018).

²² Microsoft Official Blog, "The Future Computed: Artificial Intelligence and its role in society", 2018.

²³ The Guardian, "'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft", 2016", 2016.

²⁴ Ibid

Meningkatkan penanganan Facebook terhadap konten terkait bunuh diri dan melukai diri sendiri

Pada tahun 2019, Situs Web mulai menyelenggarakan konsultasi rutin dengan para ahli dari seluruh dunia untuk membahas beberapa topik yang lebih sulit yang terkait dengan bunuh diri dan melukai diri sendiri. Ini termasuk cara menangani catatan bunuh diri, risiko yang terkait dengan isi konten daring yang menyedihkan dan penggambaran bunuh diri yang layak diberitakan. Rincian lebih lanjut dari pertemuan ini tersedia di [halaman Pencegahan Bunuh Diri](#) baru Situs Web, di Pusat Keamanannya . Konsultasi ini menghasilkan beberapa perbaikan pada cara Situs Web menangani jenis konten ini. Kebijakan mengenai [melukai diri sendiri](#), misalnya, diperkuat untuk melarang gambar pemotongan grafis untuk menghindari mempromosikan atau memicu tindakan menyakiti diri sendiri secara tidak sengaja. Bahkan ketika seseorang mencari dukungan atau mengekspresikan diri untuk membantu pemulihan mereka, Situs Web sekarang menampilkan layar sensitivitas atas gambar luka melukai diri sendiri yang disembuhkan. Jenis isi konten ini sekarang ditemukan melalui penerapan AI di mana tindakan pada konten yang berpotensi berbahaya, termasuk menghapusnya atau menambahkan layar sensitivitas, dapat diambil secara otomatis. Dari April hingga Juni 2019, Situs Web dan lebih dari sekadar

1,5 juta konten bunuh diri dan melukai diri sendiri di situsnya dan mengidentifikasi lebih dari 95 persen konten tersebut sebelum dilaporkan oleh pengguna. Selama periode waktu yang sama, Instagram bertindak atas lebih dari 800 ribu konten serupa, di mana lebih dari 77 persen terdeteksi sebelum dilaporkan oleh pengguna.

Identitas potensi perundungan atau kekerasan peer-to-peer secara waktu nyata dan mengirim pesan kepada pengguna

Instagram menerapkan AI untuk membasmi perilaku seperti penghinaan, mempermalukan, dan tidak menghormati. Dengan menggunakan perkakas pelaporan yang canggih, Moderator dapat dengan cepat menutup akun milik pelaku Bullying online.

Praktik yang baik: Penggunaan kecerdasan buatan dalam identifikasi materi pelecehan seksual anak

Dibangun di atas kontribusi Microsoft yang murah hati terhadap FotoDNA untuk memerangi eksploitasi anak dan peluncuran Google Picasa Keamanan API baru-baru ini, Situs Web juga telah mengembangkan teknologi untuk mendeteksi pelecehan seksual terhadap anak-anak puas.

Dikenal sebagai PDQ dan TMK+PDQF, teknologi ini adalah bagian dari serangkaian alat yang digunakan Facebook untuk mendeteksi konten berbahaya. Algoritma dan alat lain yang tersedia untuk industri termasuk pHash, aHash dan dHash. Algoritma pencocokan foto Situs Web, PDQ, berutang banyak inspirasi kepada pHash, meskipun dibangun dari bawah ke atas sebagai algoritma yang berbeda dengan implementasi perangkat lunak independen. Teknologi pencocokan video, TMK+PDQF, dikembangkan bersama oleh [tim Riset AI Situs Web](#) dan akademisi dari Universitas Modena dan Reggio Emilia di Italia.

Teknologi ini menciptakan cara yang efisien untuk menyimpan file sebagai hash digital pendek yang dapat menentukan apakah dua file sama atau serupa, bahkan tanpa gambar atau video asli. Hash juga dapat lebih mudah dibagikan dengan perusahaan lain dan organisasi nirlaba.

PDQ dan TMK+PDQF dirancang untuk beroperasi pada skala tinggi, mendukung aplikasi video-frame-hashing dan real-time.

Beberapa rekomendasi bagi bisnis untuk menyelaraskan prinsip-prinsip mereka saat merancang dan menerapkan solusi berbasis AI yang menargetkan anak-anak disediakan dalam Tabel 5.

