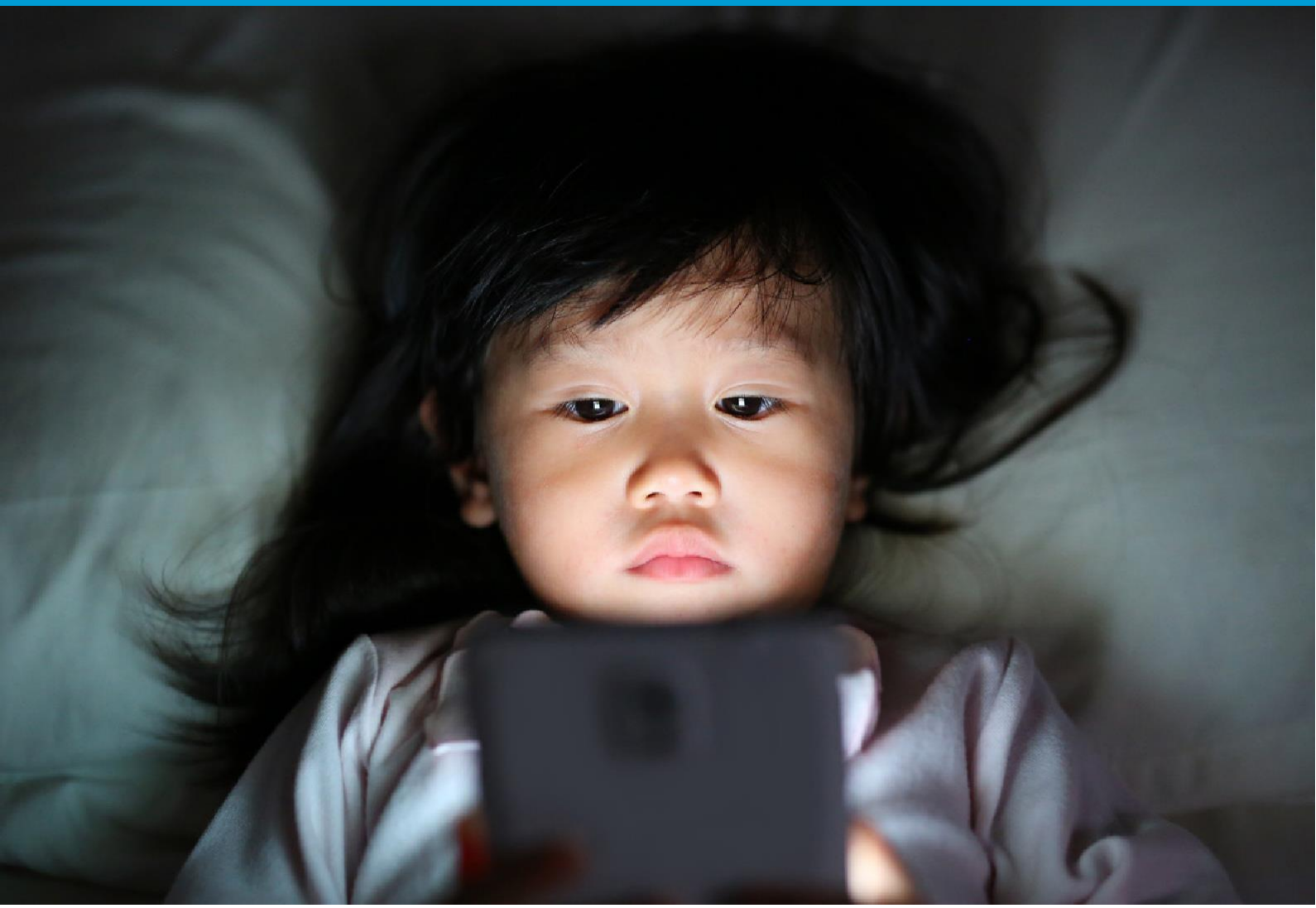
Pedoman untuk pembuat kebijakan tentang Pedoman Perlindungan Online Anak

2020



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

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

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 menyasar 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 ekses 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 lnformatika 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, berkreatifitas, 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, menggerakan tenaga pendidik dan mengkapasitasi orang tua dalam mencari formula terbaiknya dalam melindungi anak saat online. Ditengah kekhawatiran orang tua, masyarakat, aparatur negara 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 Telecomunication 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 pembuat kebijakan tentang Pedoman Perlindungan Online Anak

2020

Prakata

Tiga puluh tahun yang lalu, hampir semua pemerintah berjanji untuk menghormati, melindungi dan mempromosikan hak-hak anak. Konvensi PBB tentang Hak Anak (*Convention on the Rights of the Child* at0061u CRC) adalah perjanjian hak asasi manusia internasional yang paling banyak diratifikasi sepanjang sejarah. Meskipun telah mencapai kemajuan penting dalam tiga dekade terakhir, masih terdapat tantangan yang signifikan dan munculnya berbagai area risiko baru bagi anak-anak.

Pada tahun 2015, semua negara memperbarui komitmen mereka terhadap anak-anak pada agenda 2030 dan Tujuan Pembangunan Berkelanjutan (TPB) 17 universal. Sebagai contoh, Tujuan 16.2 menyerukan pengakhiran pelecehan, eksploitasi dan segala bentuk kekerasan dan penyiksaan terhadap anak-anak pada tahun 2030. Tetapi perlindungan anak-anak menjadi benang merah pada 11 dari 17 TPB. UNICEF menjadikan anak-anak sebagai pusat agenda 2030 seperti yang digambarkan pada Gambar 1.

Gambar 1: Anak-anak, TIK, dan TPB

Peran sentral anak-anak dalam

Agenda 2030 untuk Pembangunan Berkelanjutan mengakui bahwa TIK dapat menjadi pendorong utama untuk mencapai TPB. Penyebaran teknologi informasi dan komunikasi (TIK) dan keterkaitan secara global berpotensi untuk mempercepat kemajuan manusia, menjembatani kesenjangan digital dan mengembangkan masyarakat berpengetahuan (*knowledge societies*). Agenda 2030 lebih lanjut mendefinisikan target spesifik untuk penggunaan TIK untuk pembangunan berkelanjutan dalam pendidikan (Tujuan 4), kesetaraan gender (Tujuan 5), infrastruktur (Tujuan 9 – akses universal dan terjangkau ke Internet) dan Tujuan 17 – kemitraan dan sarana implementasi[1]. TIK memiliki kekuatan untuk mengubah perekonomian secara mendalam dan keseluruhan dengan menjadi kekuatan pendorong dalam mencapai masing-masing dari 17 TPB. TIK telah bergerak dengan memberdayakan miliaran orang di seluruh dunia – dengan menyediakan akses ke sumber daya pendidikan dan perawatan kesehatan, dan layanan-layanan seperti e-government dan media sosial.

[1] UNDP, Sustainable Development Goals | UNDP, undp.org, diakses pada 29 Januari 2020, https://www.undp.org/content/undp/en/home/sustainable-development-goals.html; Houlin Zhao, "Why ICTs Are so Crucial to Achieving the SDGs," *ITU*, ITU News Magazines, 48, diakses pada 29 Januari 2020, https://www.itu.int/en/itunews/Documents/2017/2017-03/2017_ITUNews03-en.pdf.

Ledakan teknologi informasi dan komunikasi telah menciptakan peluang yang belum pernah terjadi sebelumnya bagi anak-anak dan remaja untuk berkomunikasi, terhubung, berbagi, belajar, mengakses informasi dan mengekspresikan pendapat mereka tentang hal-hal yang mempengaruhi kehidupan mereka dan komunitas mereka.

Tetapi akses yang lebih luas dan lebih mudah ke Internet dan teknologi seluler juga menimbulkan tantangan signifikan bagi keselamatan dan kesejahteraan anak-anak – baik secara online maupun offline.

Untuk mengurangi risiko dunia digital sembari memungkinkan lebih banyak anak dan remaja untuk memetik manfaatnya, pemerintah, masyarakat sipil, komunitas lokal, organisasi internasional, dan industri harus bersatu dalam tujuan yang sama. Pembuat kebijakan khususnya diperlukan untuk mencapai tujuan internasional untuk menjaga anak-anak tetap aman saat online.

Untuk menjawab tantangan yang ditimbulkan oleh pesatnya perkembangan TIK dan tantangan perlindungan anak yang menyertainya, Child Online Protection (COP) Initiative diluncurkan sebagai inisiatif internasional *multi-stakeholder* oleh International Telecommunication Union (ITU) pada November 2008. Inisiatif ini bertujuan untuk menyatukan mitra dari semua sektor komunitas global untuk menciptakan pengalaman online yang aman dan memberdayakan bagi anak-anak di seluruh dunia.

Selain itu, Plenipotentiary Conference of the International Telecommunication Union yang diadakan di Dubai pada tahun 2018 menegaskan kembali pentingnya Inisiatif COP dengan mengakuinya sebagai wadah untuk meningkatkan kesadaran, berbagi praktik terbaik, dan untuk memberikan bantuan dan dukungan kepada Negara-negara Anggota, terutama negara-negara berkembang, dalam mengembangkan dan mengimplementasikan peta jalan COP. Konferensi ini juga mengakui pentingnya perlindungan online anak dalam kerangka Konvensi PBB tentang Hak Anak dan perjanjian hak asasi manusia lainnya dengan mendorong kolaborasi di antara semua pemangku kepentingan yang terlibat dalam perlindungan online anak.

Konferensi ini mengakui Agenda 2030 untuk Pembangunan Berkelanjutan, menangani berbagai aspek perlindungan online anak dalam Tujuan Pembangunan Berkelanjutan (TPB), khususnya TPB 1, 3, 4, 5, 9, 10 dan 16; konferensi lebih jauh mengakui Resolusi 175 (Rev. Dubai, 2018), tentang aksesibilitas bagi penyandang disabilitas dan penyandang kebutuhan khusus terhadap teknologi telekomunikasi/informasi dan komunikasi (TIK) dan Resolusi 67 (Rev. Buenos Aires, 2017) dari World Telecommunication Development Conference (WTDC), tentang peran ITU Telecommunication Development Sector (ITU-D) dalam perlindungan online anak.

Di akhir 2019, ITU/UNESCO Broadband Commission for Sustainable Development meluncurkan Laporan Keamanan Online Anak dengan rekomendasi yang dapat ditindaklanjuti tentang cara membuat Internet lebih aman untuk anak-anak.

Pada tahun 2009, pedoman pertama tentang perlindungan online anak diterbitkan oleh ITU dalam konteks Inisiatif COP. Selama dekade terakhir, Pedoman COP telah diterjemahkan ke dalam banyak bahasa dan telah digunakan oleh banyak negara di seluruh dunia sebagai titik referensi untuk peta jalan dan strategi nasional terkait perlindungan online anak. Pedoman COP telah membantu entitas pemerintah nasional, organisasi masyarakat sipil, lembaga pengasuhan anak, industri, dan banyak pemangku kepentingan lainnya dalam upaya perlindungan online anak mereka.

Lebih khusus lagi, pedoman tersebut telah digunakan untuk rancangan, pengembangan dan implementasi strategi nasional perlindungan online anak di banyak Negara Anggota seperti Kamerun, Gabon, Gambia, Ghana Kenya, Sierra Leona, Uganda, dan Zambia di kawasan Afrika; Bahrain dan Oman di kawasan Arab; Brunei, Kamboja Kiribati, Indonesia, Malaysia, Myanmar dan Vanuatu di kawasan Asia Pasifik; dan Bosnia, Georgia, Moldova, Montenegro, Polandia dan Ukraina di kawasan Eropa.

Lebih lanjut, pedoman tersebut telah membangun fondasi untuk acara-acara kawasan seperti Regional Conference on Child Online Protection (ACOP): Empowering the Future Digital citizens, di Kampala, Uganda (2014), dan ASEAN Regional Conference on Child Online Protection yang diadakan di Bangkok, Thailand (2020).

Menurut Resolusi 179 (Rev. Dubai, 2018), ITU bekerja sama dengan mitra inisiatif COP dan pemangku kepentingan telah diarahkan untuk memperbarui empat set pedoman dengan mempertimbangkan perkembangan teknologi di industri telekomunikasi, termasuk pedoman tentang anak-anak penyandang disabilitas dan anak-anak dengan kebutuhan khusus.

Melalui proses ini, pedoman ini telah diperbarui dan ditinjau secara signifikan oleh para ahli dan pemangku kepentingan terkait, menetapkan serangkaian rekomendasi untuk menjaga anak-anak tetap aman di dunia digital. Pedoman ini adalah hasil dari upaya kolaboratif *multi-stakeholder*, dengan memanfaatkan pengetahuan, pengalaman dan keahlian dari banyak organisasi dan individu dari seluruh dunia di bidang perlindungan online anak. Pedoman ini bertujuan untuk membangun fondasi bagi dunia maya yang aman dan terjamin untuk generasi mendatang. Pedoman dimaksudkan untuk menjadi cetak biru yang dapat diadaptasi dan digunakan dengan cara yang sesuai dengan adat dan hukum nasional atau lokal. Selain itu, pedoman ini membahas masalah yang mempengaruhi semua anak dan remaja di bawah usia 18 tahun, dengan mengenali kebutuhan dari setiap kelompok usia yang beragam. Lebih jauh lagi, pedoman ini bertujuan untuk memenuhi kebutuhan anak-anak dengan berbagai kondisi kehidupan yang beragam dan anak-anak dengan kebutuhan khusus dan anak-anak penyandang disabilitas. Pedoman ini juga memperkuat cakupan perlindungan online anak, mengatasi semua risiko, ancaman, dan bahaya yang mungkin dihadapi anak-anak secara online dan dengan hati-hati menyeimbangkannya dengan manfaat yang dapat diberikan oleh dunia digital bagi kehidupan anak-anak.

Pedoman ini diharapkan tidak hanya akan mengarah pada pembangunan masyarakat informasi yang lebih inklusif, tetapi juga memungkinkan Negara-negara Anggota ITU untuk memenuhi kewajiban mereka dalam melindungi dan mewujudkan hak-hak anak sebagaimana tercantum dalam Konvensi PBB tentang Hak Anak[2] yang diadopsi melalui resolusi Majelis Umum PBB 44/25 tanggal 20 November 1989 dan *Outcome Document* dari World Outcome Document dari World Summit on Information Society3 (WSIS)[3].

Melalui penerbitan pedoman ini, inisiatif COP menyerukan kepada semua pemangku kepentingan untuk menerapkan kebijakan dan strategi yang akan melindungi anak-anak di dunia maya dan mendorong akses mereka yang lebih aman terhadap semua peluang luar biasa yang dapat disediakan oleh sumber daya online.

[2] UNICEF, "Convention on the Rights of the Child," uncief.org, diakses pada 29 Januari 2020, https://www.unicef.org/child-rights-convention.

[3] WSIS diadakan dalam dua tahap: di Jenewa (10-12 Desember 2003) dan di Tunis (16-18 November 2005). Kesepakatan WSIS adalah komitmen tegas "untuk membangun masyarakat informasi yang berpusat pada manusia, inklusif dan berorientasi pada pembangunan, di mana setiap orang dapat membuat, mengakses, memanfaatkan, dan berbagi informasi dan pengetahuan."

Daftar Isi

Daftar tabel, gambar dan kotak

Tabel

Gambar

Kotak

1. Gambaran Umum

1.1 Tujuan

Pemerintah nasional memiliki kewajiban untuk memberikan perlindungan terhadap anak, baik di dunia fisik maupun dunia maya. Dalam arti penting, mengingat teknologi baru saat ini telah terintegrasi secara menyeluruh ke dalam aspek penting kehidupan banyak anak dan remaja, tidak masuk akal lagi jika kita mencoba mempertahankan perbedaan rigid antara kejadian di dunia nyata dan di dunia maya. Keduanya semakin terjalin dan saling bergantung.

Pembuat kebijakan[1] dan semua pemangku kepentingan terkait lainnya memiliki peran yang sangat penting. Kecepatan perkembangan teknologi berarti bahwa banyak metode pembuatan kebijakan tradisional tidak lagi cocok digunakan untuk mencapai tujuan ini. Pembuat kebijakan diharuskan untuk menguraikan kerangka hukum yang adaptif, inklusif, dan sesuai dengan tujuan untuk menghadapi era digital yang berubah cepat untuk melindungi anak-anak secara online.

Tujuan dari pedoman ini adalah untuk menawarkan kepada para pembuat kebijakan di Negara-negara Anggota ITU suatu kerangka kerja yang mudah digunakan dan fleksibel untuk memahami dan bertindak atas dasar kewajiban hukum mereka untuk menyediakan perlindungan anak-anak, baik di dunia nyata, fisik maupun virtual.

Hal ini dilakukan dengan menjawab beberapa pertanyaan penting bagi pembuat kebijakan:

1) Apa itu perlindungan online anak?
2) Mengapa saya sebagai pembuat kebijakan perlu memperhatikan perlindungan online anak?
3) Bagaimana konteks hukum, sosial-politik, dan pembangunan di negara saya?
4) Bagaimana seharusnya pembuat kebijakan mulai mempertimbangkan dan membentuk kebijakan perlindungan online anak yang efektif dan berkelanjutan di negaranya?

Untuk itu, pedoman ini menggunakan model, kerangka kerja, dan sumber daya yang ada untuk menawarkan konteks dan wawasan tentang praktik yang baik dari seluruh dunia.

1.2 Ruang Lingkup

Cakupan perlindungan online anak mencakup segala bahaya yang dialami anak-anak secara online, yang mencakup berbagai risiko yang mengancam keselamatan dan kesejahteraan anak-anak. Ini adalah tantangan kompleks yang harus menggunakan pendekatan dari berbagai sudut, seperti undang-undang, pemerintahan, pendidikan, kebijakan dan masyarakat.

Selain itu, perlindungan online anak harus didasarkan pada pemahaman tentang risiko, ancaman, dan bahaya umum dan khusus negara yang dihadapi anak-anak di lingkungan digital. Hal ini membutuhkan definisi yang jelas dan penetapan parameter yang jelas untuk intervensi yang mencakup dan membedakan antara tindakan yang merupakan kejahatan dan tindakan yang meskipun tidak ilegal, namun merupakan ancaman bagi kesejahteraan anak.

Untuk tujuan ini, pedoman ini memberikan gambaran tentang ancaman dan bahaya saat ini yang dihadapi anak-anak di lingkungan digital. Namun demikian, cepatnya perkembangan teknologi serta ancaman dan bahaya terkait berarti bahwa kecepatan dan metode tradisional yang digunakan pembuatan kebijakan tidak lagi dapat mengimbanginya.

[1] Istilah 'pembuat kebijakan' mengacu pada semua pemangku kepentingan yang bertanggung jawab untuk mengembangkan dan mengimplementasikan kebijakan, terutama mereka yang berada di dalam pemerintahan.

Pembuat kebijakan di era digital perlu membangun kerangka hukum dan kebijakan yang cukup adaptif dan inklusif untuk mengatasi tantangan yang ada dan sebisa mungkin mengantisipasi tantangan yang akan datang. Untuk melakukan hal ini dibutuhkan kolaborasi dengan setiap pemangku kepentingan, termasuk industri TIK, komunitas peneliti, masyarakat sipil, publik, dan anak-anak itu sendiri. Proses ini dapat didasarkan oleh pertimbangan prinsip-prinsip menyeluruh dalam perlindungan online anak.

1.3 Prinsip-prinsip menyeluruh

Sebelas prinsip lintas sektoral yang ditetapkan di sini, yang digabungkan, akan membantu dalam mengembangkan strategi nasional perlindungan online anak yang berwawasan ke depan dan holistik.

Urutan prinsip-prinsip ini mencerminkan narasi logis, bukan urutan mana yang paling penting.

Strategi nasional perlindungan online anak harus:

1. didasarkan pada visi holistik yang menggabungkan pemerintah, industri, dan masyarakat;
2. dihasilkan dari pemahaman dan analisis menyeluruh tentang lingkungan digital secara keseluruhan, namun disesuaikan dengan keadaan dan prioritas negara;
3. menghormati dan konsisten dengan hak-hak dasar anak-anak sebagaimana diabadikan dalam Konvensi PBB tentang Hak Anak dan konvensi dan hukum internasional penting lainnya;
4. menghormati dan konsisten dengan undang-undang dan strategi domestik yang ada, yang serupa dan yang terkait, seperti undang-undang pelecehan anak atau strategi keselamatan anak;
5. menghormati hak-hak sipil dan kebebasan anak, yang tidak boleh dikorbankan demi perlindungan;
6. dikembangkan dengan partisipasi aktif dari semua pemangku kepentingan terkait, termasuk anak-anak, menangani kebutuhan dan tanggung jawab mereka dan memenuhi kebutuhan kelompok minoritas dan kelompok yang terpinggirkan;
7. dirancang agar selaras dengan rencana pemerintah yang lebih luas untuk kemakmuran ekonomi dan sosial dan memaksimalkan kontribusi TIK untuk pembangunan berkelanjutan dan inklusi sosial;
8. memanfaatkan instrumen kebijakan yang paling tepat yang ada untuk mewujudkan tujuannya, dengan mempertimbangkan keadaan khusus masing-masing negara;
9. ditetapkan pada tingkat pemerintahan tertinggi, yang akan bertanggung jawab untuk menetapkan peran dan tanggung jawab terkait dan mengalokasikan sumber daya manusia dan keuangan yang memadai;
10. membantu membangun lingkungan digital yang dapat dipercaya oleh anak-anak, orang tua/pengasuh, dan pemangku kepentingan;
11. memandu upaya para pemangku kepentingan untuk memberdayakan dan mendidik anak-anak tentang literasi digital untuk melindungi diri mereka sendiri di dunia maya.