Rekomendasi tersebut didasarkan pada upaya UNICEF untuk mengembangkan panduan kebijakan global tentang AI dan anak-anak, yang akan ditujukan untuk pemerintah dan industri. Silakan lihat <https://www.unicef.org/globalinsight/featured-projects/ai-children> untuk informasi lebih lanjut tentang proyek ini. Rekomendasi tersebut juga mengacu pada makalah UNICEF dan UC Berkeley tentang AI dan Hak Anak.²⁵

Tabel 5: Daftar periksa COP untuk Fitur D: Sistem berbasis Kecerdasan Buatan

Mengintegrasikan pertimbangan hak anak ke dalam semua kebijakan perusahaan dan proses manajemen yang sesuai	Penyedia sistem berbasis AI dapat mengidentifikasi, mencegah, dan mengurangi dampak buruk TIK terhadap hak-hak anak dan remaja, dan mengidentifikasi peluang untuk mendukung kemajuan hak-hak anak dan remaja.
---	--

²⁵ UNICEF and UC Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.

<p>Mengintegrasikan pertimbangan hak anak ke dalam semua kebijakan perusahaan dan proses manajemen yang sesuai</p>	<p>Sistem AI harus dirancang, dikembangkan, diimplementasikan, dan diteliti untuk menghormati, mempromosikan, dan memenuhi hak-hak anak, sebagaimana diabadikan dalam Konvensi Hak-Hak Anak. Semakin berpengalaman di lingkungan digital, adalah waktu yang didedikasikan untuk grooming dan bantuan khusus. Sistem AI harus dimanfaatkan untuk memberikan dukungan ini secara maksimal.</p> <p>Gabungkan pendekatan desain inklusif ketika mengembangkan produk yang dihadapi anak, yang memaksimalkan keragaman gender, geografis, dan budaya, dan mencakup berbagai pemangku kepentingan, seperti orang tua, guru, psikolog anak, dan, jika sesuai, anak-anak itu sendiri.</p>
	<p>Kerangka kerja tata kelola, termasuk pedoman etika, undang-undang, standar, dan badan pengatur, harus dibentuk untuk mengawasi proses yang memastikan bahwa penerapan sistem AI tidak melanggar hak-hak anak.</p>
<p>Mengembangkan proses standar untuk menangani CSAM</p>	<p>Bekerja sama dengan pemerintah, penegak hukum, masyarakat sipil, dan organisasi hotline, penyedia sistem berbasis AI memainkan peran kunci dalam memerangi CSAM dengan mengambil tindakan berikut:</p> <p><i>Lihat pedoman umum pada Tabel 1.</i></p>
<p>Menciptakan lingkungan online yang lebih aman dan sesuai usia</p>	<p>Penyedia sistem berbasis AI dapat membantu menciptakan lingkungan digital yang lebih aman dan lebih menyenangkan bagi anak-anak dari segala usia dengan mengambil tindakan berikut:</p> <p>Mengadopsi pendekatan multi-disiplin ketika mengembangkan teknologi yang memengaruhi anak-anak dan berkonsultasi dengan masyarakat sipil, termasuk akademisi, untuk mengidentifikasi dampak potensial dari teknologi ini terhadap hak-hak beragam pengguna akhir potensial.</p> <p>Menerapkan keamanan berdasarkan desain dan privasi berdasarkan desain untuk produk dan layanan yang ditujukan kepada atau umumnya digunakan oleh anak-anak.</p> <p>Karena sistem AI haus data, perusahaan yang menggunakan AI untuk layanan mereka harus menerapkan kewaspadaan khusus sehubungan dengan pengumpulan, pemrosesan, penyimpanan, penjualan, dan penerbitan data pribadi anak-anak.</p> <p>Sistem AI harus transparan, karena seharusnya mungkin untuk menemukan bagaimana dan mengapa suatu sistem membuat keputusan tertentu atau, dalam kasus robot, bertindak seperti itu. Transparansi ini sangat penting untuk mengembangkan kepercayaan dan memfasilitasi audit, investigasi, dan jalan lain ketika dicurigai membahayakan anak-anak .</p> <p>Pastikan bahwa ada mekanisme fungsional dan hukum untuk jalan lain jika anak-anak, atau mengaku, dirugikan melalui sistem AI. Proses harus ditetapkan untuk ganti rugi tepat waktu dari setiap output diskriminatif, dan badan pengawas yang dibentuk untuk banding dan pemantauan terus-menerus terhadap keselamatan dan perlindungan anak-anak.</p> <p>Akuntabilitas dan mekanisme ganti rugi berjalan beriringan .</p>

Pedoman untuk industri tentang Perlindungan Online Anak

Menciptakan lingkungan online yang lebih aman dan sesuai usia (cont)	Kembangkan rencana untuk menangani data yang sangat sensitif, termasuk pengungkapan penyalahgunaan atau bahaya lain yang dapat dibagikan dengan perusahaan melalui produk-produknya. Platform digital dan sistem AI harus meminimalkan pengumpulan data pada anak-anak dan memaksimalkan kontrol anak-anak atas data yang mereka buat. Ketentuan penggunaan harus dapat dimengerti bagi anak-anak untuk memberdayakan kesadaran dan hak pilihan mereka.
Mendidik anak-anak, orang tua, dan pendidik tentang keselamatan anak-anak dan penggunaan TIK yang bertanggung jawab	Penyedia sistem berbasis AI dapat melengkapi langkah-langkah teknis dengan kegiatan pendidikan dan pemberdayaan. Seharusnya dimungkinkan untuk menjelaskan tujuan sistem AI kepada pengguna anak dan orang tua atau pengasuh mereka untuk memberdayakan mereka untuk memutuskan untuk menggunakan atau menolak platform tersebut.
Mempromosikan teknologi digital sebagai mode untuk keterlibatan sipil lebih lanjut	Penyedia sistem berbasis AI dapat mendorong dan memberdayakan anak-anak dan remaja dengan mendukung hak mereka untuk berpartisipasi. <i>Lihat pedoman umum pada Tabel 1.</i>
Menggunakan kemajuan teknologi untuk melindungi dan mendidik anak-anak	Sistem berbasis AI harus dikembangkan untuk mendukung perkembangan dan kesejahteraan anak-anak sebagai hasil dalam semua desain, pengembangan, dan implementasi sistem. Metrik pengembangan dan kesejahteraan terbaik yang tersedia dan diterima secara luas harus menjadi titik referensi mereka. Perusahaan harus berinvestasi dalam penelitian dan pengembangan alat berbasis AI etis untuk mendeteksi tindakan CSAE online, dan pelecehan dan intimidasi online, bekerja sama dengan para ahli utama tentang hak-hak anak dan anak-anak itu sendiri. Kemajuan teknologi AI harus diterapkan untuk menargetkan pesan yang sesuai dengan usia untuk anak-anak tanpa mengorbankan identitas, lokasi, dan detail pribadi mereka.

Referensi

[Teks GDPR](#) (Peraturan (EU) 2016/679 dari Parlemen Eropa dan Dewan 27 April 2016 tentang perlindungan orang perseorangan sehubungan dengan pemrosesan data pribadi dan tentang pergerakan bebas data tersebut, dan mencabut Arahan 95/46/ EC (Peraturan Perlindungan Data Umum)), dan teks yang dipublikasikan di [Jurnal Resmi UE](#).

[Revisi AVMS \(Audio Visual Media Services\)](#) amandemen Directive 2010/13/EU tentang koordinasi ketentuan tertentu yang ditetapkan oleh hukum, peraturan atau tindakan administratif di Negara Anggota mengenai penyediaan layanan media audiovisual (Audiovisual Media Services Directive) mengingat perubahan realitas pasar dan [Teks sebagaimana diterbitkan dalam Jurnal Resmi Uni Eropa](#).

kebijakan BBC:

- Kebijakan perlindungan dan perlindungan anak versi 2017, revisi 2018, dan versi terbaru 2019
- Bekerja dengan kaum muda dan anak-anak di BBC;
- Kerangka Kerja untuk Perusahaan Produksi Independen yang bekerja di BBC Productions tentang aturan penyedia eksternal tentang perlindungan anak;
- Panduan: Berinteraksi dengan anak-anak dan remaja secara online pada pedoman editorial untuk kegiatan online.

Investigasi yang membuktikan tidak menghormati verifikasi usia untuk media sosial di Inggris Raya: 2016, 2017; 2020.