1.4 Penggunaan pedoman ini

Pedoman ini mempertimbangkan penelitian yang relevan, model dan materi yang ada, dan menetapkan rekomendasi yang jelas untuk pengembangan strategi nasional perlindungan online anak.

- Bagian 2 memperkenalkan perlindungan online anak dan memberikan wawasan tentang penelitian terbaru, termasuk aspek-aspek mengenai teknologi baru yang muncul, ancaman utama, dan bahaya bagi anak-anak.

- Bagian 3 menetapkan bagaimana cara menyusun strategi nasional perlindungan online anak, termasuk pemangku kepentingan yang relevan, contoh tanggapan yang ada terhadap ancaman online dan kerugian serta manfaat dari adanya strategi nasional.
- Bagian 4 mencakup rekomendasi untuk kerangka kerja dan implementasi.
- Bagian 5 menguraikan ceklis nasional untuk mengembangkan strategi nasional perlindungan online anak.
- Bagian 6 menyajikan bahan referensi yang berguna.

2. Pengantar

Pada tahun 2019, lebih dari setengah populasi dunia menggunakan Internet. Kelompok pengguna terbesarnya adalah mereka yang berusia di bawah 44 tahun, dengan tingkat penggunaan yang sama tingginya antara kelompok usia 16 hingga 24 tahun dan kelompok usia 35 hingga 44 tahun. Di tingkat global, satu dari tiga anak menggunakan Internet (0-18 tahun)[2]. Di negara berkembang, anak-anak dan remaja merupakan kelompok usia terbesar pengguna Internet[3], dan diperkirakan bahwa selama lima tahun ke depan, jumlah populasi ini akan lebih dari dua kali lipat. Generasi baru tumbuh dengan Internet dan sebagian besar terhubung dengan teknologi jaringan seluler, terutama di belahan bumi selatan[4].

Meskipun akses Internet merupakan hal mendasar bagi perwujudan hak-hak anak, masih terdapat kesenjangan akses di tingkat regional, nasional, gender dan lainnya yang membatasi kesempatan bagi anak perempuan, anak-anak penyandang disabilitas, anak-anak dari kelompok minoritas dan kelompok rentan lainnya. Dalam hal kesenjangan gender dalam dunia digital, penelitian menunjukkan bahwa di setiap wilayah kecuali Amerika Serikat, jumlah pengguna Internet pria sebagian besar di atas jumlah pengguna wanita. Di banyak negara, anak perempuan tidak memiliki kesempatan akses yang sama dengan anak laki-laki, dan jika mereka memiliki kesempatan tersebut, penggunaan internet yang dilakukan anak perempuan tidak hanya jauh lebih dipantau dan dibatasi, tetapi mereka juga mungkin menghadapi risiko keamanan dalam mengakses internet[5]. Jelas bahwa anak-anak dan remaja yang tidak memiliki keterampilan digital atau berbicara bahasa minoritas tidak dapat dengan mudah menemukan konten yang relevan secara online, dan bahwa anak-anak dari daerah pedesaan memiliki keterampilan digital yang lebih rendah, menghabiskan lebih banyak waktu di dunia maya (terutama untuk bermain game), dan menerima lebih sedikit mediasi dan pemantauan dari orang tua[6].

---

2 OECD, "New Technologies and 21st Century Children: Recent Trends and Outcomes," OECD Education Working Paper No. 179 (Directorate for Educationand Skills, OECD), diakses pada 27 Januari 2020, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282018%2915&docLanguage=En.

3 Ofcom, "Children and Parents: Media Use and Attitudes Report 2018" (Ofcom), diakses pada 17 Januari 2020, https://www.ofcom.org.uk/ _data/assets/pdf_file/0024/134907/children-and-parents-media-use-and -attitudes-2018.pdf.

4 ITU, "Measuring the Information Society Report," diakses pada 16 Januari 2020, https://www.itu.int/dms_pub/ itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf.

5 "Young Adolescents and Digital Media: Uses, Risks and Opportunities in Low-and Middle-Income Countries,"GAGE, diakses pada 29 Januari 2020,https://www.gage.odi.org/publication/digital-media-risks-opportunities/.

6 Livingstone, S., Kardefelt Winther, D., dan 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. Ini dapat menimbulkan hasil yang tidak terduga, misalnya, penelitian yang dilakukan oleh HABLATAM di lima negara Amerika Latin menunjukkan bahwa di komunitas rentan, anak-anak mungkin menggunakan platform kencan, videogame, dan jejaring sosial untuk melakukan transaksi uang untuk tujuan ilegal. Contectados al Sur network, "Hablatam," Hablatam Project 2020, diakses pada 6 Februari 2020, https://hablatam.net/.

Namun, tidak akan ada pembahasan tentang risiko dan ancaman tanpa kita mengakui sifat teknologi digital yang sangat memperkaya dan memberdayakan. Internet dan teknologi digital mengubah cara kita hidup dan telah membuka banyak cara baru untuk berkomunikasi, bermain game, menikmati musik, dan terlibat dalam beragam aktivitas budaya, pendidikan, dan peningkatan keterampilan. Internet dapat memberikan akses penting ke layanan kesehatan dan pendidikan serta informasi tentang topik yang penting bagi kaum muda yang mungkin tabu di masyarakat mereka.

Mengingat anak-anak dan remaja seringkali yang paling duluan dalam mengadopsi dan beradaptasi dengan berbagai posibilitas baru yang ditawarkan oleh Internet, mereka juga dihadapkan pada berbagai masalah terkait keselamatan dan kesejahteraan yang harus diakui dan dihadapi oleh masyarakat. Sangat penting untuk mendiskusikan secara terbuka risiko yang ada untuk anak-anak dan remaja di dunia maya. Diskusi akan membuka sebuah wadah agar anak-anak dan remaja dapat diajari bagaimana cara mengenali risiko, dan mencegah atau menangani bahaya jika itu terjadi, serta keuntungan dan peluang yang dapat ditawarkan oleh Internet.

Di berbagai belahan dunia, anak muda memiliki pemahaman yang baik tentang beberapa risiko yang mereka hadapi di dunia maya.[7,8] Penelitian menunjukkan, misalnya, bahwa mayoritas anak-anak dan remaja mampu membedakan perundungan di dunia maya dari sekadar bercanda atau menggoda secara online. Mereka menyadari bahwa perundungan di dunia maya memiliki dimensi publik dan dirancang untuk menyakiti, namun menyeimbangkan peluang dan risiko anak di dunia maya masih menjadi tantangan tersendiri[9].

Bagi Negara Anggota ITU, melindungi anak-anak dan remaja di dunia maya terus menjadi prioritas, yang harus secara hati-hati diimbangi dengan upaya untuk mempromosikan peluang yang ditawarkan di dunia maya bagi anak-anak dan remaja[10], dan itu harus dilakukan dengan cara yang melindungi anak-anak dan remaja tanpa mempengaruhi akses mereka atau akses publik yang lebih luas terhadap informasi, atau kemampuan untuk menikmati kebebasan berbicara, berekspresi dan berserikat.

Dibutuhkan investasi khusus dan solusi kreatif untuk mengatasi risiko yang dihadapi oleh anak-anak dan remaja, paling tidak karena kesenjangan digital antara anak-anak dan orang dewasa yang membatasi bimbingan dari orang tua, guru, dan wali. Pada saat yang sama, ketika anak-anak dan remaja tumbuh dan menjadi dewasa, orang tua dan anggota masyarakat yang aktif, terdapat peluang potensial dan tidak dapat dilewatkan bagi mereka untuk mengurangi kesenjangan digital.

Mengingat hal ini, membangun kepercayaan di Internet harus menjadi yang utama dan menjadi pusat kebijakan publik. Pemerintah dan masyarakat perlu bekerja dengan anak-anak dan remaja untuk memahami perspektif mereka dan memantik debat publik tentang risiko dan peluang. Mendukung anak-anak dan remaja untuk mengelola risiko online dapat menjadi langkah yang efektif, tetapi pemerintah juga harus memastikan adanya layanan dukungan yang memadai bagi mereka yang mengalami bahaya atau kerugian di dunia maya, dan bahwa anak-anak mengetahui cara mengakses layanan tersebut.

---

7 Sejak 2016, ITU melakukan konsultasi dalam COP dengan pemangku kepentingan dari kalangan anak-anak dan dewasa tentang isu-isu yang relevan seperti perundungan di dunia maya, literasi digital dan aktivitas online anak-anak.

8 ITU, Youth Consultation, https://www.itu.int/en/council/cwg-cop/Pages/meetings.aspx.

9 UNICEF, "Global Kids Online Comparative Report (2019)."

10 ITU, "Celebrating 10 Years of Child Online Protection", ITU News, 6 Februari 2018, https://news.itu.int/celebrating-10-years-child-online-protection/.

Beberapa negara berupaya keras untuk mengalokasikan sumber daya yang cukup untuk mengatasi literasi digital dan keamanan anak-anak saat online. Namun, anak-anak melaporkan bahwa orang tua, guru, perusahaan teknologi, dan pemerintah adalah pemain penting dalam mengembangkan solusi untuk mendukung keamanan online mereka. Negara-negara Anggota ITU juga telah menunjukkan bahwa adanya dukungan yang signifikan untuk peningkatan berbagi pengetahuan dan upaya terkoordinasi untuk menjamin keselamatan lebih banyak anak di dunia maya[9].

Anak-anak dan remaja menavigasi lanskap digital yang semakin kompleks dan adopsi kecerdasan buatan untuk *machine learning*, *big data analytics*, robotika, *virtual reality* dan *augmented reality*, dan *Internet of Things* akan mengubah praktik media anak-anak. Ini membutuhkan pembuatan kebijakan dan investasi untuk anak-anak, orang tua, dan masyarakat di masa depan seperti halnya untuk hari ini.

2.1 Apa itu perlindungan online anak?

Teknologi online menghadirkan banyak kemungkinan bagi anak-anak dan remaja untuk berkomunikasi, mempelajari keterampilan baru, mewujudkan kreativitas, dan berkontribusi untuk menciptakan masyarakat yang lebih baik. Tetapi teknologi online juga dapat menghadirkan berbagai risiko baru, seperti membuat mereka terpapar dengan masalah privasi, konten ilegal, pelecehan, perundungan di dunia maya, penyalahgunaan data pribadi atau *grooming* untuk tujuan seksual dan bahkan pelecehan seksual anak.

Pedoman ini mengembangkan pendekatan holistik untuk menanggapi semua potensi ancaman dan bahaya yang mungkin dihadapi anak-anak dan remaja ketika memperoleh literasi digital. Pedoman ini menyadari bahwa semua pemangku kepentingan terkait memiliki peran dalam ketahanan, kesejahteraan, dan perlindungan digital anak sembari memanfaatkan peluang yang dapat ditawarkan Internet.

Melindungi anak-anak dan remaja adalah tanggung jawab bersama kita dan semua pemangku kepentingan terkait memastikan masa depan yang berkelanjutan untuk semua orang. Agar hal ini tercapai, pembuat kebijakan, industri, orang tua, pengasuh, pendidik, dan pemangku kepentingan lainnya harus memastikan bahwa anak-anak dan remaja dapat memenuhi potensi mereka – baik secara online maupun offline.

Meskipun belum ada definisi universal untuk perlindungan online anak, pedoman ini bertujuan untuk 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 kemandirian dalam menghadapi ancaman;
- pencegahan bahaya;
- keseimbangan dinamis antara memastikan perlindungan dan memberikan kesempatan bagi anak untuk menjadi warga digital;
- menjunjung tinggi hak dan kewajiban anak dan masyarakat.

Selain itu, mengingat kemajuan pesat dalam teknologi dan masyarakat serta sifat Internet yang tanpa batas, perlindungan online anak harus gesit dan adaptif agar dapat efektif. Meskipun pedoman ini menawarkan wawasan tentang risiko online utama bagi anak-anak dan remaja, termasuk konten berbahaya dan ilegal, pelecehan, perundungan di dunia maya, penyalahgunaan data pribadi, atau *grooming* untuk tujuan seksual dan pelecehan dan eksploitasi seksual anak, tantangan baru akan muncul seiring dengan perkembangan inovasi teknologi dan biasanya akan bervariasi antara satu wilayah dengan wilayah lain. Namun, tantangan baru akan paling baik ditangani dengan bekerja sama sebagai sebuah komunitas global, karena solusi baru untuk menghadapi tantangan-tantangan ini perlu ditemukan.

2.2 Anak-anak dalam dunia digital

Internet telah mengubah cara kita hidup. Internet terintegrasi sepenuhnya ke dalam kehidupan anak-anak dan remaja, sehingga mustahil untuk memisahkan antara dunia digital dan dunia fisik. Sepertiga dari semua pengguna Internet saat ini adalah anak-anak dan remaja, dan UNICEF memperkirakan bahwa 71 persen remaja sudah beraktivitas secara online.

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

Adanya akses terhadap teknologi dan belajar untuk menggunakan dan menavigasi teknologi ini dipandang penting bagi perkembangan remaja dan pertama kali digunakan pada usia dini. Pembuat kebijakan harus memahami bahwa anak-anak dan remaja sering kali mulai menggunakan platform dan layanan ini sebelum mereka mencapai batas usia minimum, oleh karena itu, pendidikan harus dimulai sejak dini.

Anak-anak dan remaja ingin terlibat dalam percakapan, dan mereka memiliki keahlian berharga selaku '*digital natives*' yang dapat mereka bagikan. Pembuat kebijakan dan praktisi harus terlibat dengan anak-anak dan remaja dalam perdebatan yang sedang berlangsung tentang lingkungan online untuk mendukung hak-hak mereka.

Akses Internet

Pada tahun 2019, lebih dari setengah populasi dunia menggunakan Internet (53,6 persen), dengan diperkirakan terdapat 4,1 miliar pengguna. Di tingkat global, satu dari tiga pengguna Internet adalah anak-anak di bawah usia 18 tahun[1]. Di beberapa negara berpenghasilan rendah, angka ini meningkat menjadi sekitar satu dari dua, sedangkan di negara berpenghasilan tinggi, rasionya sekitar satu dari lima. Menurut UNICEF, di seluruh dunia, 71 persen anak muda sudah beraktivitas secara online[2]. Oleh karena itu, anak-anak dan remaja saat ini hadir secara substansial, permanen, dan terus-menerus di Internet[3]. Internet melayani tujuan sosial, ekonomi atau politik lainnya, dan telah menjadi produk atau layanan keluarga atau konsumen yang merupakan bagian yang tak terpisahkan dari bagaimana keluarga dan anak-anak dan remaja menjalani kehidupan mereka.

Pada tahun 2017, secara regional, akses internet anak dan remaja sangat terkait dengan tingkat pendapatan. Negara-negara berpenghasilan rendah cenderung memiliki lebih sedikit pengguna Internet anak-anak daripada negara-negara berpenghasilan tinggi.

Anak-anak dan remaja di sebagian besar negara menghabiskan lebih banyak waktu online di akhir pekan daripada di hari kerja, dimana remaja (15–17 tahun) menghabiskan waktu online paling lama, rata-rata antara 2,5 dan 5,3 jam, tergantung negaranya.

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 sekitar dua jam sehari online selama seminggu dan kira-kira dua kali lipatnya setiap hari di akhir pekan. Sebagian merasa terhubung secara permanen. Tetapi banyak yang masih tidak memiliki akses Internet di rumah.

---

[1] Livingstone, S., Carr, J., dan 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,* Oktober 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

[3] Livingstone, Carr, dan Byrne, "One in Three: Internet Governance and Children's Rights."

Dalam praktiknya, sebagian besar anak-anak dan remaja yang menggunakan Internet, mengaksesnya melalui lebih dari satu perangkat: Anak-anak dan remaja yang terhubung setidaknya setiap minggu terkadang menggunakan hingga tiga perangkat berbeda untuk melakukannya. Remaja dan anak-anak di negara-negara kaya umumnya menggunakan lebih banyak perangkat, dan anak laki-laki menggunakan agak lebih banyak perangkat daripada anak perempuan di setiap negara yang disurvei.

Aktivitas paling populer – baik untuk anak perempuan maupun laki-laki – adalah menonton klip video. Lebih dari tiga perempat anak-anak dan remaja yang menggunakan Internet mengatakan bahwa mereka menonton video online setidaknya setiap minggu, baik sendirian maupun bersama anggota keluarga lainnya. Banyak anak-anak dan remaja dapat dianggap sebagai 'pengguna media sosial aktif' dengan 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 partisipasi dalam game online secara keseluruhan bervariasi di setiap negara, kira-kira selaras dengan ketersediaan akses Internet bagi anak-anak dan remaja, sementara 10 hingga 30 persen anak-anak dan remaja yang menggunakan Internet terlibat dalam aktivitas online kreatif setiap minggu.

Untuk tujuan pendidikan, banyak anak-anak dan remaja dari segala usia menggunakan Internet untuk mengerjakan pekerjaan rumah, atau bahkan untuk mengejar ketertinggalan kelas atau mencari informasi kesehatan secara online setiap minggu. Remaja tampaknya lebih ingin mengakses informasi daripada anak kecil.

2.3 Dampak teknologi terhadap pengalaman digital anak-anak

Internet dan teknologi digital dapat memberikan peluang dan menghadirkan risiko bagi anak-anak dan remaja. Misalnya, ketika anak-anak menggunakan media sosial, mereka mendapat manfaat dari banyak kesempatan untuk bereksplorasi, belajar, berkomunikasi, dan mengembangkan keterampilan utama. Misalnya, jejaring sosial dipandang oleh anak-anak sebagai platform yang memungkinkan mereka mengeksplorasi identitas diri di lingkungan yang aman. Adanya keterampilan yang relevan dan kemampuan untuk mengetahui cara mengatasi masalah yang berkaitan dengan privasi dan reputasi merupakan hal yang penting bagi anak muda.

"Aku tahu semua yang kita posting di Internet akan ada jejak digitalnya selamanya dan itu dapat mempengaruhi kehidupan kita di masa depan", anak laki-laki, 14 tahun, Chile.

Namun, dari hasil konsultasi yang menunjukkan bahwa kebanyakan anak menggunakan media sosial sebelum usia minimal tiga belas tahun[11], dan mengingat layanan verifikasi usia umumnya lemah atau bahkan tidak ada, risiko yang dihadapi anak-anak dapat meningkat. Dan meskipun anak-anak ingin belajar keterampilan digital dan menjadi warga digital, khususnya peduli dengan privasi mereka, mereka cenderung berpikir tentang privasi dalam kaitannya dengan teman dan kenalan mereka "Apa yang bisa dilihat temanku?" dan tidak terlalu soal orang asing dan pihak ketiga. Dikombinasikan dengan rasa ingin tahu alamiah anak-anak dan ambang batas risiko yang umumnya lebih rendah, hal ini dapat membuat mereka rentan terhadap *grooming*, eksploitasi, perundungan, atau jenis konten atau kontak berbahaya lainnya.

[11] Contectados al Sur network, "Hablatam"; UNICEF, "Global Kids Online Comparative Report (2019)."

Dengan semakin populernya berbagi gambar dan video melalui aplikasi seluler, dan khususnya penggunaan platform *live streaming* oleh anak-anak, hal ini menghadirkan kekhawatiran terkait privasi dan risiko lebih lanjut. Beberapa anak memproduksi gambar seksual diri mereka sendiri, teman dan saudara kandung dan membagikannya secara online. Bagi sebagian orang, terutama anak-anak yang lebih besar, hal ini dapat dilihat sebagai eksplorasi alami dari seksualitas dan identitas seksual mereka, sementara bagi yang lain, terutama anak-anak yang lebih muda, seringkali terdapat paksaan oleh orang dewasa atau anak lain. Apapun masalahnya, konten yang dihasilkan merupakan konten yang ilegal di banyak negara dan dapat membuat anak-anak menghadapi risiko penuntutan, atau dapat digunakan untuk mengeksploitasi anak lebih lanjut.

Demikian pula, game online memungkinkan anak-anak memenuhi hak dasar mereka untuk bermain, serta membangun jaringan, menghabiskan waktu bersama dan bertemu teman baru, serta mengembangkan keterampilan penting. Kegiatan ini bisa menjadi kegiatan positif. Namun, semakin banyak bukti yang menunjukkan bahwa jika anak dibiarkan tanpa pengawasan dan tidak didukung oleh orang dewasa yang bertanggung jawab, platform game online juga dapat menimbulkan risiko bagi anak-anak, mulai dari gangguan psikologis terkait bermain game, risiko keuangan, pengumpulan dan monetisasi data pribadi anak, hingga perundungan di dunia maya, ujaran kebencian, kekerasan, dan paparan perilaku atau konten yang tidak pantas[12], dan *grooming* menggunakan gambar dan video, baik yang nyata, yang dihasilkan komputer, bahkan dalam bentuk *virtual reality* yang menggambarkan dan menormalisasikan pelecehan seksual dan eksploitasi anak-anak.

Selanjutnya, perkembangan teknologi telah menyebabkan munculnya *Internet of Things*, di mana semakin banyak jumlah dan jangkauan perangkat yang dapat terhubung, berkomunikasi, dan berjejaring melalui Internet. Perangkat ini termasuk mainan, monitor bayi, dan perangkat yang didukung oleh kecerdasan buatan yang dapat menimbulkan risiko privasi dan kontak yang tidak diinginkan.

2.4 Ancaman utama terhadap anak-anak di dunia maya

Orang dewasa dan anak-anak dihadapkan pada berbagai risiko dan bahaya di dunia maya. Meskipun demikian, anak-anak adalah populasi yang jauh lebih rentan. Sebagian anak juga lebih rentan dibandingkan kelompok anak lainnya, misalnya anak penyandang disabilitas[13] atau anak-anak yang sedang berpindah. Pembuat kebijakan perlu menjamin bahwa semua anak dapat berkembang dan dididik dalam lingkungan digital yang aman. Gagasan bahwa anak-anak rentan dan harus dilindungi dari segala bentuk eksploitasi dituangkan dalam Konvensi PBB tentang Hak Anak.

Beberapa area di lingkungan digital menawarkan peluang besar bagi anak-anak, tetapi pada saat yang sama dapat menambah risiko yang mungkin sangat merugikan anak-anak dan merusak kesejahteraan mereka. Terdapat kekhawatiran, baik untuk orang dewasa maupun anak-anak, bahwa misalnya Internet dapat digunakan untuk menyerang privasi pribadi, menjajakan disinformasi, atau lebih buruk lagi, memungkinkan akses ke pornografi.

Dalam hal ini sangat penting untuk dibedakan antara risiko dan bahaya bagi anak-anak. Tidak setiap aktivitas yang mengandung unsur risiko berbahaya dan tidak semua risiko pasti berbahaya bagi anak-anak, misalnya *Sexting*, yang merupakan cara remaja mengeksplorasi seksualitas dan hubungan mereka, yang mana tidak lantas berbahaya.

[12] UNICEF, "Global Kids Online Comparative Report (2019)." (UNICEF, 2019)

[13] Lundy et al., "TWO CLICKS FORWARD AND ONE CLICK BACK," Report on children with disabilities in the digitalenvironment (Council of Europe, Oktober 2019), https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

Gambar 2: Klasifikasi ancaman online terhadap anak-anak[14]

	Konten Anak sebagai penerima (produksi massal)	**Kontak** Anak sebagai partisipan (aktivitas yang diprakarsai oleh orang dewasa)	**Tingkah Laku** Anak sebagai aktor (pelaku / korban)
Agresif	**Konten kekerasan / berdarah**	**Pelecehan, penguntitan (*stalking*)**	**Perundiungan, aktivitas permusuhan antar teman sebaya**
Seksual	**Konten pornografi**	**'Grooming', kekerasan seksual ketika bertemu orang asing**	**Pelecehan seksual, '*sexting*'**
Nilai	**Konten rasis / kebencian**	**Persuasi ideologi**	**Konten buatan pengguna yang berpotensi berbahaya**
Komersial	**Iklan, pemasaran tersirat (*embedded marketing*)**	**Eksploitasi dan penyalahgunaan data pribadi**	**Judi, pelanggaran hak cipta**

Sumber: EU Kids Online (Livingstone, Haddon, Görzig, dan Ólafsson (2011)

Kemunculan era digital telah menghadirkan tantangan baru bagi perlindungan anak. Anak-anak harus diberdayakan untuk menjelajahi dunia online dengan aman dan menuai berbagai manfaatnya.

Pembuat kebijakan harus memastikan bahwa undang-undang, perlindungan, dan pedoman yang relevan tersedia untuk memungkinkan anak-anak berkembang dan belajar dengan aman. Anak-anak perlu dibekali dengan keterampilan yang diperlukan untuk mengidentifikasi ancaman dan sepenuhnya memahami implikasi dan nuansa perilaku mereka di dunia maya.

Saat anak-anak sedang online, mereka dapat menghadapi banyak ancaman dari organisasi, orang dewasa, dan teman sebayanya.

Konten dan manipulasi

- Paparan konten yang tidak pantas atau bahkan kriminal dapat menyebabkan anak-anak melakukan tindakan ekstrem seperti melukai diri sendiri, perilaku destruktif, dan perilaku kekerasan. Paparan konten semacam itu sama-sama dapat mengarah pada radikalisasi atau menganut ide-ide rasis atau diskriminatif. Diakui bahwa banyak anak tidak mematuhi batasan usia yang ditempatkan di situs web.
- Paparan informasi yang tidak akurat atau tidak lengkap membatasi pemahaman anak-anak tentang dunia di sekitar mereka. Tren penyesuaian konten mengikuti perilaku pengguna dapat menyebabkan 'gelembung filter', membatasi anak-anak untuk mengembangkan dan menjangkau berbagai konten.
- Paparan konten yang disaring oleh alogritma dengan maksud untuk memanipulasi dapat sangat memengaruhi perkembangan, opini, nilai, dan kebiasaan anak. Mengisolasi anak-anak dalam *'echo chamber'* atau 'gelembung filter' mencegah mereka mengakses berbagai pendapat dan ide.

[14] Livingstone, S., Haddon, L., Görzig, A., dan Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Fullfindings*. LSE, London: EU Kids Online, http://eprints.lse.ac.uk/33731/

Kontak dari orang dewasa atau teman sebaya

Anak-anak dapat menghadapi berbagai ancaman kontak dari teman sebaya atau orang dewasa.

- Perundungan di dunia maya dapat menyebar lebih luas dan lebih cepat daripada di dunia nyata. Itu bisa terjadi kapan saja, siang atau malam, sehingga menyerang yang sebelumnya dianggap sebagai 'ruang aman' dan bisa dilakukan secara anonim.
- Anak-anak yang menjadi korban di dunia nyata kemungkinan besar akan menjadi korban di dunia maya. Ini menempatkan anak-anak penyandang disabilitas pada risiko online yang lebih tinggi, karena penelitian menunjukkan bahwa anak-anak penyandang disabilitas lebih berpeluang mengalami pelecehan dalam bentuk apa pun, dan secara khusus lebih berpeluang mengalami viktimisasi seksual. Viktimisasi dapat mencakup perundungan, pelecehan, pengucilan, dan diskriminasi berdasarkan disabilitas aktual maupun yang dirasakan anak, atau pada aspek yang terkait dengan disabilitas mereka seperti cara mereka berperilaku atau berbicara, atau peralatan atau layanan yang mereka gunakan.
- Pencemaran nama baik dan merusak reputasi: gambar dan video dapat diubah dan dibagikan ke miliaran orang. Komentar yang dinilai buruk dapat ditemukan selama beberapa dekade, bebas dilihat siapa saja.
- Anak-anak dapat menjadi sasaran, menjadi korban *grooming* dan dilecehkan melalui Internet oleh pelaku, baik di daerahnya maupun di belahan dunia lain, dan pelaku sering kali memalsukan identitas mereka. Hal ini dapat terjadi dalam beberapa bentuk, seperti radikalisasi atau dipaksa untuk mengirimkan konten seksual eksplisit diri mereka sendiri.
- Ditekan, ditipu, atau dipaksa untuk melakukan pembelian dengan atau tanpa izin dari yang membayar tagihan.
- Iklan yang tidak diinginkan menimbulkan masalah persetujuan dan penjualan data.

Tingkah laku anak, yang berpotensi menimbulkan berbagai konsekuensi

- Perundungan di dunia maya dapat sangat mengganggu dan merusak karena dapat menyebar lebih luas, dengan tingkat publisitas yang lebih besar, dan konten yang diedarkan secara elektronik dapat muncul kembali kapan saja, yang dapat mempersulit korban perundungan untuk menyudahi insiden tersebut; bisa berupa gambar visual yang merusak atau kata-kata yang menyakitkan; konten tersedia 24 jam sehari; perundungan dengan cara elektronik dapat terjadi 24/7 sehingga dapat menyerang privasi korban bahkan di tempat-tempat yang 'aman' seperti rumah mereka; dan informasi pribadi dapat dimanipulasi, gambar visual diubah dan kemudian diteruskan ke orang lain. Selain itu, hal ini dapat dilakukan secara anonim. Pengungkapan informasi pribadi yang mengarah pada risiko cedera fisik, termasuk bertemu langsung dengan kenalan dari dunia maya, dengan kemungkinan terjadi pelecehan fisik dan/atau seksual.
- Pelanggaran hak milik pribadi atau orang lain melalui plagiarisme dan pengunggahan konten tanpa izin, termasuk pengambilan dan pengunggahan foto yang tidak pantas tanpa izin.
- Pelanggaran hak cipta orang lain, misalnya dengan mengunduh musik, film, atau program TV berbayar karena dapat membahayakan korban pencurian.
- Penggunaan Internet dan/atau game online secara kompulsif dan berlebihan, sehingga mengurangi aktivitas sosial dan/atau di luar ruangan yang penting bagi kesehatan, untuk membangun kepercayaan diri, perkembangan sosial, dan kesejahteraan secara umum.
- Mencoba menyakiti, melecehkan, atau menggertak orang lain, termasuk berpura-pura menjadi orang lain, seringkali sebagai anak lain.
- Perilaku yang semakin umum dilakukan oleh remaja adalah '*sexting*' (berbagi gambar atau teks seksual melalui ponsel). Gambar dan teks ini sering dibagikan di antara partner dalam suatu hubungan atau dengan calon partner, tetapi terkadang akhirnya dibagikan kepada audiens yang lebih luas. Diperkirakan kemungkinan remaja muda kurang memiliki pemahaman yang memadai tentang implikasi dari perilaku ini dan potensi risiko yang ditimbulkannya.

2.5 Bahaya utama bagi anak-anak di dunia maya

Bagian sebelumnya mengacu pada ancaman yang dapat dihadapi anak-anak di dunia maya. Bagian ini menyoroti bahaya yang dapat terjadi akibat ancaman tersebut.

Bahaya

Menurut studi UNICEF tentang penggunaan Internet, kategori berikut dianggap sebagai risiko dan bahaya:

- Pelecehan diri dan menyakiti diri sendiri:
  - konten bunuh diri
  - diskriminasi
- Paparan materi yang tidak sesuai:
  - paparan konten ekstremis/kekerasan/berdarah
  - pemasaran secara tersirat (*embedded marketing*)
  - judi online
- Sekitar 20 persen anak-anak yang disurvei tentang masalah ini mengatakan bahwa dalam setahun terakhir mereka telah melihat situs web atau diskusi online tentang orang-orang yang secara fisik melukai atau menyakiti diri mereka sendiri.
- Radikalisasi:
  - persuasi ideologi
  - ujaran kebencian
- Anak-anak lebih berpeluang melaporkan mereka terganggu oleh ujaran kebencian atau konten seksual online, diperlakukan dengan cara yang menyakitkan secara online atau offline, atau dengan bertemu langsung dengan seseorang yang pertama kali mereka kenal secara online.
- Pelecehan dan eksploitasi seksual:
  - konten buatan sendiri
  - Sexual grooming
  - materi pelecehan seksual anak (*child sexual abuse material* atau CSAM)
  - perdagangan manusia
  - eksploitasi seksual anak dalam perjalanan dan pariwisata

Sebuah studi tahun 2017 terhadap anak-anak di Denmark, Hongaria, dan Inggris menemukan bahwa 6 persen anak-anak memiliki foto eksplisit mereka yang dibagikan tanpa seizin mereka.

Pada tahun 2019, Internet Watch Foundation (IWF) mengidentifikasi lebih dari 132.000 halaman web yang dikonfirmasi berisi gambar dan video pelecehan seksual terhadap anak. Setiap halaman web dapat berisi apa saja, mulai dari satu hingga ribuan gambar pelecehan ini.

Risiko terkait kekerasan online, seperti penyebaran foto telanjang tanpa persetujuan dan perundungan di dunia maya secara seksual, ditandai dengan dinamika gender yang tidak setara, dimana anak perempuan biasanya lebih terdampak oleh tekanan gender terhadap perilaku seksual dan mengalami konsekuensi yang lebih negatif dan menimbulkan bahaya.

- Pelanggaran dan penyalahgunaan data pribadi:
  - peretasan
  - penipuan dan pencurian

  Banyak orang yang familar dengan penipuan dan peretasan, tetapi pelanggaran privasi terkait aktivitas online anak dipandang sebelah mata. Orang dewasa seringkali meremehkan anak muda dengan memeriksa ponsel mereka dan mengamati aktivitas mereka secara online, misalnya, laporan dari anak-anak di Brasil menunjukkan bahwa baik anak laki-laki maupun perempuan dari rentang usia yang beragam menganggap orang tua lebih mengontrol penggunaan Internet anak perempuan. Upaya untuk menjelaskan hal ini seringkali menunjukkan bahwa anak perempuan dalam beberapa kasus bisa jadi lebih rentan karena struktur sosial di mana mereka tinggal, khususnya yang berkaitan dengan keselamatan mereka, dalam konteks di mana batas antara interaksi online dan offline menjadi semakin kabur.
- Perundungan di dunia maya, penguntitan (*stalking*), dan pelecehan: Aktivitas permusahan teman sebaya dan penuh kekerasan

  Chat room dan situs jejaring sosial dapat menjadi pintu masuk kekerasan dan perundungan, karena pengguna yang bersifat anonim, termasuk anak muda, terlibat dalam komunikasi yang agresif atau kasar. Di tujuh negara di Eropa – Belgia, Denmark, Irlandia, Italia, Portugal, Rumania, dan Inggris – Livingstone, Mascheroni, lafsson, dan Haddon[1] ditemukan bahwa pada tahun 2010, rata-rata 8 persen anak-anak mengalami perundungan di dunia maya, sementara 12 persen anak-anak menjadi korban perundungan di dunia maya pada tahun 2014.

Sangat penting untuk digarisbawahi bahwa anak-anak yang rentan seringkali berisiko lebih tinggi menjadi korban perundungan di dunia maya.

[1] Livingstone, S., Mascheroni, G., Ólafsson, K., dan Haddon, L., (2014) *Children's online risks and opportunities: comparative findings from EU Kids Online and Net Children Go Mobile*. London: London School of Economics and PoliIcal Science, www.eukidsonline.net dan http://www.netchildrengomobile.eu/.

Fokus: Peningkatan ketidaksetaraan

Pada tahun 2017, sekitar 60 persen anak-anak tidak beraktivitas online di wilayah Afrika, dibandingkan dengan hanya 4 persen di Eropa. Pengguna internet pria melebihi jumlah pengguna wanita di setiap wilayah dunia, dan penggunaan internet oleh anak perempuan sering kali dipantau dan dibatasi. Dengan perluasan *broadband* ke bagian dunia yang tidak terhubung, ketimpangan ini akan meningkat secara signifikan[15].

Anak-anak yang bergantung ponsel daripada komputer mungkin kurang mendapatkan pengalaman online yang terbaik. Anak-anak yang berbicara dalam bahasa minoritas seringkali tidak dapat menemukan konten yang relevan bagi mereka secara online, dan anak-anak dari daerah pedesaan lebih berpeluang kata sandi atau uang mereka dicuri.

[15] Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)."

Penelitian menunjukkan bahwa banyak remaja di seluruh dunia harus menghadapi hambatan signifikan terhadap partisipasi mereka di dunia maya. Bagi banyak orang, tantangan akses, seperti konektivitas yang buruk, biaya kuota internet dan perangkat yang mahal, dan kurangnya peralatan yang memadai, masih menjadi hambatan utama.

Dengan perluasan *broadband* yang terjangkau ke negara berkembang, terdapat kebutuhan mendesak untuk menerapkan langkah-langkah untuk meminimalkan risiko dan ancaman terhadap anak-anak, sembari juga memungkinkan mereka untuk memanfaatkan semua manfaat yang ditawarkan dunia digital.

Fokus: Materi Pelecehan Seksual Anak (*Child Sexual Abuse Material* atau CSAM)

Skala masalah

Internet telah mengubah skala dan sifat produksi, distribusi, dan ketersediaan CSAM. Pada tahun 2018, perusahaan teknologi yang berbasis di Amerika Serikat melaporkan lebih dari 45 juta gambar dan video online yang diduga menunjukkan anak-anak yang sedang mengalami pelecehan seksual dari seluruh dunia. Ini adalah industri global dan skala serta keparahan kekerasan ini meningkat meskipun terdapat berbagai upaya untuk menghentikannya.

Secara historis, di dunia nyata, upaya menemukan CSAM mengharuskan pelaku untuk mengambil risiko yang cukup besar dengan biaya yang signifikan untuk mengakses materi tersebut. Dengan Internet, pelaku saat ini dapat mengakses materi ini dengan relatif mudah dan terlibat dalam perilaku yang semakin berisiko. Kamera semakin kecil, semakin terintegrasi ke dalam setiap aspek kehidupan kita, membuat proses pembuatan CSAM dan memperoleh konten dari pelecehan non-kontak menjadi lebih mudah daripada sebelumnya.

Kita tidak akan mampu menentukan ukuran atau bentuk yang tepat dari perusahaan gelap dan ilegal ini. Namun, yang jelas jumlah gambar ilegal yang beredar saat ini bisa mencapai jutaan. Hampir semua anak yang ada di dalam gambar mengalami gambar mereka diduplikasi. Pada tahun 2018, IWF melacak seberapa sering gambar dari seorang anak yang diketahui telah diselamatkan pada tahun 2013 kembali muncul. Selama tiga bulan, analis IWF melacak gambar-gambar tersebut 347 kali – 5 kali sehari setiap hari kerja.

Lanskap saat ini

Setiap kali sebuah gambar anak yang sedang dilecehkan muncul dan kembali muncul di dunia maya, atau diunduh oleh pelaku, anak itu kembali mengalami pelecehan. Korban dipaksa untuk menjalani sisa hidup mereka yang panjang dengan gambar-gambar mereka beredar.

Segera setelah ditemukannya materi yang menggambarkan, atau halaman web yang menampilkan pelecehan seksual terhadap anak, penting untuk menghapus atau memblokir konten tersebut secepat mungkin. Sifat global Internet membuat hal ini sulit dilakukan: pelaku dapat memproduksi materi di satu negara dan menyimpannya di negara lain untuk konsumen di negara ketiga. Hampir tidak mungkin untuk membuat surat perintah atau pemberitahuan nasional tanpa adanya kerjasama internasional yang canggih.

Laju inovasi dalam dunia digital membuat lanskap pelaku terus berubah. Ancaman utama yang baru-baru ini muncul antara lain:

- Munculnya enkripsi yang secara tidak sengaja memungkinkan pelaku untuk mengoperasikan dan berbagi materi dengan saluran tersembunyi, di saat yang sama juga membuat deteksi dan penegakan hukum lebih sulit untuk dilakukan.
- Forum khusus untuk *grooming* anak-anak bermunculan di berbagai sudut tersembunyi di Internet, yang mana menormalisasikan dan mendorong perilaku ini, dan seringkali mewajibkan memberikan 'konten baru' untuk bergabung.
- Ekspansi Internet yang cepat memungkinkan pengguna untuk online di area yang belum mengembangkan/menerapkan strategi perlindungan yang komprehensif atau infrastruktur yang relevan.
- Anak-anak menggunakan perangkat tanpa pengawasan di usia yang sangat muda, dan perilaku seksual online sedang dinormalisasikan. Jumlah gambar pelecehan yang dibuat oleh mereka sendiri meningkat setiap tahun.

Fokus: Konten yang dibuat sendiri

Anak-anak dan remaja dapat mengambil gambar atau video yang membahayakan diri mereka sendiri. Meskipun tindakan ini sendiri belum tentu ilegal dan dapat terjadi sebagai bagian dari perkembangan seksual yang normal dan sehat, terdapat risiko bahwa konten semacam ini dapat diedarkan secara online atau offline untuk membahayakan anak-anak atau digunakan untuk memeras. Meskipun sebagian anak mungkin ditekan atau dipaksa untuk membagikan gambar seksual, sebagian lainnya, (khususnya remaja) mungkin dengan sukarela memproduksi konten seksual. Ini tidak berarti bahwa mereka menyetujui atau bertanggung jawab atas penggunaan dan/atau distribusi gambar-gambar ini secara eksploitatif atau melecehkan.

Sexting didefinisikan sebagai "produksi gambar seksual sendiri",[16] atau sebagai "pertukaran pesan atau gambar seksual" dan "pembuatan, pembagian, dan penerusan gambar telanjang atau hampir telanjang yang menjurus ke arah seksual melalui ponsel dan/atau Internet"[17]. *Sexting* adalah bentuk konten seksual eksplisit yang dibuat sendiri,[18] dan praktiknya "sangat bervariasi tergantung konteks, makna, dan niat"[19].

Meskipun *sexting* mungkin merupakan bentuk paling umum dari konten seksual eksplisit yang dibuat sendiri yang melibatkan anak-anak, dan sering dilakukan oleh dan di kalangan remaja yang menyetujuinya dan memperoleh kesenangan dari pengalaman ini, ada juga banyak bentuk *sexting* yang tidak diinginkan. Ini mengacu pada aspek aktivitas non-konsensual, seperti berbagi atau menerima foto, video, atau pesan seksual eksplisit yang tidak diinginkan, misalnya oleh orang yang dikenal atau tidak dikenal yang mencoba melakukan kontak, menekan, atau *grooming* terhadap anak. *Sexting* juga bisa menjadi bentuk perundungan seksual, di mana seorang anak ditekan untuk mengirim gambar ke pacar / teman sebaya yang kemudian menyebarkannya ke jaringan teman sebaya tanpa persetujuan mereka.