Glosarium

Definisi di bawah ini terutama diambil dari terminologi yang ada yang ditetapkan dalam Konvensi Hak Anak, 1989, serta Interagency Working Group on Sexual Exploitation of Children dalam [Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, 2016 \(Luxembourg Guidelines\)](#), oleh [Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 2007](#), serta oleh laporan [Global Kids Online UNICEF, 2019](#).

Remaja

Remaja adalah orang berusia 10-19 tahun. Penting untuk dicatat bahwa "remaja" bukanlah istilah yang mengikat di bawah hukum internasional, dan orang-orang di bawah usia 18 tahun dianggap sebagai anak-anak, sedangkan orang-orang 18–19 tahun dianggap dewasa, kecuali mayoritas dicapai lebih awal di bawah hukum nasional.²⁶

Kecerdasan buatan (AI)

Dalam arti luas, kecerdasan buatan (AI) mengacu secara tidak jelas pada sistem yang merupakan fiksi ilmiah murni (disebut AI "kuat" dengan bentuk sadar diri) dan sistem yang sudah beroperasi dan mampu melakukan tugas-tugas yang sangat kompleks (sistem yang dijelaskan sebagai AI "lemah" atau "sedang", seperti pengenalan wajah atau suara, dan mengemudi di kendaraan).²⁷

Sistem AI

Sistem AI adalah sistem berbasis mesin yang dapat, untuk serangkaian tujuan yang ditentukan manusia, membuat prediksi, rekomendasi, atau keputusan yang memengaruhi lingkungan nyata atau virtual. Sistem AI dirancang untuk beroperasi dengan berbagai tingkat otonomi.²⁸

²⁶ UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014.

²⁷ Council of Europe, "What's AI?".

²⁸ OECD, "Recommendation of the Council on Artificial Intelligence", 2019.

Alexa

Amazon Alexa, yang hanya dikenal sebagai Alexa, adalah asisten AI virtual yang dikembangkan oleh Amazon. Ia mampu melakukan interaksi suara, pemutaran musik, membuat daftar tugas, mengatur alarm, streaming podcast, memutar buku audio, dan menyediakan cuaca, lalu lintas, olahraga, dan informasi real-time lainnya, seperti berita. Alexa juga dapat mengontrol beberapa perangkat pintar menggunakan dirinya sebagai sistem otomatisasi rumah. Pengguna dapat memperluas kemampuan Alexa dengan menginstal "keterampilan" (fungsionalitas tambahan yang dikembangkan oleh vendor pihak ketiga, dalam pengaturan lain yang lebih umum disebut aplikasi seperti cuaca program dan fitur audio).²⁹

Kepentingan terbaik anak

Mengacu pada semua elemen yang diperlukan untuk membuat keputusan dalam situasi tertentu untuk anak individu atau kelompok anak tertentu.³⁰

Anak

Sesuai dengan pasal 1 Konvensi Hak-Hak Anak, seorang anak adalah siapa pun yang berusia di bawah 18 tahun, kecuali mayoritas diperoleh lebih awal di bawah hukum nasional.³¹

Eksplorasi dan pelecehan seksual terhadap anak (Child sexual exploitation and abuse / CSEA)

Mendeskripsikan semua bentuk eksploitasi seksual dan pelecehan seksual, misalnya "(a) bujukan atau paksaan seorang anak untuk terlibat dalam aktivitas seksual yang melanggar hukum; (b) penggunaan eksploitatif anak-anak dalam prostitusi atau praktik seksual melanggar hukum lainnya ; (c) penggunaan eksploitatif anak-anak dalam pertunjukan dan materi pornografi",³² serta "kontak seksual yang biasanya melibatkan kekerasan terhadap seseorang tanpa persetujuan".³³ Eksploitasi dan pelecehan seksual anak (CSEA) semakin banyak terjadi melalui Internet, atau dengan beberapa koneksi ke lingkungan online.

²⁹ UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014.

³⁰ Lihat Konvensi Perserikatan Bangsa-Bangsa tentang Hak-Hak Anak.

³¹ UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014.

³² Pasal 34 Konvensi Perserikatan Bangsa-Bangsa tentang Hak-Hak Anak.

³³ Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Luxembourg Guidelines), 2016.