Fokus: Perundungan di Dunia Maya

Meskipun perundungan adalah fenomena yang sudah ada jauh sebelum adanya Internet, meningkatnya skala, ruang lingkup dan keberlanjutan perundungan yang dilakukan secara online dapat memperparah apa yang sudah menjadi pengalaman tidak menyenangkan dan

---

16 Karen Cooper et al., "Adolescents and Self-Taken Sexual Images: A Review of the Literature," *Computers in Human Behaviour* 55 (Februari 2016): 706–16, https://doi.org/10.1016/j.chb.2015.10.003.

17 Jessica Ringrose et al., "A Qualitative Study of Children, Young People and 'Sexting': A Report Prepared for the NSPCC" (London, UK: National Society for the Prevention of Cruelty to Children, 2012), http://doi.wiley.com/10.1046/j.1365-2206.1997.00037.x.

18 UNODC, "Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children" (Vienna: UN, 2015), https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.[3] UNODC, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, hlm.22.

19 Cooper et al., "Adolescents and Self-Taken Sexual Images."

seringkali berbahaya bagi para korbannya. Perundungan di dunia maya (*cyberbullying*) didefinisikan sebagai kejahatan yang disengaja dan berulang yang dilakukan melalui penggunaan komputer, ponsel, dan perangkat elektronik lainnya. Ini sering terjadi bersamaan dengan perundungan di dunia nyata yang terjadi di sekolah atau di tempat lain, dapat mengandung dimensi rasisme, penistaan agama atau seksisme, dan dapat merupakan perpanjangan dari bahaya yang terjadi di dunia nyata, seperti melalui peretasan akun, penyebaran foto dan video online dan sifat 24/7 dari pesan yang menyakitkan dan ketersediaan konten. Umumnya hal ini merupakan masalah sosial daripada kriminal, dan kebijakan untuk mengatasi perundungan di dunia maya memerlukan pendekatan holistik yang melibatkan sekolah, keluarga dan terutama anak-anak itu sendiri.

Fokus: *Grooming* online dan pemerasan seksual

Dengan kemajuan pesat dalam teknologi dan peningkatan akses ke Internet dan komunikasi digital dalam beberapa tahun terakhir, risiko tinggi tindak kriminal online yang menargetkan anak-anak pasti mengikuti. Di antara bentuk-bentuk eksploitasi seksual anak online yang muncul adalah *grooming* online dan pemerasan seksual terhadap anak-anak. *Grooming* online secara luas mengacu pada proses orang dewasa berteman dan mempengaruhi seorang anak (di bawah usia 18 tahun), melalui penggunaan Internet atau teknologi digital lainnya, untuk memfasilitasi interaksi seksual kontak maupun non-kontak dengan anak. Melalui proses *grooming*, pelaku berusaha untuk membuat anak patuh untuk menjaga kerahasiaan dan agar tidak terdeteksi dan menghindari hukuman[20]. Penting untuk diketahui bahwa ada juga kasus kekerasan sesama teman sebaya.

INTERPOL melaporkan bahwa Internet memfasilitasi *grooming* karena internet memiliki sejumlah besar target potensial yang mudah diakses dan memungkinkan para pelaku untuk menampilkan diri mereka dengan cara yang menarik bagi anak. Penjahat seks anak online menggunakan manipulasi, paksaan, dan rayuan untuk menurunkan hambatan dan membujuk anak untuk terlibat dalam aktivitas seksual. Pelaku sengaja melakukan proses identifikasi calon korban yang rentan, pengumpulan intelijen tentang dukungan keluarga anak, dan menggunakan tekanan atau rasa malu/takut untuk melecehkan anak secara seksual. Groomer dapat menggunakan materi pornografi dewasa dan materi pelecehan atau eksploitasi anak untuk menghalangi target potensial mereka, menghadirkan aktivitas seksual anak sebagai hal yang wajar dan normal. Internet telah mengubah cara orang berinteraksi dan mendefinisikan ulang konsep 'teman'. Seorang pelaku *grooming* dapat menjalin pertemanan dengan seorang anak secara online dengan sangat mudah dan cepat, yang mengharuskan kita mengkaji ulang pesan didikan tradisional 'bahaya orang asing'.

Grooming online pertama kali diakui secara resmi dalam instrumen hukum internasional pada tahun 2007 oleh Konvensi Dewan Eropa tentang Perlindungan Anak terhadap Eksploitasi Seksual dan Pelecehan Seksual (Konvensi Lanzarote). Pasal 23 mengkriminalisasi "menghasut anak untuk tujuan seksual", yang mensyaratkan adanya usulan yang disengaja untuk bertemu dengan anak untuk tujuan melakukan pelanggaran seksual yang diikuti dengan "tindakan material yang mengarah pada pertemuan tersebut." Dalam banyak kasus *grooming*, anak-anak dilecehkan dan dieksploitasi secara seksual secara online – 'pertemuan' yang disyaratkan oleh Konvensi Lanzarote dan banyak undang-undang nasional yang ada sepenuhnya virtual – tetapi, bagaimanapun, sama berbahayanya bagi anak seperti pertemuan fisik. Sangat penting bahwa kriminalisasi terhadap *grooming* meluas "ke kasus-

[20] International Centre for Missing & Exploited Children, "Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review," Edisi Pertama (International Centre for Missing & Exploited Children, 2017), https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf.

kasus ketika pelecehan seksual bukan hasil pertemuan langsung tetapi dilakukan secara online."[21].

Pemerasan seksual[22] dapat terjadi sebagai salah satu bentuk *grooming* online atau sebagai pelanggaran tersendiri. Meskipun pemerasan seskual dapat terjadi tanpa proses grooming online, dalam beberapa kasus *grooming* online dapat menyebabkan pemerasan seksual[23]. Pemerasan seksual dapat terjadi dalam konteks *grooming* online ketika seorang pelaku memanipulasi dan memberikan pengaruh terhadap anak selama proses *grooming* melalui ancaman, perundungan, dan paksaan untuk mengirim gambar seksual diri mereka sendiri (konten yang dibuat sendiri)[24]. Jika korban tidak memenuhi permintaan seksual, gambar intim lain, uang, atau keuntungan lainnya, gambarnya dapat diposting secara online dengan tujuan menimnbulkan penghinaan atau penderitaan atau memaksa anak untuk menghasilkan materi seksual eksplisit lainnya[25].

Pemerasan seksual disebut sebagai "serangan seksual secara virtual" karena efek emosional dan psikologis yang serupa yang dialami korban[26]. Dalam beberapa kasus, pelecehan tersebut sangat menimbulkan trauma sehingga para korban berusaha melukai diri sendiri atau bunuh diri sebagai cara untuk melarikan diri dari pelecehan tersebut.

Europol mencatat bahwa pengumpulan informasi untuk mengkaji ruang lingkup pemerasan seksual yang mempengaruhi anak-anak itu adalah kegiatan yang menantang dan kejadian ini mungkin sangat banyak yang tidak dilaporkan[27]. Selain itu, kurangnya terminologi dan definisi umum untuk *grooming* online dan pemerasan seksual merupakan hambatan untuk pengumpulan data yang akurat dan pemahaman tentang ruang lingkup sebenarnya atas masalah ini secara global.

2.6 Anak-anak dengan kerentanan

Anak-anak dan remaja dapat menjadi rentan karena beragam alasan. Penelitian yang dilakukan pada tahun 2019 menyatakan bahwa "kehidupan digital anak-anak yang rentan jarang mendapat perhatian yang bernuansa dan sensitif, yang mana kesulitan yang mereka alami di "kehidupan nyata" cenderung lebih menarik perhatian. Lebih lanjut, laporan tersebut selanjutnya mengatakan bahwa "mereka [anak-anak dan remaja] paling hanya menerima saran keamanan online generik yang sama seperti semua anak dan remaja lainnya, padahal diperlukan intervensi spesialis".

---

[21] Lanzarote Committee, Committee of the Parties to the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, *Solicitation of children for sexual purposes through information and communication technologies (grooming), Opinion on Article 23 of the Lanzarote Convention and its explanatory note*, Jun. 17, 2015, *pada https://edoc.coe.int/en/children-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html* (terakhir dikunjungi pada 6 November 2019).

[22] National Center for Missing and Exploited Children (NCMEC), *Sextortion*, *at* http://www.missingkids.com/theissues/onlineexploitation/sextortion (terakhir dikunjungi pada 6 November 2019).

[23] Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27-28, *pada* http://luxembourgguidelines.org/english-version.

[24] Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27-28, *pada* http://luxembourgguidelines.org/english-version.

[25] Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27-28, *at* http://luxembourgguidelines.org/english-version.

[26] Benjamin Wittes et al., "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault" (Brookings Institution, 11 Mei 2016), https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.

[27] Europol, "Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective" (European Cybercrime Centre, Mei 2017), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

Tiga contoh kerentanan spesifik adalah: anak migran, anak dengan gangguan spektrum autisme dan anak penyandang disabilitas), tetapi tentu saja masih banyak kategori lainnya.

Anak migran

Anak-anak dan remaja dari latar belakang migran sering datang ke satu negara (atau sudah tinggal di sana) dengan serangkaian pengalaman dan harapan sosial budaya tertentu. Meskipun teknologi biasanya dianggap sebagai fasilitator untuk terhubung dan berpartisipasi, risiko dan peluang di dunia maya dapat sangat beragam di berbagai konteks. Lebih lanjut, temuan dan penelitian empiris menunjukkan fungsi vital media digital secara umum:

- Penting untuk orientasi (saat bepergian ke negara baru).
- Merupakan fungsi sentral untuk apropriasi dan pengenalan dengan masyarakat/budaya negara penerima.
- Media sosial dapat memainkan peran kunci dalam menjaga kontak dengan keluarga dan teman sebaya, dan untuk mengakses informasi umum.

Di samping banyak aspek positif, media digital juga dapat membawa tantangan bagi para migran, seperti:

- Infrastruktur – penting untuk memikirkan ruang aman di dunia maya sehingga anak-anak dan remaja migran dapat memperoleh manfaat privasi dan keamanan.
- Sumber daya – para migran menghabiskan sebagian besar uang mereka untuk kuota internet prabayar.
- Integrasi – selain memiliki akses ke teknologi, anak-anak migran dan remaja juga perlu mendapatkan pendidikan digital yang baik.

Anak dengan Gangguan Spektrum Autisme (*Autism Spectrum Disorder* atau ASD)

Spektrum autisme merangkum dua domain inti dalam proses diagnostik perilaku DSM-5:

- perilaku terbatas dan berulang ("kebutuhan akan kesamaan");
- kesulitan dengan perilaku sosial dan komunikasi;
- sering disertai dengan disabilitas intelektual, masalah bahasa dan masalah serupa lainnya.

Teknologi dan Internet menawarkan kesempatan tanpa batas bagi anak-anak dan remaja ketika belajar, berkomunikasi, dan bermain. Namun, di samping manfaat ini, terdapat banyak risiko di mana anak-anak dan remaja penyandang ASD mungkin lebih rentan:

- Internet dapat memberikan anak-anak dan remaja penyandang autisme kesempatan untuk bersosialisasi dan minat khusus yang mungkin tidak mereka miliki secara offline.
- Tantangan sosial, seperti kesulitan memahami niat orang lain, dapat membuat kelompok ini rentan terhadap "teman" yang memiliki niat buruk.
- Tantangan online sering dikaitkan dengan karakteristik inti autisme: panduan konkret dan spesifik dapat meningkatkan pengalaman online individu, tetapi tantangan yang mendasarinya akan tetap ada.

Anak-anak penyandang disabilitas

Anak-anak penyandang disabilitas menghadapi banyak risiko online yang sama seperti yang dialami anak-anak tanpa disabilitas, tetapi mereka mungkin juga menghadapi risiko khusus terkait disabilitas mereka. Anak-anak penyandang disabilitas sering menghadapi pengucilan, stigmatisasi, dan hambatan (fisik, ekonomi, sosial dan sikap) untuk berpartisipasi dalam komunitas mereka. Pengalaman-pengalaman ini dapat mendorong anak penyandang disabilitas untuk mencari interaksi sosial dan pertemanan di ruang online, yang bisa menjadi kegiatan positif, membangun kepercayaan diri dan menciptakan

jaringan dukungan. Namun, hal ini juga dapat menempatkan mereka pada risiko yang lebih besar menjadi korban *grooming*, rayuan online, dan/atau pelecehan seksual – penelitian menunjukkan bahwa anak-anak yang mengalami kesulitan di dunia nyata dan mereka yang terpengaruh oleh kesulitan psikososial berisiko tinggi mengalami insiden tersebut.[28].

Secara keseluruhan, anak-anak yang menjadi korban di dunia nyata kemungkinan besar akan menjadi korban di dunia maya. Ini menempatkan anak-anak penyandang disabilitas pada risiko yang lebih tinggi saat berada di dunia maya, namun mereka memiliki kebutuhan yang lebih besar untuk beraktivitas online. Penelitian menunjukkan bahwa anak-anak penyandang disabilitas lebih berpeluang mengalami pelecehan dalam bentuk apa pun[29], dan secara khusus lebih berpeluang mengalami viktimisasi seksual[30]. Viktimisasi dapat mencakup perundungan, pelecehan, pengucilan, dan diskriminasi berdasarkan disabilitas aktual maupun yang dirasakan anak, atau pada aspek yang terkait dengan disabilitas mereka seperti cara mereka berperilaku atau berbicara, peralatan atau layanan yang mereka gunakan.

Pelaku *grooming*, rayuan online, dan/atau pelecehan seksual terhadap anak penyandang disabilitas dapat mencakup tidak hanya pelaku yang menargetkan anak, tetapi juga mereka yang menargetkan anak penyandang disabilitas. Pelaku tersebut dapat termasuk para '*devotees*' – orang-orang yang bukan penyandang disabilitas yang tertarik secara seksual kepada penyandang disabilitas (paling umum terhadap orang yang diamputasi dan orang yang menggunakan alat bantu gerak), sebagian di antaranya bahkan berpura-pura menjadi disabilitas[31]. Tindakan yang dilakukan orang-orang tersebut dapat berupa mengunduh foto dan video anak-anak 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 ditargetkan atau tepat untuk menangani tindakan tersebut.

Terdapat kekhawatiran bahwa '*sharenting*' (orang tua berbagi informasi dan foto anak-anak mereka secara online) dapat melanggar privasi anak, menyebabkan perundungan, menyebabkan rasa malu, atau memiliki konsekuensi negatif di kemudian hari[32]. Orang tua dari anak-anak penyandang disabilitas dapat berbagi informasi tersebut untuk mencari dukungan atau nasihat, yang mana membuat anak-anak penyandang disabilitas lebih berisiko mengalami dampak yang merugikan.

Sebagian anak penyandang disabilitas mungkin menghadapi kesulitan dalam menggunakan, atau bahkan dikucilkan dari lingkungan online karena desain yang tidak dapat diakses (misalnya aplikasi yang tidak memungkinkan untuk memperbesar ukuran teks), penolakan akomodasi yang diminta (misalnya software pembaca layar atau kontrol komputer adaptif), atau kebutuhan akan dukungan yang tepat (misalnya pelatihan tentang cara menggunakan peralatan, dukungan personal untuk melakukan interaksi sosial[33]).

---

[28] Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content," *Berkman Center for Internet & Society, Harvard University*, Desember 2008, 87, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.`

[29] UNICEF, "State of the World's Children Report: Children with Disabilities," 2013, https://www.unicef.org/publications/files/SOWC2013_Exec_Summary_ENG_Lo_Res_24_Apr_2013.pdf.

[30] Katrin Mueller-Johnson, Manuel P. Eisner, dan Ingrid Obsuth, "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors," *Journal of Interpersonal Violence* 29, no. 17 (November 2014): 3180–3206, https://doi.org/10.1177/0886260514534529.

[31] Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder," *Sexual and Disability* 15, no. 4 (1997): 18, https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf.

[32] UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy," Innocenti Discussion Paper 2017-03 (UNICEF, Office of Research-Innocenti), diakses pada 16 Januari 2020, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf.

[33] Untuk pedoman tentang hak-hak ini, lihat Konvensi Hak Penyandang Disabilitas Pasal 9 tentang Aksesibilitas dan Pasal 21 tentang Kebebasan berekspresi dan berpendapat, dan akses ke informasi.

Terkait dengan risiko kontrak atau penandatanganan syarat dan ketentuan, anak-anak penyandang disabilitas memiliki risiko lebih tinggi untuk menerima persyaratan hukum yang terkadang bahkan orang dewasa pun tidak dapat memahaminya.

2.7 Persepsi anak-anak tentang risiko online

Paparan kekerasan, akses ke konten, barang, dan layanan yang tidak pantas di seluruh dunia; kekhawatiran tentang penggunaan yang berlebihan; masalah perlindungan data dan privasi adalah risiko yang disorot oleh anak-anak [34].

Remaja melaporkan berbagai kekhawatiran mengenai keterlibatan mereka dengan teknologi digital. Hal ini di antaranya masalah keamanan online yang umum dibahas, seperti ketakutan berinteraksi dengan orang asing di dunia maya, mengakses konten yang tidak pantas, atau terpapar *malware* atau virus – sementara aspek lainnya terkait dengan keandalan akses mereka ke teknologi; orang tua yang mencampuri kehidupan 'pribadi' mereka di dunia maya; dan keterampilan literasi digital mereka[35].

Penelitian EU Kids Online menunjukkan bahwa pornografi dan konten kekerasan menjadi perhatian online anak-anak di Eropa. Secara keseluruhan, anak laki-laki tampak lebih terganggu oleh kekerasan, sementara anak perempuan lebih peduli dengan risiko terkait kontak[36]. Kekhawatiran akan risiko dunia maya lebih tinggi di kalangan anak-anak dari negara 'penggunaan tinggi, risiko tinggi'.

Di Amerika Latin, hasil dari konsultasi anak telah menunjukkan bahwa hilangnya privasi, kekerasan dan pelecehan merupakan kekhawatiran utama anak[37]. Anak-anak melaporkan dihubungi oleh orang yang tidak mereka kenal — ini terutama terjadi saat bermain game online. Dalam situasi seperti itu, strategi utama tampaknya adalah dengan tidak menggubris dan/atau memblokir orang tersebut. Anak perempuan dihadapkan pada pelecehan di media sosial sejak usia dini. Mereka berhasil mengatasi bentuk-bentuk kekerasan ini sendiri, memblokir pengguna, dan mengubah pengaturan privasi. Pelecehan datang dari pengguna yang terkadang tidak berbicara bahasa Spanyol, tetapi berhasil mengirimi mereka gambar, meminta pertemanan, dan mengomentari kiriman mereka. Beberapa anak laki-laki juga melaporkan telah menerima permintaan semacam itu.

Di berbagai belahan dunia, anak-anak memiliki pemahaman yang baik tentang beberapa risiko yang mereka hadapi saat online[38]. Penelitian telah menunjukkan bahwa mayoritas anak-anak mampu membedakan perundungan di dunia maya dari sekadar bercanda atau menggoda secara online, menyadari bahwa perundungan di dunia maya memiliki dimensi publik dan dirancang untuk menyakiti[39].

---

[34] Amanda Third et al., "Children's Rights in the Digital Age" (Melbourne: oung and Well Cooperative Research Centre, September 2014), http://www.uws.edu.au/data/assets/pdf_file/0003/753447/ Childrens-rights-in-the-digital-age.pdf.

[35] Amanda Third et al., "Young and Online: Children's Perspectives on Life in the Digital Age," The State of the World's Children 2017 Companion Report (Sydney: Western Sydney University, 2017). Laporan tersebut merangkum pandangan 490 anak berusia 10–18 tahun, dari 26 negara yang berbicara dalam 24 bahasa resmi.

[36] Livingstone, S. (2014) *EU Kids Online: Findings, methods, recommendations*. LSE, London: EU Kids Online, https://lsedesignunit.com/EUKidsOnline/.

[37] Contectados al Sur network, "Hablatam."

[38] Sejak 2016, ITU melakukan konsultasi dalam COP dengan pemangku kepentingan dari kalangan anak-anak dan dewasa tentang isu-isu yang relevan seperti perundungan di dunia maya, literasi digital dan aktivitas online anak-anak.

[39] UNICEF, "Global Kids Online Comparative Report (2019)."

3. Menyusun strategi nasional perlindungan online anak

Dalam mengembangkan strategi nasional perlindungan online anak untuk mempromosikan keamanan online bagi anak-anak dan remaja, pemerintah pusat dan lembaga pembuat kebijakan perlu mengidentifikasi praktik terbaik dan terlibat dengan pemangku kepentingan utama.

Bagian berikut menyoroti aktor dan pemangku kepentingan beserta uraian peran dan tanggung jawab potensial mereka terkait dengan perlindungan online anak.

3.1 Aktor dan pemangku kepentingan

Pembuat kebijakan dapat mengidentifikasi individu, kelompok, dan organisasi yang sesuai yang mewakili masing-masing aktor dan pemangku kepentingan dalam yurisdiksi mereka. Mengapresiasi setiap kegiatan mereka saat ini, baik kegiatan yang direncanakan maupun yang potensial, penting dalam koordinasi nasional dan dalam mengatur strategi perlindungan online anak.

Anak-anak dan remaja

Di seluruh dunia, anak-anak dan remaja telah menunjukkan bahwa mereka dapat beradaptasi dan menggunakan teknologi baru dengan sangat mudah. Internet menjadi semakin penting di sekolah dan sebagai arena di mana anak-anak dapat bekerja, bermain, dan berkomunikasi.

Menurut laporan terbaru dari ChildFund Alliance, hanya 18,1 persen anak yang diwawancarai yang berpikir bahwa pemerintah mengambil tindakan untuk melindungi mereka. Dalam hal ini, penting bagi pembuat kebijakan untuk terlibat dengan anak-anak, mengakui hak mereka untuk didengar (Pasal 12 KHA).

Untuk dapat melindungi anak, pembuat kebijakan harus membakukan definisi anak dalam semua dokumen hukum. Seorang anak harus didefinisikan sebagai siapa saja yang berusia di bawah 18 tahun. Hal ini sesuai dengan Pasal 1 Konvensi PBB tentang Hak Anak (UN *Convention on the Rights of the Child* atau UNCRC), yang menyatakan bahwa "seorang anak berarti setiap manusia yang berusia di bawah 18 tahun". Perusahaan tidak boleh menganggap siapa pun yang berusia di bawah 18 tahun tetapi cukup umur secara hukum untuk menyetujui pemrosesan data sebagai orang dewasa. Definisi sempit ini tidak dibenarkan oleh bukti apapun terkait *milestone* perkembangan masa kanak-kanak. Hal ini merusak hak mereka dan mengancam keselamatan anak-anak.

Meskipun banyak anak mungkin tampak percaya diri dalam menggunakan teknologi, banyak yang merasa tidak aman[40] saat online dan memiliki beberapa kekhawatiran[41] terkait Internet.

Kurangnya pengalaman anak-anak dan remaja tentang dunia luar dapat membuat mereka rentan terhadap berbagai risiko. Mereka berhak untuk mendapatkan bantuan dan perlindungan. Penting juga untuk diingat bahwa tidak semua anak dan remaja akan memiliki

[40] ChildFund Alliance, "VIOLENCE AGAINST CHILDREN AS EXPLAINED BY CHILDREN," Save Voices Big Dreams, 2019, https://childfundalliance.org/zdocs/a9357061-749f-4ebf-a1e9-b1aee81cb216/SVBD-THE_REPORT-digital.pdf.

[41] Council of Europe, "It's Our World: Children's Views on How to Protect Their Rights in the Digital World," Report on child consultations (Council of Europe, Children's Right Division, Oktober 2017), https://rm.coe.int/it-s-our-world-children-s-views-on-how-to-protect-their-rights-in-the-/1680765dff.

pengalaman yang sama dalam menggunakan Internet atau teknologi baru. Beberapa anak berkebutuhan khusus yang disebabkan oleh disabilitas fisik atau lainnya mungkin sangat rentan dalam lingkungan online dan akan membutuhkan dukungan tambahan.

Berbagai survei telah berkali-kali menunjukkan bahwa apa yang orang dewasa pikirkan tentang anak-anak dan remaja lakukan di dunia maya dan apa yang sebenarnya terjadi bisa sangat berbeda. Setengah dari semua anak yang disurvei mengatakan bahwa di negara mereka orang dewasa tidak mendengarkan pendapat mereka tentang masalah yang penting bagi mereka[42]. Oleh karena itu, dalam pengaturan apa pun yang dibuat di tingkat pusat untuk mengembangkan kebijakan di area ini, penting untuk memastikan ditemukannya mekanisme yang tepat yang memungkinkan didengarnya semua suara anak dan remaja dan dipertimbangkannya pengalaman nyata mereka dalam menggunakan teknologi.

Orang tua, wali, dan pendidik

Orang tua, wali dan pendidik menghabiskan sebagian besar waktu dengan anak-anak. Mereka harus mendapatkan edukasi literasi digital untuk memahami lingkungan online dan mampu melindungi anak-anak dan mengajari anak-anak cara melindungi dirinya sendiri.

Institusi pendidikan memiliki tanggung jawab khusus untuk mengajar anak-anak tentang cara agar tetap aman saat online, terlepas apakah mereka menggunakan Internet di sekolah, di rumah atau di mana pun, pembuat kebijakan harus memasukkan dalam kurikulum nasional literasi digital sejak usia sangat dini (3 hingga 18 tahun). Hal ini agar anak-anak dapat melindungi diri mereka sendiri, mengetahui hak-hak mereka sehingga menggunakan Internet sebagai sumber pengetahuan[43].

Pembuat kebijakan diingatkan bahwa orang tua dan wali hampir selalu menjadi garis pertahanan dan dukungan pertama, terakhir dan terbaik bagi anak-anak mereka sendiri. Namun ketika menghadapi Internet, mereka mungkin merasa agak kebingungan. Sekali lagi, sekolah dapat menjadi jalur komunikasi penting untuk menjangkau orang tua dan wali, untuk membuat mereka sadar akan risiko dan berbagai peluang positif yang dihadirkan oleh teknologi baru. Namun, sekolah tidak boleh menjadi satu-satunya jalan yang digunakan untuk menjangkau orang tua dan wali. Penting untuk menggunakan beragam jalur komunikasi untuk mengoptimalkan peluang untuk menjangkau sebanyak mungkin orang tua dan wali. Industri memiliki peran penting di sini dalam mendukung pengguna atau pelanggan mereka. Orang tua dan wali dapat memilih untuk mengelola aktivitas dan akses online anak mereka, berbicara dengan anak tentang perilaku dan penggunaan teknologi yang benar, memahami apa yang dilakukan anak di dunia maya sehingga obrolan di keluarga memadukan pengalaman online dan offline sebagai satu kesatuan.

Orang tua dan wali juga perlu menjadi contoh yang baik kepada anak-anak mereka tentang cara menggunakan perangkat mereka dan berperilaku dengan cara yang tepat di Internet.

Pembuat kebijakan harus diingatkan bahwa orang tua dan wali harus dikonsultasikan untuk mendapatkan pandangan, pengalaman, dan pemahaman mereka tentang melindungi anak-anak mereka di dunia maya.

---

[42] ChildFund Alliance, "Violence against children as explained by children."

[43] UNICEF, "Policy Guide on Children and Digital Connectivity" (Policy Lab, Data, Research and Policy, United Nations Children's Fund, Juni 2018), https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf.

Terakhir, pembuat kebijakan bersama dengan lembaga publik lainnya dapat mengembangkan kampanye kesadaran publik, termasuk untuk orang tua, pengasuh dan pendidik. Perpustakaan umum, puskesmas, bahkan pusat perbelanjaan dan pusat ritel besar lainnya dapat menyediakan tempat untuk mengakses informasi keamanan elektronik dan keterampilan digital. Ketika melaksanakan tugas ini, pemerintah harus memastikan saran yang diberikan bersifat netral, bebas dari kepentingan pribadi, dan mencakup berbagai macam masalah dalam ruang digital.

Industri

Industri adalah salah satu pemangku kepentingan utama dalam ekosistem ini karena sektor ini memiliki pengetahuan teknologi yang perlu ditangani dan dipahami oleh pembuat kebijakan untuk mengembangkan kerangka hukum. Oleh karena itu, penting bagi pembuat kebijakan untuk melibatkan industri dalam proses penjabaran undang-undang perlindungan online anak.

Kita juga perlu mendorong industri untuk memasukkan pendekatan keselamatan dengan desain ketika mengembangkan teknologi baru dalam bisnis mereka. Tentunya perusahaan yang mengembangkan atau menyediakan produk dan layanan teknologi baru harus membantu penggunanya untuk memahami cara kerjanya dan cara menggunakannya dengan aman dan tepat.

Industri juga memiliki tanggung jawab besar untuk membantu mempromosikan kesadaran akan agenda online dan keamanan, terutama kepada anak-anak dan orang tua atau wali mereka, tetapi juga kepada masyarakat luas. Dengan terlibat dengan cara ini, pemangku kepentingan industri akan belajar lebih banyak tentang kekhawatiran pemangku kepentingan lainnya dan risiko serta bahaya yang dihadapi pengguna akhir. Dengan pengetahuan ini, Industri dapat memperbaiki produk dan layanan yang ada, dan mengidentifikasi berbagai bahaya dalam pengembangan produknya.

Kemajuan terbaru dalam kecerdasan buatan membuka jalan bagi industri untuk membangun *check and balance* yang jauh lebih kuat untuk mengidentifikasi pengguna dan untuk menyediakan lingkungan yang kondusif bagi anak-anak untuk menciptakan perilaku online yang positif. Kemajuan ini juga dapat menimbulkan risiko baru bagi anak-anak.

Di beberapa negara, Internet diatur oleh kerangka regulasi mandiri (*self-regulation*) maupun regulasi bersama (*co-regulation*). Namun, beberapa negara sedang mempertimbangkan, atau telah menerapkan, kerangka hukum dan peraturan, termasuk kewajiban bagi perusahaan untuk mendeteksi, memblokir dan/atau menghilangkan bahaya terhadap anak-anak dari platform atau layanan mereka, serta menyediakan rute pelaporan yang jelas dan akses ke bantuan.

Komunitas riset dan lembaga swadaya masyarakat

Di dalam universitas dan komunitas riset, kemungkinan besar terdapat sejumlah akademisi dan cendekiawan yang memiliki minat profesional dan pengetahuan yang sangat detail tentang dampak sosial dan teknis dari Internet. Mereka adalah sumber daya yang sangat berharga dalam hal membantu pemerintah pusat dan pembuat kebijakan untuk mengembangkan strategi, yang didasarkan pada fakta dan bukti yang kuat. Mereka juga dapat bertindak sebagai penyeimbang intelektual untuk kepentingan bisnis yang terkadang terlalu jangka pendek dan komersial.

Demikian pula, dalam komunitas lembaga swadaya masyarakat (LSM), terdapat berbagai keahlian dan informasi yang dapat menjadi sumber yang sangat berharga dalam menjangkau atau memberikan layanan kepada anak-anak, orang tua, pengasuh dan pendidik untuk membantu mempromosikan agenda keamanan online dan secara umum melindungi kepentingan publik.

Penegakan hukum

Sebuah fakta yang menyedihkan bahwa sehebat apapun sebuah teknologi, ia juga menarik perhatian unsur-unsur kriminal dan anti-sosial. Internet telah sangat meningkatkan sirkulasi CSAM dan bahaya online lainnya. Predator seksual telah menggunakan Internet untuk melakukan kontak awal dengan anak-anak dengan memikat anak-anak ke dalam bentuk kontak yang sangat berbahaya, baik di dunia maya maupun dunia nyata. Perundungan dan bentuk-bentuk pelecehan lainnya dapat sangat berbahaya bagi kehidupan anak-anak dan Internet telah menjadi cara baru untuk hal ini terjadi.

Oleh karena itu, komunitas penegak hukum harus terlibat sepenuhnya dengan strategi apa pun secara menyeluruh untuk membantu menjadikan Internet lebih aman bagi anak-anak dan remaja. Pejabat penegak hukum perlu mendapatkan pelatihan yang tepat untuk melakukan investigasi terhadap kejahatan terkait Internet terhadap anak-anak dan remaja. Mereka membutuhkan tingkat pengetahuan teknis yang tepat dan akses ke fasilitas forensik agar mereka dapat mengekstrak dan menafsirkan data yang diperoleh dari komputer atau Internet dalam waktu sesingkat mungkin.

Selain itu, penegak hukum perlu menetapkan mekanisme yang jelas untuk memungkinkan anak-anak dan remaja, atau anggota masyarakat mana pun, untuk melaporkan setiap insiden atau kekhawatiran yang mungkin mereka miliki terkait keamanan online anak atau remaja. Banyak negara, misalnya, telah membentuk *hotline* untuk memfasilitasi laporan CSAM dan mekanisme khusus serupa untuk memfasilitasi laporan jenis masalah lain, misalnya perundungan. Pembuat kebijakan harus bekerja dengan International Association of Internet Hotlines (INHOPE), mendukung mereka dalam menilai dan memproses laporan CSAM dan memanfaatkan bantuan dari INHOPE untuk organisasi di seluruh dunia dalam pembuatan hotline bagi negara yang belum memilikinya. Pembuat kebijakan harus memastikan adanya saluran komunikasi yang terbuka antara penegak hukum dan pemangku kepentingan lainnya. Penegakan hukum adalah sumber utama untuk CSAM yang ditangkap dalam batas yuridiksi negara. Harus dilakukan sebuah proses untuk memeriksa materi ini untuk menentukan apakah korban lokal dapat diidentifikasi. Jika hal ini tidak memungkinkan, materi harus diteruskan ke INTERPOL untuk dimasukkan ke dalam Basis Data ICSE. Karena hal ini merupakan ancaman global, pembuat kebijakan perlu memastikan kerjasama internasional antara lembaga penegak hukum di seluruh dunia. Ha ini akan mengurangi waktu proses formal dan memungkinkan agen untuk mendapatkan respons yang lebih cepat.

Layanan sosial

Ketika anak-anak atau remaja menghadapi bahaya atau dilecehkan secara online, misalnya foto mereka yang tidak pantas atau ilegal diposting di internet, para korban mungkin memerlukan dukungan atau konseling khusus jangka panjang. Mungkin juga dibutuhkan layanan bantuan menyeluruh dan praktik restoratif bagi pelaku terutama pelaku berusia muda yang juga mungkin menjadi korban pelecehan online atau offline. Profesional yang bekerja dalam layanan sosial perlu mendapatkan pelatihan yang tepat agar dapat memberikan dukungan semacam ini. Dukungan harus diberikan melalui saluran online dan offline.

Layanan perawatan kesehatan

Layanan perawatan kesehatan yang dibutuhkan setelah kasus kekerasan terhadap anak harus tercakup dalam rencana dasar perawatan kesehatan di tingkat nasional. Institusi perawatan kesehatan harus melaksanakan pelaporan wajib atas kekerasan. Profesional perawatan kesehatan harus dibekali dan memiliki pengetahuan yang memadai agar dapat mendukung anak-anak dalam hal ini. Layanan perawatan kesehatan harus mencakup dukungan untuk kesehatan mental dan kesejahteraan anak-anak.

Kementerian

Kebijakan Perlindungan Online Anak akan masuk dalam kewenangan sejumlah kementerian, sehingga perlu melibatkan semua kementerian terkait untuk menciptakan strategi dan rencana aksi nasional yang sukses. Kemeneterian dimaksud antara lain:

- Kementerian Dalam Negeri
- Kementerian Kesehatan
- Kementerian Pendidikan
- Peradilan
- Kementerian Komunikasi dan Informatika
- Regulator

Regulator berada pada posisi terbaik untuk berkontribusi pada peran pengendali dan akuntan dengan bekerja sama dengan lembaga pemerintah. Hal ini dapat termasuk media dan regulator perlindungan data.

Operator jaringan broadband, seluler, dan Wifi

Operator dapat mendeteksi, memblokir, dan melaporkan konten ilegal dalam jaringan mereka dan menyediakan alat, layanan, dan konfigurasi yang ramah keluarga untuk digunakan orang tua dalam memilih cara mengelola akses anak-anak mereka. Penting bagi penyedia untuk memastikan bahwa kebebasan sipil dan privasi sama-sama dihormati.

Hak Anak

Lembaga hak asasi manusia independen untuk anak dapat memainkan peran penting dalam memastikan perlindungan anak secara online. Meskipun mandatnya berbeda-beda, lembaga-lembaga tersebut umumnya memiliki fungsi untuk:

- memantau dampak undang-undang, kebijakan, dan praktik terhadap perlindungan hak-hak anak;
- mempromosikan penerapan standar hak asasi manusia internasional di tingkat nasional;
- menyelidiki pelanggaran hak anak;
- memberikan keahlian tentang hak-hak anak ke pengadilan;
- memastikan bahwa pandangan anak-anak didengar terkait hal-hal yang berkaitan dengan hak asasi mereka, termasuk pengembangan hukum dan kebijakan yang relevan;
- mempromosikan pemahaman dan kesadaran publik tentang hak-hak anak; dan
- melakukan inisiatif-inisiatif pendidikan dan pelatihan hak asasi manusia.

Penting untuk memasukkan konsultasi langsung dengan anak-anak yang termasuk hak mereka berdasarkan pasal 12 UNCRC. Fungsi penasehat, investigasi, peningkatan kesadaran dan pendidikan dari lembaga hak asasi manusia independen untuk anak-anak semuanya relevan untuk mencegah dan menanggapi bahaya yang dapat dialami anak-anak di dunia maya.

Oleh karena itu, lembaga-lembaga semacam ini harus berada di jantung pengembangan pendekatan berbasis hak yang komprehensif untuk memperkuat kerangka hukum, peraturan dan kebijakan yang mengatur perlindungan online anak, termasuk konsultasi langsung dengan anak-anak, sebagaimana hak mereka berdasarkan pasal 12 UNCRC.

Baru-baru ini, terdapat contoh yurisdiksi yang memperkenalkan atau mempertimbangkan pengenalan lembaga negara dengan mandat khusus untuk mendukung hak-hak anak di dunia maya, termasuk perlindungan mereka dari kekerasan atau bahaya. Jika terdapat lembaga semacam ini, lembaga ini juga harus dikaitkan erat dengan upaya untuk memperkuat respons terhadap perlindungan online anak di tingkat nasional.

3.2 Tanggapan yang ada untuk perlindungan online anak

Beberapa inisiatif telah dikembangkan untuk diterapkan di tingkat nasional dan internasional dalam menghadapi semakin pentingnya TIK dalam kehidupan anak-anak di seluruh dunia dan risiko yang melekat pada anak kecil di masyarakat kita.

Model nasional

Di tingkat nasional, beberapa undang-undang harus disorot karena mencakup aspek-aspek penting dari kerangka komprehensif tentang Perlindungan Online Anak. Aspek tersebut termasuk, tetapi tidak terbatas pada:

- Audiovisual Media Services Directive (AVMSD) (diulas pada 2018, EU)
- *General Data Protection Regulation* (GDPR) (2018, EU)

Terdapat perkembangan inovatif dalam respons regulasi dan kelembagaan negara-negara anggota dalam menghadapi ancaman keselamatan dan kesejahteraan anak-anak di dunia maya. Untuk mnanggapi CSAM, perundungan di dunia maya, dan bahaya lain yang dihadapi anak-anak secara online, tidak dapat menggunakan hanya satu cara, tetapi perlu dicatat bahwa terdapat pendekatan baru yang dicoba dalam beberapa tahun terakhir:

Kode Desain Sesuai Usia (2019, UK)

Pada awal 2019, Kantor Komisi Informasi menerbitkan proposal untuk 'kode desain sesuai usia' untuk perlindungan online anak lebih lanjut. Kode yang diusulkan berpusat pada kepentingan terbaik anak, sebagaimana diatur dalam UNCRC, dan menetapkan beberapa ekspektasi untuk industri. Hal ini meliputi langkah-langkah verifikasi usia yang kuat, layanan lokasi dinonaktifkan secara default untuk anak-anak, agar industri mengumpulkan dan menyimpan hanya jumlah minimum data pribadi anak-anak, agar produk aman sesuai desain dan agar penjelasan sesuai usia dan dapat diakses.

Undang-Undang Komunikasi Digital yang Berbahaya (diulas pada 2017, Selandia Baru)

Undang-undang tahun 2015 menjadikan kekerasan di dunia maya sebagai kejahatan tertentu dan berfokus pada berbagai bahaya, mulai dari perundungan di dunia maya hingga balas dendam melalui pornografi. Hal ini bertujuan untuk menghindari mencegah, dan mengurangi komunikasi digital yang berbahaya, sehingga memposting komunikasi digital dengan tujuan menyebabkan tekanan emosional yang serius kepada orang lain menjadi tindakan yang ilegal, dan menetapkan serangkaian 10 prinsip komunikasi. Hal ini membuat pengguna dapat menyampaikan aduan ke organisasi independen jika prinsip-prinsip ini dilanggar atau mengajukan perintah pengadilan terhadap *author* atau *host* komunikasi jika masalah tidak diselesaikan.

The eSafety Commissioner (2015, Australia)

eSafety Commissioner adalah lembaga pemerintah pertama di dunia yang didedikasikan khusus untuk keamanan online. Didirikan pada tahun 2015, eSafety memiliki peran yang diatur undang-undang untuk memimpin, mengoordinasikan, mendidik, dan memberi nasihat tentang masalah keamanan online untuk memastikan semua warga Australia memiliki pengalaman online yang aman, positif, dan memberdayakan. eSafety mengelola skema investigasi yang berfokus pada berbagai bahaya, termasuk perundungan serius di dunia maya terhadap anak-anak, pelecehan berbasis gambar, dan konten terlarang. Lembaga ini memiliki wewenang untuk menyelidiki dan mengambil tindakan untuk menangani aduan atau laporan yang melibatkan jenis bahaya ini – termasuk, dalam beberapa kasus, wewenang untuk mengeluarkan pemberitahuan kepada individu dan layanan online untuk menghapus materi. Di samping kewenangan investigasinya, eSafety mengadopsi pendekatan komunitas yang menyeluruh, yang mengacu pada inisiatif dan intervensi sosial, budaya dan teknologi. Upaya pencegahan, perlindungan, dan proaktifnya memberikan pendekatan komprehensif terhadap keamanan online.

Model internasional

Di tingkat internasional dan transnasional, rekomendasi dan standar telah diterbitkan oleh berbagai pemangku kepentingan. Pedoman ini dibangun di atas kerja dan upaya berikut:

Pedoman pelaksanaan Protokol Opsional pada Konvensi Hak Anak tentang Penjualan Anak, Prostitusi Anak, dan Pornografi Anak.

Pedoman Dewan Eropa untuk menghormati, melindungi, dan memenuhi hak anak di lingkungan digital[44].