Materi eksploitasi dan pelecehan seksual terhadap anak (Child sexual exploitation and abuse material / CSAM)

Evolusi cepat TIK telah menciptakan bentuk-bentuk baru CSEA online, yang dapat terjadi secara virtual dan tidak harus menyertakan pertemuan tatap muka fisik dengan anak.³⁴ Meskipun banyak yurisdiksi masih melabeli gambar dan video pelecehan seksual terhadap anak-anak "pornografi anak" atau "gambar tidak senonoh anak-anak", Pedoman ini merujuk pada masalah tersebut secara kolektif sebagai "materi pelecehan seksual anak" (CSAM). Istilah ini sesuai dengan Pedoman Komisi Broadband dan Model Respons Nasional³⁵ Dari Aliansi Global WePROTECT dan lebih akurat menjelaskan kontennya. Pornografi mengacu pada industri yang sah dan dikomersialkan, dan seperti yang dinyatakan oleh Pedoman Luksemburg, penggunaan istilah tersebut:

"dapat (secara tidak sengaja atau tidak) berkontribusi untuk mengurangi gravitasi, meremehkan, atau bahkan melegitimasi apa yang sebenarnya adalah pelecehan seksual dan/atau eksploitasi seksual terhadap anak-anak. Istilah 'pornografi anak' berisiko menyindir bahwa tindakan tersebut dilakukan dengan persetujuan anak dan mewakili materi seksual yang sah." Saat menggunakan istilah CSAM, kami merujuk pada materi yang mewakili tindakan yang melecehkan secara seksual dan/atau eksploitatif kepada seorang anak. Ini termasuk, namun tidak terbatas pada, materi yang merekam pelecehan seksual terhadap anak-anak oleh orang dewasa, gambar anak-anak yang termasuk dalam perilaku seksual eksplisit, dan organ seksual anak-anak ketika gambar diproduksi atau digunakan untuk tujuan seksual terutama.

Lihat [Pedoman Luksemburg](#) untuk istilah seperti "materi pelecehan seksual anak yang dihasilkan komputer atau digital".

Anak-anak dan remaja

Menjelaskan semua orang di bawah usia 18 tahun, di mana "anak-anak" (juga disebut sebagai "anak-anak yang lebih muda" dalam pedoman ITU ini) mencakup semua orang di bawah usia 15 tahun dan "orang muda" terdiri dari orang-orang dalam kelompok usia 15-18 tahun.

Mainan yang terhubung

Mainan yang terhubung terhubung ke Internet menggunakan teknologi seperti Wi-Fi dan Bluetooth, dan biasanya beroperasi bersama dengan aplikasi pendamping untuk memungkinkan permainan interaktif bagi anak-anak. Menurut Juniper Research, pada tahun 2015 pasar mainan yang terhubung mencapai USD 2,8 miliar dan diprediksi akan meningkat menjadi USD 11 miliar pada tahun 2020. Mainan ini mengumpulkan dan menyimpan informasi pribadi dari anak-anak termasuk nama, geolokasi, alamat, foto, rekaman audio dan video.³⁶

³⁴ Luxembourg Guidelines (seperti di atas), 2016 dan laporan UNICEF [Global Kids Online](#), 2019.

³⁵ Broadband Commission for Sustainable Development, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online", 2019; WePROTECT Global Alliance, "Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response", 2016.

³⁶ Jeremy Greenberg, "Dangerous Games: Connected Toys, COPPA, and Bad Security", Georgetown Law Technology Review, 2017.

Cyberbullying

Cyberbullying menggambarkan tindakan agresif yang sengaja dilakukan berulang kali oleh kelompok atau individu yang menggunakan teknologi digital dan menargetkan korban yang tidak dapat dengan mudah membela diri.³⁷ Biasanya melibatkan "menggunakan teknologi digital dan Internet untuk memposting informasi yang menyakitkan tentang seseorang, dengan sengaja berbagi informasi pribadi, foto atau video dengan cara yang menyakitkan, mengirim pesan yang mengancam atau menghina (melalui email, pesan instan, obrolan atau teks), menyebarkan rumor dan palsu informasi tentang korban atau dengan sengaja mengecualikan mereka dari komunikasi online".³⁸