Pedoman ini ditujukan kepada semua negara anggota Dewan Eropa, dengan tujuan membantu negara-negara anggota dan pemangku kepentingan terkait lainnya dalam upaya mereka untuk mengadopsi pendekatan strategis yang komprehensif dalam memaksimalkan hak anak secara penuh di lingkungan digital. Di antara banyak topik yang dibahas adalah perlindungan data personal, penyediaan konten ramah anak yang disesuaikan dengan kapasitas mereka yang berkembang, saluran bantuan dan *hotline*, kerentanan dan ketahanan, serta peran dan tanggung jawab perusahaan. Selain itu, pedoman tersebut meminta negara untuk terlibat dengan anak-anak, termasuk dalam proses pengambilan keputusan, untuk memastikan bahwa kebijakan nasional secara memadai menangani perkembangan di lingkungan digital. Pedoman saat ini tersedia dalam 19 bahasa. Pedoman akan disertai dengan versi dokumen yang ramah anak, serta Buku Pegangan untuk pembuat kebijakan, yang akan memberikan langkah-langkah nyata tentang bagaimana menerapkan pedoman tersebut.

Dewan Eropa - Konvensi Lanzarote

Konvensi Dewan Eropa tentang Perlindungan Anak dari Eksploitasi Seksual dan Pelecehan Seksual (Konvensi Lanzarote), yang mengharuskan Negara untuk menawarkan respon holistik terhadap kekerasan seksual terhadap anak, melalui "pendekatan 4ps": Pencegahan, Perlindungan, Penuntutan dan Promosi kerjasama nasional dan internasional.

[44] Council of Europe (2020), The Digital Environment,,https://www.coe.int/en/web/children/the-digital-environment. Pedoman Dewan Eropa untuk menghormati, melindungi, dan memenuhi hak anak dalam lingkungan digital adalah seperangkat standar pertama yang diadopsi oleh badan antarpemerintah. (CM/Rec, 2018).

Operasi Konvensi dalam kaitannya dengan lingkungan digital telah diklarifikasi oleh Komite Para Pihak pada Konvensi tentang Perlindungan Anak terhadap Eksploitasi Seksual dan Pelecehan Seksual ("Komite Lanzarote"), melalui adopsi sejumlah dokumen. Dokumen ini adalah: Pendapat tentang gambar dan/atau video anak yang menjurus ke seksual atau eksplisit yang dibuat, dibagikan, dan diterima oleh anak-anak (6 Juni 2019); Opini Interpretatif tentang penerapan Konvensi Lanzarote terhadap kejahatan seksual terhadap anak yang difasilitasi melalui penggunaan TIK (12 Mei 2017); Deklarasi tentang alamat web yang mengiklankan materi atau gambar pelecehan seksual terhadap anak atau pelanggaran Komite Lanzarote melakukan pemantauan terhadap pelaksanaan Konvensi: putaran pemantauan tematik kedua. Komite berfokus pada perlindungan anak terhadap eksploitasi seksual dan pelecehan seksual yang difasilitasi oleh TIK: sebuah laporan akan diterbitkan pada putaran pemantauan pada tahun 2020. Pada 2019, terdapat 46 Negara Pihak Konvensi, termasuk Tunisia – negara non-anggota pertama yang melakukan aksesi.

Pedoman Dewan Eropa lebih lanjut

Standar dan pedoman Dewan Eropa lebih lanjut berkontribusi pada pencapaian kolektif untuk kerangka kerja komprehensif yang ditujukan untuk semua pemangku kepentingan. Konvensi tentang Kejahatan Dunia Maya Dewan Eropa berisi kewajiban bagi Para Pihak untuk mengkriminalisasi serangkaian pelanggaran terkait materi pelecehan seksual anak: saat ini diratifikasi oleh 64 Negara Pihak. Dewan Eropa berfokus, antara lain, pada pemberdayaan anak-anak dan orang-orang di sekitar mereka untuk menavigasi bidang digital dengan aman. Ini dipromosikan melalui pedoman pendidikan, termasuk Buku Pegangan Literasi Internet yang direvisi sepenuhnya (2017), Buku Panduan Pendidikan Kewarganegaraan Digital (2019) dan buku petunjuk yang ditujukan untuk orang tua (Pengasuhan di era digital – Bimbingan orang tua untuk perlindungan online anak-anak dari eksploitasi seksual dan pelecehan seksual (2017); Kewarganegaraan digital…dan anak Anda – Apa yang perlu diketahui dan dilakukan setiap orang tua (2019). Terakhir, Dewan Eropa telah melakukan penelitian konsultatif dengan anak-anak sehubungan dengan hak-hak mereka di lingkungan digital - Ini adalah dunia kita: Pandangan anak-anak tentang cara melindungi hak-hak mereka di lingkungan digital (2017) dan melakukan beberapa penelitian konsultatif pertama yang berfokus pada pengalaman anak-anak penyandang disabilitas di lingkungan digital - Dua klik maju dan satu klik mundur: Laporan tentang anak-anak penyandang disabilitas di lingkungan digital (2019).

Laporan Keamanan Online Anak

Keamanan Online Anak: Meminimalkan Risiko Kekerasan, Pelecehan, dan Eksploitasi Online + Deklarasi Universal Keamanan Online Anak[45].

Rekomendasi OECD tentang Perlindungan Online Anak (2012 / Tinjauan 2019-2020) Inisiatif nasional dan transnasional lainnya harus lebih disorot sebagai dukungan kerjasama internasional serta upaya nasional untuk membangun strategi perlindungan online anak. Beberapa di antaranya seperti:

The International Child Sexual Exploitation image database

Dikelola oleh INTERPOL, the International Child Sexual Exploitation image database (ICSE DB) adalah alat intelijen dan investigasi yang kuat yang memungkinkan penyelidik khusus untuk berbagi data dengan rekan kerja di seluruh dunia. Tersedia melalui sistem komunikasi polisi global INTERPOL yang aman (dikenal sebagai I-247), ICSE DB menggunakan software perbandingan gambar yang canggih untuk membuat hubungan antara korban, pelaku, dan tempat.

ICSE DB memungkinkan pengguna bersertifikat di negara-negara anggota untuk mengakses database secara *real time*, mempertanyakan kepemilikan yang ada, mengunggah data baru, triase dan menyortir materi, dekonflik, melakukan analisis dan berkomunikasi dengan pakar lain di seluruh dunia dalam menanggapi pertanyaan terkait investigasi eksploitasi seksual anak.

The WePROTECT Global Alliance

The WePROTECT Global Alliance (WPGA) adalah gerakan global yang menyatukan pengaruh, keahlian, dan sumber daya yang diperlukan untuk mengubah cara penanganan eksploitasi seksual anak secara oline (*online child sexual exploitation* atau OSCE) di seluruh dunia. Ini adalah kemitraan antara pemerintah, perusahaan teknologi global, dan organisasi masyarakat sipil. Sifatnya yang merangkul berbagai pemangku kepentingan merupakan hal yang unik di bidang ini. Visi WePROTECT Global Alliance adalah untuk mengidentifikasi dan melindungi lebih banyak korban, menangkap lebih banyak pelaku, dan akhiri eksploitasi seksual anak secara online. WeProtect Global Alliance terdiri dari sejumlah komponen, khususnya Model Respon Nasional dan Respon Strategis Global. Detail lebih lanjut dapat ditemukan di Lampiran 3.

The 2020 Child Online Safety Index

The DQ Institute 2020 Child Online Safety Index (COSI) adalah platform analitik *real time* pertama di dunia untuk membantu negara-negara memantau status keamanan online anak-anak mereka dengan lebih baik.

COSI didasarkan pada enam pilar yang membentuk kerangka kerja COSI. Pilar satu dan dua, Risiko Siber dan Penggunaan Digital yang Disiplin, berkaitan dengan penggunaan teknologi digital secara bijak. Pilar tiga dan empat, Kompetensi Digital dan Bimbingan dan Edukasi, terkait dengan pemberdayaan. Dua pilar terakhir berkaitan dengan infrastruktur, yaitu pilar Infrastruktur Sosial dan Konektivitas.

3.3 Contoh tanggapan terhadap bahaya di dunia maya

Ada sejumlah contoh tanggapan terhadap bahaya di dunia maya di Lampiran 4. Contoh-contoh ini mencakup tanggapan edukasi, legislatif, dan identifikasi bahaya online.

3.4 Manfaat strategi nasional perlindungan online anak

Harmonisasi Hukum

Pengadopsian undang-undang yang sesuai oleh semua negara dalam melawan penyalahgunaan TIK untuk tujuan kriminal atau lainnya merupakan inti untuk mencapai keamanan siber global. Karena ancaman dapat berasal dari mana saja di seluruh dunia, tantangan tersebut pada dasarnya berada dalam lingkup internasional dan memerlukan kerja sama internasional, bantuan investigasi, dan ketentuan substantif dan prosedural umum.

[45] Broadband Commission for Sustainable Development (2019), The State of Broadband 2019: Broadband as a Foundation for Sustainable Development, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

Oleh karena itu, penting bagi negara-negara untuk menyelaraskan kerangka hukum mereka untuk memerangi kejahatan di dunia maya, melindungi anak-anak di dunia maya, dan memfasilitasi kerja sama internasional[46].

Pengembangan undang-undang nasional yang memadai, kerangka hukum kejahatan dunia maya terkait, dan melalui pendekatan ini, penyelarasan di tingkat internasional merupakan langkah kunci menuju keberhasilan setiap strategi nasional perlindungan online anak. Hal ini terutama membutuhkan ketentuan hukum pidana substantif yang diperlukan untuk mengkriminalisasi tindakan seperti penipuan komputer, akses ilegal, gangguan data, pelanggaran hak cipta dan CSAM, di saat yang sama juga menjaga agar anak-anak tidak dikriminalisasi secara berlebihan. Fakta bahwa ketentuan yang ada dalam KUHP yang berlaku untuk tindakan serupa yang dilakukan di dunia nyata tidak berarti bahwa ketentuan tersebut dapat diterapkan juga untuk tindakan yang dilakukan melalui Internet. Oleh karena itu, analisis menyeluruh terhadap undang-undang nasional saat ini sangat penting untuk mengidentifikasi kemungkinan kesenjangan. Langkah selanjutnya adalah mengidentifikasi dan mendefinisikan bahasa legislatif dan materi rujukan yang dapat membantu negara-negara dalam menetapkan hukum dan aturan prosedur kejahatan dunia maya yang selaras. Instrumen praktis tersebut dapat digunakan oleh negara-negara untuk penjabaran kerangka hukum keamanan siber dan undang-undang terkait. ITU telah bekerja dengan Negara-negara Anggota dan pemangku kepentingan yang relevan dalam arah ini dan sangat berkontribusi untuk memajukan penyelarasan undang-undang kejahatan dunia maya di seluruh dunia.

Mengingat kecepatan inovasi teknologi yang cepat, regulasi mandiri (*self-regulation*) dan regulasi bersama (*co-regulation*) telah diajukan sebagai solusi potensial terhadap usangnya peraturan yang ada dan proses legislatif yang panjang. Namun, agar efektif, pembuat peraturan/pembuat kebijakan perlu mendefinisikan dengan jelas tujuan dan tantangan tertentu dalam perlindungan online anak, menerapkan proses peninjauan dan metodologi yang jelas untuk menilai efektivitas pengaturan mandiri dan pengaturan bersama, dan jika regulasi mandiri dan regulasi bersama gagal untuk mengatasi tantangan yang diidentifikasi, memulai proses legislatif formal untuk mengatasi tantangan tersebut. Juga, langkah-langkah regulasi mandiri yang berhasil dapat secara bertahap diadopsi ke dalam hukum formal dalam proses legislatif untuk menjadi pelindung hukum dan mencegah kemunduran atau berhentinya kepatuhan terhadap inisiatif regulasi mandiri tertentu.

Koordinasi

Kemungkinan besar, di berbagai aktor dan pemangku kepentingan, sudah ada berbagai kegiatan dan tindakan yang bertujuan untuk melindungi anak-anak di dunia maya, tetapi ini upaya ini dilakukan secara terpisah. Pemahaman ini penting untuk mengapresiasi upaya yang ada dalam pengembangan strategi nasional perlindungan online anak. Strategi ini akan mengoordinasikan dan mengarahkan upaya yang ada melalui orkestrasi kegiatan yang ada dan kegiatan yang baru.

[46] Broadband Commission for Sustainable Development (2019)

4. Rekomendasi kerangka kerja dan implementasi

Pemerintah harus mengatasi semua manifestasi kekerasan terhadap anak di lingkungan digital. Namun, langkah-langkah yang diambil untuk melindungi anak-anak di lingkungan digital tidak boleh terlalu membatasi pelaksanaan hak-hak lain, seperti hak atas kebebasan berekspresi, hak untuk mengakses informasi atau hak atas kebebasan berserikat. Daripada membatasi keingintahuan dan rasa inovasi anak-anak karena takut menghadapi risiko online, sangat penting untuk memanfaatkan sumber daya anak-anak dan meningkatkan ketahanan mereka sembari mengeksplorasi potensi lingkungan digital.

Dalam banyak kasus, tindakan kekerasan terhadap anak dilakukan oleh anak lain. Dalam situasi seperti itu, pemerintah sedapat mungkin harus melakukan pendekatan restoratif yang memperbaiki kerusakan yang dilakukan, sembari mencegah kriminalisasi anak. Pemerintah harus mempromosikan penggunaan TIK dalam mencegah dan menangani kekerasan, seperti pengembangan teknologi dan sumber daya bagi anak-anak untuk mengakses informasi, memblokir materi berbahaya dan melaporkan ketika terjadi kasus kekerasan[47].

Untuk menghadapi situasi keamanan online anak global, pemerintah harus memfasilitasi komunikasi antara entitas terkait mereka dan bekerja sama secara terbuka untuk menghilangkan bahaya bagi anak-anak di dunia maya.

4.1 Rekomendasi kerangka kerja

4.1.1 Kerangka Hukum

Pemerintah harus meninjau dan, jika perlu, memperbarui kerangka hukumnya untuk mendukung realisasi penuh hak-hak anak di lingkungan digital. Kerangka hukum yang komprehensif harus membahas langkah-langkah pencegahan; pelarangan segala bentuk kekerasan terhadap anak di lingkungan digital; penyediaan pemulihan yang efektif, pemulihan dan reintegrasi untuk mengatasi pelanggaran hak-hak anak; pembentukan mekanisme konseling, pelaporan dan pengaduan yang peka anak; dan mekanisme akuntabilitas untuk melawan impunitas[48].

Bila memungkinkan, undang-undang harus netral teknologi, sehingga penerapannya tidak tergerus oleh perkembangan teknologi di masa depan[49].

Implementasi undang-undang yang efektif mengharuskan pemerintah untuk menerapkan langkah-langkah pelengkap, termasuk inisiatif peningkatan kesadaran dan mobilisasi sosial, upaya dan kampanye pendidikan, dan pengembangan kapasitas profesional yang bekerja dengan dan untuk anak-anak.

Dalam mengembangkan hukum yang tepat, penting juga untuk diingat bahwa anak-anak bukanlah kelompok yang homogen. Mungkin diperlukan tanggapan yang berbeda-beda untuk anak-anak dari kelompok usia yang berbeda-beda, serta anak-anak yang memiliki kebutuhan khusus atau yang berisiko tinggi untuk dilukai di atau melalui lingkungan digital.

[47] Special Representative of the Secretary-General on Violence against Children, *Annual Report of the Special Representative of the Secretary-General on Violence against Children to the Human Rights Council,* A/HRC/31/20 (Januari 2016), para. 103 dan 104.

[48] Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), hlm. 55.

[49] Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), hlm. 64.

Pemerintah harus menciptakan lingkungan hukum dan peraturan yang jelas dan dapat diprediksi yang mendukung bisnis dan pihak ketiga lainnya untuk memenuhi tanggung jawab mereka untuk melindungi hak-hak anak di seluruh operasi mereka, baik di dalam maupun luar negeri[50].

Aspek-aspek berikut akan membantu pembuat kebijakan dalam meninjau ruang lingkup kerangka hukum dan ketentuan berikut:

- *grooming* atau bentuk lain dari rayuan jarak jauh, pemerasan atau pemaksaan anak-anak ke dalam kontak seksual atau aktivitas seksual yang tidak pantas;
- memastikan kepemilikan, produksi dan distribusi CSAM, terlepas dari niat untuk mendistribusikan;
- pelecehan, perundungan, pelecehan, atau ujaran kebencian secara online;
- materi teroris online;
- keamanan di dunia maya;
- refleksi bahwa apa yang ilegal secara offline sama-sama ilegal secara online.

4.1.2 Kerangka kebijakan dan kelembagaan

Menjamin realisasi hak-hak anak di lingkungan digital mengharuskan pemerintah untuk menyeimbangkan antara memaksimalkan manfaat penggunaan TIK oleh anak-anak dan meminimalkan risiko yang terkait dengannya. Hal ini dapat dicapai dengan memasukkan langkah-langkah untuk melindungi anak-anak di dunia maya dalam rencana *broadband* nasional[51] dan dengan mengembangkan beragam strategi perlindungan online anak yang tersendiri. Agenda tersebut harus sepenuhnya terintegrasi dengan kerangka kebijakan yang ada yang relevan dengan hak-hak anak atau perlindungan anak dan selanjutnya harus melengkapi kebijakan perlindungan anak nasional dengan menawarkan kerangka kerja khusus untuk semua risiko dan potensi bahaya bagi anak-anak yang bertujuan untuk menciptakan lingkungan digital yang aman, inklusif dan memberdayakan[52].

Pemerintah harus memiliki kerangka koordinasi nasional dengan mandat yang jelas dan kewenangan yang memadai untuk mengkoordinasikan semua kegiatan yang terkait dengan hak anak dan media digital dan TIK di tingkat lintas sektor, nasional, regional, dan lokal. Pemerintah harus memasukkan tujuan yang terikat waktu dan proses yang transparan untuk mengevaluasi dan memantau kemajuannya dan harus memastikan ketersedian sumber daya manusia, teknis dan keuangan yang diperlukan untuk efektivitas operasi kerangka kerja ini[53].

Pemerintah harus membangun platform *multi-stakeholder* untuk mengarahkan pengembangan, implementasi dan pemantauan agenda digital nasional untuk anak-anak. Platform semacam ini harus menyatukan perwakilan dari konstituen yang paling penting, termasuk: anak-anak dan remaja; asosiasi orang tua/pengasuh; bagian pemerintah terkait; sektor pendidikan, keadilan, kesehatan dan kepedulian sosial; lembaga hak asasi manusia nasional dan badan regulator terkait; masyarakat sipil; industri; akademisi; dan asosiasi profesi terkait.

---

[50] UN Committee on the Rights of the Child, *General Comment No. 16*, para. 53.

[51] The State of the Broadband 2019, Recommendation 5.6, halaman 78. https://www.itu.int/dms_pub/itu-s/opb/ pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

[52] Untuk ketentuan model tentang perlindungan anak untuk rencana broadband nasional, lihat bab 10 Laporan Keamanan Online Anak.

[53] Special Representative of the Secretary-General on Violence against Children, *Annual Report of the Special Representative of the Secretary-General on Violence against Children* (Desember 2014) A/HRC/28/55 and *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), para. 88.

4.1.3 Kerangka peraturan

Pemerintah bertanggung jawab atas pelanggaran hak anak yang disebabkan atau disumbangkan oleh perusahaan ketika gagal melakukan tindakan yang diperlukan, tepat dan wajar untuk mencegah dan memperbaiki pelanggaran tersebut atau dengan cara lain bekerja sama dengan atau menoleransi pelanggaran tersebut[54].

Prinsip Panduan Bisnis dan Hak Asasi Manusia mengantisipasi bahwa perusahaan harus menyediakan mekanisme pemulihan dan pengaduan yang sah, dapat diakses, dapat diprediksi, adil, sesuai dengan hak, transparan, berdasarkan dialog dan keterlibatan, dan sumber pembelajaran berkelanjutan. Mekanisme pengaduan yang dibentuk oleh perusahaan dapat memberikan solusi alternatif yang fleksibel dan tepat waktu dan kadang-kadang mungkin demi kepentingan terbaik anak untuk masalah yang diangkat terkait perilaku perusahaan untuk diselesaikan melalui mekanisme tersebut. Dalam semua kasus, akses ke pengadilan atau tinjauan yudisial atas pemulihan administratif dan prosedur lainnya harus tersedia[55]. Pertimbangan harus diberikan pada mekanisme yang menciptakan layanan yang aman dan sesuai usia bagi anak-anak bagi pengguna untuk melaporkan kekhawatiran mereka.

Terlepas dari adanya mekanisme pengaduan internal, pemerintah harus menetapkan mekanisme pemantauan untuk penyelidikan dan pemulihan pelanggaran hak anak, dengan tujuan untuk meningkatkan akuntabilitas TIK dan perusahaan terkait lainnya, serta memperkuat tanggung jawab badan pengatur untuk pengembangan standar yang relevan dengan hak anak dan TIK[56]. Hal ini sangat penting karena pemulihan lain yang tersedia bagi mereka yang terkena dampak buruk oleh aksi korporasi – seperti proses perdata dan ganti rugi yudisial lainnya – seringkali tidak praktis dan mahal[57].