Cyberhate, diskriminasi, dan ekstremisme kekerasan

"Cyberhate, diskriminasi, dan ekstremisme kekerasan adalah bentuk kekerasan dunia maya yang berbeda karena mereka menargetkan identitas kolektif, bukan individu, ... sering berkaitan dengan ras, orientasi seksual, agama, kebangsaan atau status imigrasi, jenis kelamin/jenis kelamin dan politik".³⁹

Kewarganegaraan digital

Kewarganegaraan digital mengacu pada kemampuan untuk terlibat secara positif, kritis dan kompeten dalam lingkungan digital, memanfaatkan keterampilan komunikasi dan penciptaan yang efektif, untuk mempraktikkan bentuk-bentuk partisipasi sosial yang menghormati hak asasi manusia dan martabat melalui penggunaan teknologi yang bertanggung jawab.⁴⁰

Literasi digital

Literasi digital berarti memiliki keterampilan yang dibutuhkan seseorang untuk hidup, belajar, dan bekerja dalam masyarakat di mana komunikasi dan akses ke informasi semakin meningkat melalui teknologi digital seperti platform Internet, media sosial, dan perangkat seluler.⁴¹ Ini mencakup komunikasi yang jelas, keterampilan teknis dan pemikiran kritis.

Ketahanan digital

Istilah ini menggambarkan kapasitas anak untuk mengatasi secara emosional dengan bahaya yang dihadapi secara online. Ini juga mengacu pada kecerdasan emosional yang diperlukan untuk memahami ketika seorang anak berisiko online, tahu bagaimana mencari bantuan, belajar dari pengalaman dan pulih ketika segala sesuatunya berjalan salah.⁴²

³⁷ Anna Costanza Baldry et al. "Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities", *Children and Youth Services Review*, 2019.

³⁸ The Luxembourg Guidelines, 2016 and the UNICEF Global Kids Online report, 2019 (as above).

³⁹ UNICEF *Global Kids Online report*, 2019 (as above).

⁴⁰ Council of Europe, "Digital Citizenship and Digital Citizenship Education".

⁴¹ Western Sydney University, "What is digital literacy?".

⁴² Dr. Andrew K. Przybylski, et al., "A Shared Responsibility: Building children's' online resilience", *Virgin Media and Parent Zone*, 2014

Pemegang kuasa

Menjelaskan semua orang yang memegang posisi dalam manajemen sekolah atau struktur tata kelola.

Grooming/online grooming

Grooming/online grooming, sebagaimana didefinisikan dalam Pedoman Luksemburg, mengacu pada "proses membangun/membangun hubungan dengan seorang anak baik secara langsung atau melalui penggunaan Internet atau teknologi digital lainnya untuk memfasilitasi kontak seksual *online* atau *offline* dengan orang tersebut". Ini adalah kegiatan kriminal berteman dengan seorang anak ..., untuk mencoba membujuk anak untuk melakukan hubungan seksual.

Teknologi informasi dan komunikasi (TIK)

Teknologi informasi dan komunikasi (TIK) menggambarkan semua teknologi informasi yang menekankan aspek komunikasi. Ini termasuk semua layanan dan perangkat yang menghubungkan Internet seperti komputer, laptop, tablet, smartpone, konsol game, dan jam tangan pintar. ⁴³ Ini juga mencakup layanan seperti radio dan televisi serta broadband, perangkat keras jaringan dan sistem satelit.

Game online

Game online didefinisikan sebagai memainkan semua jenis game digital komersial tunggal atau multipemain melalui perangkat apa pun yang terhubung ke Internet, termasuk konsol khusus, komputer desktop, laptop, tablet dan ponsel. "Ekosistem game online" didefinisikan termasuk menonton orang lain bermain video game melalui platform e-sports, streaming, atau berbagi video, yang biasanya memberikan opsi bagi pemirsa untuk mengomentari atau berinteraksi dengan pemain dan anggota audiens lainnya. ⁴⁴

Alat kontrol orang tua

Perangkat lunak yang memungkinkan pengguna, biasanya orang tua, untuk mengontrol beberapa atau semua fungsi komputer atau perangkat lain yang dapat terhubung ke Internet. Biasanya, program tersebut dapat membatasi akses ke jenis atau kelas situs web atau layanan online tertentu. Beberapa juga menyediakan ruang lingkup untuk manajemen waktu, yaitu perangkat dapat diatur untuk memiliki akses ke Internet hanya antara jam-jam tertentu. Versi yang lebih canggih dapat merekam semua teks yang dikirim atau diterima dari perangkat. Program biasanya akan dilindungi kata sandi. ⁴⁵

⁴³ UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014 (as above).

⁴⁴ UNICEF, "Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry", 2019.

⁴⁵ UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014 (seperti di atas).

Informasi pribadi

Istilah ini menjelaskan informasi yang dapat diidentifikasi secara individual mengenai seseorang, yang dikumpulkan secara online. Ini termasuk nama lengkap, detail kontak, seperti alamat rumah dan email, dan nomor telepon, dan sidik jari atau materi pengenalan wajah, nomor asuransi, atau faktor lainnya yang memungkinkan kontak fisik atau online atau lokalisasi seseorang. Dalam konteks ini, ini lebih lanjut mengacu pada informasi apa pun tentang seorang anak dan rombongannya yang dikumpulkan secara online oleh penyedia layanan secara online, termasuk mainan yang terhubung dan Internet of things, dan teknologi terhubung lainnya .

Privasi

Privasi sering diukur dalam hal berbagi informasi pribadi secara online, memiliki profil media sosial publik, berbagi informasi dengan orang-orang yang bertemu secara online, menggunakan pengaturan privasi, berbagi kata sandi dengan teman, dan kekhawatiran tentang privasi.⁴⁶

Media pelayanan publik

Ini adalah lembaga penyiaran nasional atau media yang telah menerima lisensi transmisi mereka berdasarkan serangkaian kewajiban kontraktual dengan negara bagian atau parlemen. Kewajiban ini telah diperpanjang di banyak negara dalam beberapa tahun terakhir untuk mengatasi konsekuensi transformasi digital melalui program literasi media dan digital serta kewajiban untuk mengatasi kesenjangan digital.

Sexting

Sexting umumnya didefinisikan sebagai pengiriman, penerimaan, atau pertukaran konten seksual yang diproduksi sendiri termasuk gambar, pesan, atau video melalui ponsel dan/atau Internet.⁴⁷ Penciptaan, distribusi, dan kepemilikan gambar seksual anak-anak adalah ilegal di sebagian besar negara. Jika gambar seksual anak-anak yang diproduksi sendiri diungkapkan, orang dewasa tidak boleh melihatnya. Berbagi gambar seksual oleh orang dewasa dengan anak selalu merupakan tindakan kriminal, yang dapat berbahaya dan mungkin perlu untuk melaporkan gambar tersebut dan menghapusnya.

Sextortion atau pemerasan seksual terhadap anak-anak

Sextortion adalah "pemerasan seseorang dengan bantuan gambar yang dihasilkan sendiri dari orang tersebut untuk memeras bantuan seksual, uang, atau manfaat lain darinya di bawah ancaman berbagi materi di luar persetujuan orang yang digambarkan (misalnya memposting gambar pada media sosial)".⁴⁸

⁴⁶ US Federal Trade Commission, "[Children's Online Privacy Protection Act](#)", 1998.

⁴⁷ The Luxembourg Guidelines, 2016 (seperti di atas).

⁴⁸ The Luxembourg Guidelines, 2016 (seperti di atas).

Internet of Things

"Internet of Things (IoT) mewakili langkah selanjutnya menuju digitalisasi masyarakat dan ekonomi kita, di mana objek dan orang saling berhubungan melalui jaringan komunikasi dan laporan tentang status mereka dan/atau lingkungan sekitarnya." ⁴⁹

URL

Singkatan ini adalah singkatan dari "uniform resource locator", alamat halaman Internet. ⁵⁰

Realitas virtual

" Realitas virtual adalah penggunaan teknologi komputer untuk menciptakan efek dunia tiga dimensi interaktif di mana objek memiliki rasa kehadiran spasial." ⁵¹

Wi-Fi

Wi-Fi (Wireless Fidelity) adalah kelompok standar teknis yang memungkinkan transmisi data melalui jaringan nirkabel. ⁵²

⁴⁹ European Commission, "Policy: The Internet of Things".

⁵⁰ UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014 (seperti di atas).

⁵¹ NASA, "Virtual Reality: Definition and Requirements".

⁵² US Federal Trade Commission, "Children's Online Privacy Protection Act", 1998