Komite PBB tentang Hak Anak telah menyoroti potensi peran lembaga hak asasi manusia nasional di bidang ini, dengan menguraikan bagaimana mereka dapat berperan dalam menerima, menyelidiki dan menengahi pengaduan pelanggaran oleh entitas industri; melakukan penyelidikan publik terhadap pelanggaran skala besar; dan melakukan tinjauan legislatif untuk memastikan kepatuhan terhadap Konvensi Hak Anak. Komite telah mengindikasikan bahwa, jika perlu, "Negara-negara harus memperluas mandat legislatif dari lembaga-lembaga hak asasi manusia nasional untuk mengakomodasi hak-hak anak dan bisnis". Sangat penting bahwa setiap mekanisme pengaduan harus peka terhadap anak, memastikan privasi dan perlindungan korban, dan melakukan kegiatan pemantauan, tindak lanjut dan verifikasi untuk korban anak.

Salah satu contoh area di mana lembaga hak asasi manusia nasional atau badan regulator lainnya dapat memberikan pemulihan yang efektif untuk anak-anak adalah dalam kasus perundungan di dunia maya. Mekanisme pemulihan internal dan pengaduan terkadang terbukti tidak efektif dalam kasus tersebut karena, meskipun kontennya menyedihkan dan berbahaya, seringkali tidak ditangani oleh undang-undang nasional dan tidak ada dasar yang jelas untuk meminta penghapusan konten kepada *host*.

---

54 UN Committee on the Rights of the Child, *General Comment No.* 16, para. 28.
55 Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, A/HRC/17/31 (2011), para. 71.
56 UN Committee on the Rights of the Child, *Report of the 2014 Day of General Discussion*, para. 96.
57 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (2016), para. 71.

Memberdayakan otoritas publik untuk menerima keluhan terkait kasus perundungan di dunia maya dan untuk menengahi dengan *host* konten agar materi yang relevan dihapus akan menjadi perlindungan penting bagi anak-anak[58]. Ini akan memiliki keuntungan dalam memberikanrespon yang cepat – yang sangat penting dalam konteks perundungan di dunia maya – dan juga dasar hukum yang jelas untuk mengatasi penghapusan materi perundungan di dunia maya.

Dalam membingkai pendekatannya terhadap regulasi lingkungan digital, pemerintah juga harus menyadari dampak regulasi tersebut terhadap penikmatan semua hak asasi manusia, termasuk kebebasan berekspresi[59].

Pemerintah harus mewajibkan bisnis untuk melakukan uji tuntas hak-hak anak. Ini akan memastikan bahwa perusahaan mengidentifikasi, mencegah dan mengurangi dampaknya terhadap hak-hak anak termasuk di seluruh relasi bisnis mereka dan dalam operasi global[60].

Selain itu, pemerintah harus mempertimbangkan langkah-langkah pelengkap seperti memastikan bahwa entitas industri yang kegiatannya dapat berdampak pada hak-hak anak di lingkungan digital harus mematuhi standar tertinggi dalam hal mencegah dan menanggapi potensi pelanggaran hak agar memenuhi syarat untuk mendapatkan pendanaan atau memenangkan kontrak.

4.2 Rekomendasi implementasi

Pemerintah harus memastikan akses terhadap pemulihan yang efektif bagi anak-anak korban pelanggaran hak, termasuk bantuan untuk mencari ganti rugi yang cepat dan tepat atas kerugian yang diderita, melalui kompensasi jika sesuai. Pemerintah juga harus memberikan dukungan dan bantuan yang memadai bagi anak korban pelanggaran terkait media digital dan TIK, termasuk layanan komprehensif untuk memastikan pemulihan dan reintegrasi anak secara penuh, dan mencegah reviktimisasi korban anak[61].

Konseling yang peka anak, aman dan mudah diakses, mekanisme pelaporan dan pengaduan, seperti saluran bantuan, harus ditetapkan oleh undang-undang dan harus menjadi bagian dari sistem perlindungan anak nasional. Penting untuk memastikan bahwa layanan ini terhubung ke layanan regulasi mana pun untuk membantu merampingkan interaksi anak dengan badan institusional ketika mereka mungkin sedang mengalami kesulitan. Saluran bantuan sangat berharga ketika menghadapi masalah yang sangat sensitif, seperti pelecehan seksual, yang mungkin sulit didiskusikan oleh anak-anak dengan teman sebaya, orang tua, pengasuh, atau guru. Saluran bantuan juga memainkan peran penting dalam mengarahkan anak-anak ke layanan seperti layanan hukum, rumah aman, penegakan hukum atau rehabilitasi[62].

Selain itu, pemerintah perlu memahami dan melacak perilaku pelaku untuk meningkatkan tingkat deteksi pelaku dan mengurangi risiko pelaku yang telah dihukum kembali menjalankan aksinya. Membangun saluran bantuan yang menawarkan konseling dan dukungan telepon atau chat gratis dan anonim untuk orang-orang yang mengalami perasaan atau pikiran tentang minat seksual pada anak-anak – calon pelaku.

---

58 Bertrand de Crombrugghe, "Report of the Human Rights Council on Its Thirty-First Session" (UN Human Rights Council, 2016

59 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (2016), para. 45.

60 UN Committee on the Rights of the Child, *General Comment No. 16*, para. 62.

61 UN Committee on the Rights of the Child, *Report of the 2014 Day of General Discussion*, para. 106.

62 Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks*, hlm. 51 dan hlm. 65.

Membantu pelaku mengubah perilaku mereka meminimalkan risiko kembali melakukan kejahatan.Mekanisme penanganan pengaduan yang sah juga merupakan bagian penting dari kerangka kerja untuk pemulihan yang efektif.

Regulator harus melakukan pengukuran dan studi independen untuk menilai bagaimana platform melaporkan dan menangani masalah yang berkaitan dengan perlindungan anak.

Terdapat teknologi bagi regulator untuk memantau platform secara independen. Penyedia industri harus didukung untuk mempublikasikan laporan transparansi.

Bersama dengan komunitas internasional dan industri, pemerintah harus mengembangkan seperangkat metrik universal yang dapat digunakan pemangku kepentingan untuk mengukur semua aspek keamanan online anak yang relevan.

4.2.1 Eksploitasi seksual

Pertimbangan konkret bagi pembuat kebijakan ketika mempertimbangkan ancaman bahaya terhadap anak-anak, khususnya materi pelecehan seksual terhadap anak, konten yang dibuat sendiri, *grooming* dan pemerasan seksual serta risiko online lainnya. Hal ini dapat meliputi:

- Langkah-langkah untuk mendisrupsi atau mengurangi lalu lintas di CSAM, misalnya dengan membuat *hotline* nasional atau Portal Pelaporan IWF, dan dengan menerapkan langkah-langkah untuk memblokir akses ke konten online yang diketahui mengandung atau mengiklankan ketersediaan CSAM.
- Memastikan adanya proses nasional untuk memastikan semua CSAM yang ditemukan di suatu negara disalurkan ke sumber daya nasional yang terpusat yang memiliki kekuatan legislatif untuk mengarahkan perusahaan agar menghapus konten.
- Strategi untuk mengatasi permintaan CSAM terutama di antara mereka yang memiliki keyakinan untuk pelanggaran tersebut. Penting untuk membangun kesadaran akan fakta bahwa ini bukan kejahatan tanpa korban: anak-anak dilecehkan untuk menghasilkan materi yang dilihat dan dengan sengaja melihat atau mengunduh CSAM, seseorang berkontribusi langsung pada pelecehan anak yang digambarkan dan yang lainnya juga mendorong kekerasan lebih banyak anak untuk menghasilkan lebih banyak gambar.
- Membangun kesadaran akan fakta bahwa anak-anak tidak akan pernah setuju untuk dilecehkan secara seksual, baik untuk produksi CSAM atau dengan cara lain. Dorong orang yang menggunakan CSAM untuk mencari bantuan, sementara pada saat yang sama, buat mereka sadar bahwa mereka akan dimintai pertanggungjawaban pidana atas aktivitas ilegal yang mereka lakukan.
- Strategi lain untuk mengatasi permintaan CSAM. Misalnya, beberapa negara memiliki daftar terpidana pelaku kejahatan seksual. Pengadilan telah mengeluarkan perintah pengadilan yang melarang pelaku menggunakan Internet sama sekali atau menggunakan bagian dari Internet yang sering dikunjungi oleh anak-anak dan remaja. Masalah dengan perintah ini sampai sekarang adalah salah satu penegakannya. Namun, di beberapa negara, pertimbangan diberikan untuk mengintegrasikan daftar pelaku yang diketahui ke dalam daftar blokir yang akan mencegah orang-orang yang ada di dalamnya untuk mengunjungi atau bergabung dengan situs web tertentu, misalnya situs web yang diketahui dikunjungi oleh sejumlah besar anak-anak dan anak muda. Tentu saja, jika pelaku bergabung dengan situs web saat menggunakan nama yang berbeda atau login palsu, efektivitas tindakan tersebut dapat sangat dikurangi tetapi dengan mengkriminalisasi perilaku ini, pencegahan lebih lanjut dapat dilakukan.

- Memberikan dukungan jangka panjang yang sesuai untuk para korban. Jika anak-anak atau remaja telah menjadi korban online, di mana misalnya gambar ilegal mereka telah muncul di Internet, mereka secara alami akan merasa sangat khawatir tentang siapa yang mungkin telah melihatnya dan apa dampaknya terhadap mereka. Hal ini bisa membuat anak atau remaja merasa rentan terhadap perundungan atau eksploitasi dan pelecehan seksual lebih lanjut. Dalam konteks ini, penting untuk menyediakan layanan dukungan profesional untuk mendukung anak-anak dan remaja yang berada dalam situasi seperti ini. Dukungan semacam itu mungkin perlu diberikan dalam jangka panjang.
- Memastikan bahwa mekanisme dibuat dan dipromosikan secara luas untuk menyediakan sarana yang mudah dipahami dan cepat untuk melaporkan konten ilegal atau perilaku online ilegal atau mengkhawatirkan, misalnya sistem yang serupa dengan yang telah ditetapkan oleh Virtual Global Taskforce and INHOPE. Penggunaan sistem INTERPOL i24/7 harus didorong.
- Memastikan bahwa cukup banyak petugas penegak hukum yang terlatih dengan baik dalam menyelidiki Internet dan kejahatan berbasis komputer dan memiliki akses ke fasilitas forensik yang sesuai untuk memungkinkan mereka mengekstrak dan menafsirkan data digital yang relevan.
- Berinvestasi untuk melatih penegak hukum, kejaksaan dan otoritas peradilan terkait metode yang digunakan oleh penjahat online untuk melakukan kejahatan ini. Investasi juga akan diperlukan dalam memperoleh dan memelihara fasilitas yang diperlukan untuk memperoleh dan menafsirkan bukti forensik dari perangkat digital. Selain itu, penting untuk menjalin kerjasama bilateral dan multilateral dan pertukaran informasi dengan otoritas penegak hukum dan badan investigasi yang relevan di negara lain.

4.2.2 Pendidikan

Mendidik anak-anak tentang literasi digital sebagai bagian dari strategi untuk memastikan mereka mendapatkan manfaat dari teknologi, bebas dari bahaya. Ini akan memungkinkan anak-anak untuk mengembangkan keterampilan berpikir kritis yang akan membantu mereka mengidentifikasi dan memahami sisi baik dan buruk dari perilaku mereka di ruang digital. Meskipun penting untuk menggambarkan kepada anak-anak bahaya yang dapat terjadi di dunia maya, ini hanya akan efektif jika dimasukkan sebagai bagian dari program literasi digital yang lebih luas yang harus sesuai dengan usia anak dan fokus pada keterampilan dan kompetensi. Penting untuk memasukkan konsep pembelajaran sosial dan emosional dalam pendidikan keamanan online karena ini akan mendukung pemahaman dan pengelolaan emosi siswa untuk memiliki hubungan yang sehat dan saling menghormati, baik online maupun offline.

Anak-anak harus memiliki alat dan pengetahuan yang tepat untuk mengatasi Internet sebagai salah satu cara terbaik untuk menjaga mereka tetap aman. Memperkenalkan literasi digital dalam kurikulum sekolah adalah salah satu caranya. Cara lainnya adalah dengan menciptakan sumber daya pendidikan di luar kurikulum sekolah.

Mereka yang bekerja dengan anak-anak harus memiliki pengetahuan dan keterampilan yang sesuai untuk mendukung anak-anak agar percaya diri dalam menanggapi dan menyelesaikan masalah terkait perlindungan online anak serta memberikan keterampilan digital yang diperlukan kepada anak-anak agar mereka berhasil memanfaatkan teknologi.

4.2.3 Industri

Pelaku industri nasional dan internasional harus berupaya untuk meningkatkan kesadaran tentang masalah seputar keamanan online anak dan membantu semua orang dewasa yang bertanggung jawab atas kesejahteraan anak, termasuk orang tua dan pengasuh, sekolah, organisasi dan komunitas yang melayani pemuda, mengembangkan pengetahuan dan keterampilan yang mereka butuhkan untuk menjaga anak-anak tetap aman. Industri harus mengadopsi pendekatan desain yang lebih aman untuk produk, layanan, dan platform mereka, dengan mengakui keselamatan sebagai tujuan intinya.

- Menyediakan *tools* ramah keluarga yang sesuai dengan usia untuk membantu penggunanya mengelola perlindungan keluarga mereka secara online dengan lebih baik.

- Menyediakan mekanisme pelaporan yang sesuai bagi penggunanya untuk melaporkan masalah dan kekhawatiran. Pengguna harus berekspektasi akan mendapat tanggapan yang tepat waktu atas laporan ini dengan informasi tentang tindakan yang diambil dan, jika berlaku, di mana pengguna dapat memperoleh dukungan lebih lanjut.
- Selain itu, berikan pelaporan proaktif tentang pelecehan terhadap anak untuk mendeteksi dan menangani segala bentuk pelecehan (yang diklasifikasikan sebagai aktivitas kriminal) terhadap anak. Praktik ini menunjukkan bahwa jika semua pemangku kepentingan berkontribusi untuk mendeteksi, memblokir, dan melaporkan, kita dapat berpikir untuk memiliki Internet yang lebih bersih dan aman untuk semua. Industri harus mempertimbangkan untuk mengambil semua *tools* yang relevan untuk mencegah platform mereka dieksploitasi, seperti Layanan IWF.

Sangat penting untuk melibatkan semua aktor yang relevan dalam ekosistem agar mereka menyadari risiko dan bahaya online untuk dapat mencegah anak-anak terpapar risiko yang tidak perlu.

Mengembangkan metrik bersama untuk keamanan online anak untuk mengukur semua aspek terkait masalah tersebut. Standar dan metrik bersama adalah satu-satunya cara untuk melacak kemajuan di negara-negara dan untuk menentukan keberhasilan proyek dan kegiatan yang dilaksanakan untuk menghapus kekerasan terhadap anak dan mengakui kekuatan ekosistem keamanan online anak.

5. Mengembangkan strategi nasional perlindungan online anak

5.1 Ceklis nasional

Untuk merumuskan strategi nasional yang berfokus pada keamanan online anak, pembuat kebijakan perlu mempertimbangkan berbagai strategi. Tabel 1 menjelaskan area utama untuk dipertimbangkan.

Tabel 1: Area kunci untuk dipertimbangkan

	#	Area kunci untuk dipertimbangkan	Keterangan lebih lanjut
Kerangka hukum	1	Tinjau kerangka hukum yang ada untuk menentukan bahwa semua kekuatan hukum yang diperlukan ada untuk memungkinkan penegakan hukum dan lembaga terkait lainnya untuk melindungi orang di bawah usia 18 tahun secara online di semua platform yang menggunakan Internet.	Secara umum akan diperlukan adanya suatu badan hukum yang menjelaskan bahwa suatu dan setiap kejahatan yang dapat dilakukan terhadap anak di dunia nyata juga dapat, secara *mutatis mutandis*, dilakukan di Internet atau di jaringan elektronik lainnya. Mungkin juga perlu untuk mengembangkan undang-undang baru atau mengadaptasi yang sudah ada untuk melarang jenis perilaku tertentu yang hanya dapat terjadi di Internet, misalnya bujukan jarak jauh anak-anak untuk melakukan atau menonton tindakan seksual, atau *grooming* anak-anak untuk bertemu di dunia nyata untuk tujuan seksual. Sebagai tambahan untuk tujuan ini, umumnya akan diperlukan kerangka hukum yang melarang penyalahgunaan komputer untuk tujuan kriminal, melarang peretasan atau penggunaan kode komputer berbahaya atau non-konsensual lainnya dan menetapkan bahwa Internet adalah sebuah tempat di mana kejahatan dapat dilakukan.
	2	Menetapkan, secara *mutatis mutandis,* bahwa setiap tindakan terhadap anak yang ilegal di dunia nyata adalah ilegal secara online dan bahwa perlindungan data online dan aturan privasi untuk anak-anak juga cukup memadai.	

	#	Area kunci untuk dipertimbangkan	Keterangan lebih lanjut
Kerangka peraturan	3	Pertimbangkan pengembangan kebijakan regulasi. Ini mungkin termasuk pengembangan regulasi mandiri atau regulasi bersama serta sebuah kerangka peraturan sepenuhnya. Model regulasi mandiri atau atau regulasi bersama dapat mencakup perumusan dan publikasi kode praktik yang baik atau harapan keamanan online dasar, baik dalam hal membantu melibatkan, mengkoordinasikan atau mengatur dan mempertahankan keterlibatan semua pemangku kepentingan yang relevan dan dalam hal meningkatkan kecepatan di mana tanggapan yang tepat terhadap perubahan teknologi dapat dirumuskan dan diterapkan. Sebuah model peraturan dapat mendefinisikan harapan dan kewajiban di seluruh pemangku kepentingan dan mengabadikannya dalam konteks hukum. Hukuman untuk pelanggaran kebijakan juga dapat dipertimbangkan.	Beberapa negara telah menetapkan model pengaturan sendiri atau bersama dalam kaitannya dengan pengembangan kebijakan di bidang ini dan melalui model tersebut, mereka telah, misalnya, menerbitkan kode praktik yang baik untuk memandu industri Internet dalam hal langkah-langkah yang dapat bekerja paling baik ketika datang untuk menjaga anak-anak dan remaja lebih aman saat online. Misalnya di Uni Eropa di mana kode di seluruh UE telah diterbitkan baik untuk situs jejaring sosial dan jaringan telepon seluler sehubungan dengan penyediaan konten dan layanan kepada anak-anak dan remaja melalui jaringan mereka. Regulasi mandiri dan regulasi bersama dapat lebih gesit dalam hal meningkatkan kecepatan respon yang tepat terhadap perubahan teknologi dapat dirumuskan dan diterapkan. Baru-baru ini beberapa negara telah mengembangkan dan/atau menerapkan kerangka peraturan. Dalam contoh ini, kerangka peraturan telah muncul dari model regulasi mandiri atau regulasi bersama dan mendefinisikan persyaratan dan harapan bagi pemangku kepentingan, terutama penyedia industri, untuk melindungi pengguna mereka dengan lebih baik.

	#	Area kunci untuk dipertimbangkan	Keterangan lebih lanjut
Pelaporan - konten ilegal	4	Pastikan bahwa mekanisme telah ditetapkan dan dipromosikan secara luas untuk menyediakan sarana yang mudah dipahami untuk melaporkan berbagai konten ilegal yang ditemukan di Internet. Misalnya, *hotline* nasional, yang memiliki kapasitas untuk merespons dengan cepat dan menghapus atau membuat materi ilegal tidak dapat diakses. Industri harus memiliki mekanisme untuk mengidentifikasi, memblokir dan menghapus pelecehan anak secara online, mengambil semua layanan yang relevan dengan organisasi mereka.	Mekanisme untuk melaporkan penyalahgunaan layanan online atau untuk melaporkan perilaku yang tidak pantas atau ilegal secara online, misalnya ke *hotline* nasional, harus diiklankan dan dipromosikan secara luas baik di Internet maupun di media lain. Jika tidak ada *hotline* nasional, IWF menawarkan solusi Portal Pelaporan. Tautan untuk melaporkan mekanisme penyalahgunaan harus ditampilkan dengan jelas di bagian yang relevan dari situs web mana pun yang memungkinkan konten buatan pengguna muncul. Seharusnya juga memungkinkan bagi orang yang merasa terancam dengan cara apa pun, atau orang yang telah menyaksikan aktivitas yang mengkhawatirkan di Internet, untuk dapat melaporkannya secepat mungkin ke lembaga penegak hukum terkait yang perlu dilatih dan siap untuk merespon. Virtual Global Taskforce adalah badan penegak hukum yang menyediakan mekanisme 24/7 untuk menerima laporan tentang perilaku atau konten ilegal dari orang-orang di AS, Kanada, Australia, dan Italia, dengan negara-negara lain diharapkan segera bergabung. Lihat www.virtualglobaltaskforce.com. Lihat juga INHOPE.
Pelaporan - kekhawatiran pengguna	5	Industri harus memberi pengguna kesempatan untuk melaporkan kekhawatiran dan masalah kepada pengguna mereka dan meresponsnya dengan tepat.	Penyedia harus diwajibkan untuk menyediakan, dan memberi tanda dengan jelas, pengguna mereka dengan kemampuan untuk melaporkan masalah dan masalah dalam layanan mereka. Hal-hal ini harus ramah anak dan siap tersedia.

	#	Area kunci untuk dipertimbangkan	Keterangan lebih lanjut
Aktor dan pemangku kepentingan	6	Libatkan semua pemangku kepentingan terkait yang berkepentingan dengan perlindungan online anak, khususnya: • Agensi pemerintahan • Penegak hukum • Organisasi layanan sosial • Penyedia Layanan Internet (ISP) dan Penyedia Layanan Elektronik (ESP) lainnya • Penyedia jaringan telepon seluler • Penyedia Wi-Fi publik • Perusahaan *hi-tech* lain yang relevan • Organisasi guru • Organisasi wali murid • Anak-anak dan remaja • Perlindungan anak dan LSM terkait lainnya • Komunitas akademik dan penelitian • Pemilik warnet dan penyedia akses publik lainnya, misalnya perpustakaan, telecenter, PC Bang,[63] dan pusat game online dll.	Beberapa pemerintah nasional merasakan manfaat untuk menyatukan semua pemangku kepentingan dan pemain utama untuk fokus pada pengembangan dan penerapan inisiatif nasional seputar menjadikan Internet sebagai tempat yang lebih aman bagi anak-anak dan remaja, dan meningkatkan kesadaran akan masalah tersebut dan cara menanganinya dengan cara yang sangat praktis. Penting dalam strategi ini untuk menyadari bahwa banyak orang yang secara universal dan terus-menerus terhubung ke Internet melalui berbagai perangkat. Operator *broadband*, seluler, dan Wi-Fi perlu dilibatkan. Selain itu, jaringan perpustakaan umum, telecenter dan kafe internet di banyak negara dapat menjadi sumber penting akses Internet, terutama bagi anak-anak dan remaja.
Penelitian	7	Melakukan penelitian spektrum aktor-aktor dan pemangku kepentingan nasional untuk menentukan pendapat, pengalaman, keprihatinan, dan peluang mereka terkait dengan perlindungan online anak. Ini juga harus mempertimbangkan sejauh mana tanggung jawab bersama dengan kegiatan yang ada atau yang direncanakan untuk melindungi anak-anak secara online.	

[63] "PC Bang" adalah istilah yang umum digunakan di Republik Korea dan di beberapa negara lain untuk menggambarkan sebuah ruangan besar di mana LAN memfasilitasi permainan game skala besar, baik online atau antar pemain di dalam ruangan.

	#	Area kunci untuk dipertimbangkan	Keterangan lebih lanjut
Pendidikan literasi dan kompetensi digital	8	Kembangkan fitur literasi digital sebagai bagian dari kurikulum sekolah nasional yang sesuai usia dan berlaku untuk semua anak.	Sekolah dan sistem pendidikan secara umum akan mewakili fondasi komponen pendidikan dan literasi digital dari strategi nasional perlindungan online anak. Setiap kurikulum sekolah nasional harus mencakup aspek perlindungan online anak dan bertujuan untuk memberikan anak-anak dari segala usia keterampilan yang sesuai dengan usia untuk mendapatkan manfaat dan keberhasilan menggunakan teknologi dan peka terhadap ancaman dan bahaya yang harus berhasil dihindari. Aspek itu harus mengenali dan menghargai perilaku online yang positif dan konstruktif. Dalam kampanye pendidikan dan kesadaran apa pun, penting untuk mencapai nuansa yang tepat. Pesan berbasis rasa takut harus dihindari, dan keunggulan harus diberikan pada banyak fitur positif dan menyenangkan dari teknologi baru. Internet memiliki potensi besar sebagai sarana untuk memberdayakan anak-anak dan remaja untuk menemukan dunia baru. Mengajarkan bentuk perilaku online yang positif dan bertanggung jawab adalah tujuan utama dari program pendidikan dan kesadaran. Mereka yang bekerja dengan anak-anak, terutama guru, harus dilatih dan diperlengkapi dengan tepat agar berhasil mendidik dan membekali anak-anak dengan keterampilan ini. Mereka harus memahami ancaman dan bahaya online bersama-sama dengan kemampuan untuk mengenali tanda-tanda pelecehan dan bahaya dengan yakin, dan untuk menanggapi dan melaporkan kekhawatiran ini untuk melindungi anak-anak mereka.

	#	Area kunci untuk dipertimbangkan	Keterangan lebih lanjut
Sumber daya pendidikan	9	Manfaatkan pengetahuan dan pengalaman semua pemangku kepentingan dan kembangkan pesan dan materi keamanan Internet yang mencerminkan norma dan hukum budaya lokal dan pastikan bahwa ini didistribusikan secara efisien dan disajikan dengan tepat kepada semua target audiens utama. Pertimbangkan untuk meminta bantuan media massa dalam mempromosikan pesan kesadaran. Kembangkan materi yang menekankan aspek positif dan pemberdayaan Internet untuk anak-anak dan remaja dan menghindari pesan berbasis rasa takut. Promosikan bentuk perilaku online yang positif dan bertanggung jawab. Pertimbangkan untuk mengembangkan sumber daya untuk membantu orang tua menilai keamanan online anak-anak mereka sendiri dan belajar tentang cara meminimalkan risiko dan memaksimalkan potensi keluarga mereka sendiri melalui pendidikan yang ditargetkan.	Saat memproduksi materi pendidikan, penting untuk diingat bahwa banyak orang yang baru mengenal teknologi tidak akan merasa nyaman menggunakannya. Oleh karena itu, penting untuk memastikan bahwa materi keselamatan tersedia dalam bentuk tertulis atau diproduksi dengan menggunakan media lain yang lebih familiar bagi pendatang baru, misalnya, dengan video. Banyak perusahaan Internet besar memproduksi situs web yang berisi banyak informasi tentang isu-isu online untuk anak-anak dan remaja. Namun, seringkali materi ini hanya tersedia dalam bahasa Inggris atau kelompok bahasa yang sangat terbatas. Oleh karena itu, sangat penting agar materi diproduksi secara lokal yang mencerminkan hukum dan norma budaya setempat. Hal ini penting untuk kampanye keamanan Internet atau materi pelatihan apa pun yang dikembangkan.
Perlindungan anak	10	Pastikan bahwa ada mekanisme perlindungan anak yang universal dan sistematis yang mewajibkan semua orang yang bekerja dengan anak-anak (perawatan sosial, kesehatan, sekolah, dll.) untuk mengidentifikasi, menanggapi, dan melaporkan insiden pelecehan dan bahaya yang terjadi secara online.	Sebuah sistem perlindungan anak universal harus ada dan berlaku untuk semua orang yang bekerja dengan anak-anak, mewajibkan mereka untuk melaporkan pelecehan atau kekerasan anak untuk memungkinkan situasi tersebut diselidiki dan diselesaikan.

	#	Area kunci untuk dipertimbangkan	Keterangan lebih lanjut
Kesadaran nasional	11	Lakukan kampanye kesadaran nasional untuk menciptakan peluang untuk menyoroti masalah perlindungan online anak secara universal. Mungkin bisa dilakukan dengan memanfaatkan kampanye global seperti Hari Internet Lebih Aman (*Safer Internet Day*) untuk membangun kampanye.	Orang tua, wali, dan profesional, seperti guru, memiliki peran penting dalam membantu menjaga anak-anak dan remaja lebih aman saat online. Program pendukung harus dikembangkan yang membantu membangun kesadaran akan masalah ini dan juga menyediakan strategi untuk menghadapinya. Pertimbangan juga harus diberikan untuk meminta bantuan media massa dalam mempromosikan pesan dan kampanye kesadaran. Kesempatan seperti *Safer Internet Day* akan membantu dalam merangsang dan mendorong dialog nasional tentang perlindungan online anak. Banyak negara telah berhasil membangun kampanye kesadaran nasional yang berlabuh di sekitar *Safer Internet Day* dan melibatkan berbagai aktor dan pemangku kepentingan dalam memperkuat pesan universal di seluruh media dan media sosial.

	#	Area kunci untuk dipertimbangkan	Keterangan lebih lanjut
Alat, layanan, dan pengaturan	12	Pertimbangkan peran pengaturan perangkat, alat teknis (seperti program pemfilteran), serta aplikasi dan pengaturan perlindungan anak yang dapat membantu. Dorong pengguna untuk bertanggung jawab atas perangkat mereka dengan mendorong pembaruan sistem operasi ditambah penggunaan perangkat lunak dan aplikasi keamanan yang sesuai.	Ada beberapa layanan yang tersedia yang dapat membantu menyaring materi yang tidak diinginkan atau memblokir kontak yang tidak diinginkan. Beberapa program keamanan dan filter anak ini mungkin pada dasarnya gratis karena merupakan bagian dari sistem operasi komputer atau disediakan sebagai bagian dari paket yang tersedia dari ISP atau ESP. Pabrikan dari beberapa konsol game juga menyediakan alat serupa jika perangkat tersebut mendukung Internet. Program-program ini belum tentu mudah digunakan namun dapat memberikan tingkat dukungan awal, terutama dalam keluarga dengan anak-anak yang lebih kecil. Sebagian besar perangkat dilengkapi dengan pengaturan yang membantu melindungi anak-anak dan juga mempromosikan penggunaan yang sehat dan seimbang. Ini meluas ke mekanisme yang memungkinkan orang tua untuk mengelola perangkat anak-anak mereka, mengalokasikan waktu, aplikasi dan layanan yang dapat mereka gunakan dan mengelola pembelian. Baru-baru ini laporan dan pengaturan telah dikembangkan untuk memungkinkan pengguna dan orang tua untuk lebih memahami dan mengelola durasi layar dan akses. Alat teknis ini harus digunakan sebagai bagian dari arsenal yang lebih luas. Keterlibatan orang tua dan/atau wali sangat penting. Ketika anak-anak mulai sedikit lebih besar, mereka akan menginginkan lebih banyak privasi dan mereka juga akan merasakan keinginan yang kuat untuk mulai menjelajah sendiri. Selain itu, pada hubungan penagihan antara vendor dan pelanggan, proses verifikasi usia dapat memainkan peran yang sangat berharga dalam membantu vendor barang dan jasa yang dibatasi usia atau penerbit materi yang ditujukan hanya untuk audiens pada atau di atas usia tertentu, untuk menjangkau audiens tertentu. Jika tidak ada hubungan penagihan, penggunaan teknologi verifikasi usia menjadi problematik atau di banyak negara, itu tidak dimungkinkan karena kurangnya sumber data yang dapat diandalkan.

5.2 Contoh pertanyaan

Dengan mengidentifikasi pemangku kepentingan dan aktor nasional, pertanyaan berikut dapat diedarkan kepada pemangku kepentingan dan aktor dan mengundang mereka untuk dilengkapi dan ditanggapi. Tanggapan mereka akan membantu menentukan tingkat cakupan kebijakan, kekuatan serta area yang menjadi fokus di seluruh ceklis nasional.

- Sejauh mana keamanan online dan hak anak-anak menjadi tanggung jawab Anda?
- Bagaimana keamanan online dan hak-hak anak diintegrasikan ke dalam kebijakan Anda dan proses yang ada?
- Sejauh mana keamanan online tercakup dalam undang-undang yang ada?
- Apa prioritas keamanan online Anda?
- Aktivitas apa yang Anda miliki untuk mendukung keamanan online?
- Bagaimana Anda bekerja dengan agensi dan organisasi lain untuk meningkatkan/mempromosikan keamanan online?
- Dapatkah anak-anak/orang tua melaporkan masalah atau isu keamanan online kepada Anda?
- Apa tiga tantangan utama Anda di dunia online?
- Apa tiga peluang utama Anda di dunia online?

Akan sangat membantu untuk melakukan penelitian dan memahami persepsi dan pengalaman anak-anak beserta para orang tua sehubungan dengan perlindungan online anak.

6. Materi referensi

Keamanan online anak: Dokumen dan publikasi utama

2020

- ECPAT International, Sexual Exploitation Of Children In The Middle East And North Africa, 2020
- DQ Institute, 2020 Child Online Safety Report, 2020
- EU Kids Online, EU Kids Online 2020: Survey results from 19 countries, 2020

2019

- Internet Watch Foundation (IWF), Annual Report, 2019
- WeProtect Global Alliance, Global Threat Assessment, 2019
- Broadband Commission / ITU, Child Online Safety. Universal Declaration, 2019
- Broadband Commission / ITU, Child Safety Online: Minimizing the Risk of Violence, Abuse and Exploitation Online, 2019
- Global Kids Online, Growing up in a connected world, 2019
- Rethinking the Detection of Child Sexual Abuse Imagery on the Internet, in Proceedings of the 2019 World Wide Web Conference, 13–17 Mei 2019, San Francisco, Amerika Serikat, 2019
- UK Home Office, Online Harms White Paper (UK only), 2019
- PA Consulting, A tangled web: rethinking the approach to online CSEA, 2019
- UK Information Commissioner Office, Consultation on Code of Practice to help protect children online (Inggris saja), 2019
- Global Fund to End Violence against Children, Disrupting Harm: evidence to understand online child sexual exploitation and abuse, 2019
- Global Partnership to End Violence against Children, Safe to Learn Call for Action, Youth Manifesto, 2019
- UNESCO, Behind the numbers: Ending school violence and bullying, 2019 (termasuk data tentang perilaku menyakitkan online dan perundungan di dunia maya)
- United Nations Human Rights, children's rights in relation to the digital environment, 2019
- Australian eSafety Commissioner, Safety by Design Overview, 2019
- UNICEF, Why businesses should invest in digital child safety brief, 2019
- U.S. Department of State, Trafficking in Persons report, 2019

2018

- WeProtect Global Alliance, Global Threat Assessment, 2018
- Child Dignity on the Digital World, Technical Working Group Report, 2018 Council of Europe, Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 2018
- Global Fund to End Violence against Children, Two years of supporting solutions: results from the Fund's investments, 2018
- WeProtect Global Alliance, Country examples of Model of National Response capabilities and implementation, 2018
- INTERPOL and ECPAT International, Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material, 2018
- EUROPOL, Internet Organized Crime Threat Assessment (IOCTA), 2018
- NetClean, Report about Child Sexual Abuse Cybercrime, 2018
- International Centre for Missing & Exploited Children (ICMEC), Child Sexual Abuse Material: Model Legislation & Global Review, 9th Edition, 2018

- International Centre for Missing & Exploited Children (ICMEC), Studies in Child Protection: Sexual Extortion and Non-Consensual Pornography, 2018
- International Association of Internet Hotlines, INHOPE Report, 2018
- Internet Watch Foundation (IWF), Annual Report, 2018
- Thorn, Production and Active Trading of Child Sexual Exploitation Images, 2018
- ITU, Global Cybersecurity Index, 2018
- CSA Centre of Expertise, Interventions for perpetrators of online child sexual exploitation - a scoping review and gap analysis, 2018
- NatCen, Behaviour and Characteristics of Perpetrators of Online-facilitated CSEA - a rapid evidence assessment, 2018
- UNICEF, Policy guide on children and digital connectivity, 2018

2017

- The National Center for Missing & Exploited Children (NCMEC), The online enticement of children: an in-depth analysis of CyberTipline Reports, 2017
- 5Rights Foundation, Digital Childhood, development milestones in digital environment, 2017
- Childnet, DeShame Report, 2017
- Canadian Centre for Child Protection, Survivors' survey, 2017
- Internet Watch Foundation (IWF), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review, 2017
- Thorn, Sextortion online survey with 2,097 victims of sextortion ages 13 to 25, 2017
- UNICEF, Children in a Digital World, 2017
- Western Sydney University, Young and Online: Children's Perspectives on Life in Digital Age, 2017
- ECPAT International, Sexual Exploitation of Children in South East Asia, 2017

2016

- UNICEF, Perils and possibilities: growing up online, 2016
- UNICEF, Child protection in the digital age: National responses to online CSEA in ASEAN, 2016
- Centre for Justice and Crime Prevention, Child Online Protection in the MENA Region, 2016
- ECPAT International, Interagency Working Group on Sexual Exploitation of Children, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (The Luxembourg Guidelines), 2016

2015

- WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, 2015
- NCMEC, A Global Landscape of Hotlines Combating CSAM, 2015
- ITU dan UNICEF, Guidelines for Industry on Child Online Protection, 2015

Terkait dengan hak asasi manusia di dunia digital

- Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 2018
- UNESCO, Internet Universality Indicators, 2019
- Ranking Digital Rights (RDR), 2019 RDR Corporate Accountability Index, 2019
- Broadband Commission for Sustainable Development, The State of the Broadband, 2019
- ITU, Measuring Digital Development, 2019
- ITU, Measuring Information Society Report, 2018
- UNICEF, Children and Digital Marketing Industry Toolkit, 2018
- Broadband Commission for Sustainable Development, Digital health, 2017
- Broadband Commission for Sustainable Development, Digital Skills for life and work, 2017
- Broadband Commission for Sustainable Development, Digital gender divide, 2017
- UNICEF, Privacy, protection of personal information and reputation, 2017
- UNICEF, Freedom of expression, association, access to information and participation, 2017
- UNICEF, Access to the Internet and digital literacy, 2017
- UN CRC, Guidelines on effective protection of children from sexual exploitation, 2019

Untuk sumber-sumber lebih lanjut, silakan melihat daftar sumber bacaan lainnya di www.itu-cop-guidelines.com

Lampiran 1: Terminologi

Definisi di bawah ini terutama diambil dari terminologi yang ada sebagaimana diuraikan dalam Konvensi Hak Anak, 1989, serta oleh kelompok kerja Antar-lembaga tentang eksploitasi seksual anak dalam Pedoman Terminologi tentang Perlindungan Anak dari Eksploitasi Seksual dan Pelecehan Seksual, 2016[64] (Luxembourg Guidelines), oleh Konvensi Dewan Eropa: Perlindungan Anak terhadap Eksploitasi Seksual dan Pelecehan Seksual, 2012[65] serta oleh Laporan Global Kids Online, 2019[66].

Remaja

Remaja adalah seseorang yang berusia 10-19 tahun. Penting untuk dicatat bahwa remaja bukanlah istilah yang mengikat menurut hukum internasional, dan mereka yang berusia di bawah 18 tahun dianggap sebagai anak-anak, sedangkan yang berusia 19 tahun dianggap dewasa, kecuali jika usia dewasa dicapai lebih awal menurut hukum nasional[67].

Kecerdasan buatan (Artificial Intelligence atau AI)

Dalam arti luas, istilah ini merujuk secara samar ke sistem yang murni fiksi ilmiah (disebut AI "kuat" dengan bentuk sadar diri) dan sistem yang sudah beroperasi dan mampu melakukan tugas yang sangat kompleks (pengenalan wajah atau suara, mengemudi kendaraan - sistem ini digambarkan sebagai AI "lemah" atau "sedang")[68].

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, dan dirancang untuk beroperasi dengan berbagai tingkat otonomi[69].

Kepentingan terbaik bagi anak

Menjelaskan semua elemen yang diperlukan untuk membuat keputusan dalam situasi tertentu untuk individu atau sekelompok anak tertentu[70].

---

64 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse," 2016,114, http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf.

65 Council of Europe, Conseil de l'Europe, and Council of Europe, Protection of Children against Sexual Exploitation and Sexual Abuse: Council of Europe Convention (Strasbourg: Council of Europe Publishing, 2012), https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf.

66 Globalkidsonline.net, "Done Right, Internet Use Can Increase Learning and Skills," November 2019, http://globalkidsonline.net/synthesis-report-2019/.

67 UNICEF and ITU, Guidelines for Industry on Child Online Protection (itu.int/cop, 2015), https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

68 Council of Europe, "What's AI?," coe.int, Artificial Intelligence, diakses pada 16 Januari 2020, https://www.coe.int/en/web/artificial-intelligence/what-is-ai.

69 OECD, "Recommendation of the Council on Artificial Intelligence" (OECD, 2019), https://webcache.googleusercontent.com/search?q=cache:hTtMv9k1ak8J:https://legalinstruments.oecd.org/api/print%3Fids%3D648%26lang%3Den+&cd=3&hl=en&ct=clnk&gl=ch&client=safari.

70 OHCHR, "Convention on the Rights of the Child," diakses pada 16 Januari 2020, https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

Anak

Sesuai dengan pasal 1 Konvensi Hak Anak, seorang anak adalah setiap orang yang berusia di bawah 18 tahun, kecuali jika usia dewasa dicapai lebih awal menurut hukum nasional[71].

Eksploitasi dan pelecehan seksual anak (CSEA)

Menjelaskan segala bentuk eksploitasi seksual dan pelecehan seksual (CRC, 1989, pasal 34), misalnya "(a) bujukan atau paksaan seorang anak untuk terlibat dalam aktivitas seksual yang melanggar hukum; (b) Pemanfaatan anak secara eksploitatif dalam prostitusi atau praktik seksual lain yang melanggar hukum; (c) Penggunaan anak-anak secara eksploitatif dalam pertunjukan dan materi pornografi" serta "kontak seksual yang biasanya melibatkan pemaksaan terhadap seseorang tanpa persetujuan". Eksploitasi dan pelecehan seksual terhadap anak-anak semakin banyak terjadi melalui Internet, atau dengan beberapa koneksi ke lingkungan online[72].

Materi pelecehan (dan eksploitasi) seksual anak (CSAM)

Evolusi TIK yang cepat telah menciptakan bentuk-bentuk baru eksploitasi dan pelecehan seksual anak secara online, yang dapat terjadi secara virtual dan tidak harus mencakup pertemuan tatap muka secara fisik dengan anak[73]. Meskipun banyak yurisdiksi masih melabeli gambar dan video pelecehan seksual anak sebagai 'pornografi anak' atau 'gambar anak-anak yang tidak senonoh', pedoman ini akan merujuk pada subjek secara kolektif sebagai materi pelecehan seksual anak (selanjutnya, CSAM). Hal ini sesuai dengan Broadband Commission Guidelines dan Model Respon Nasional dari WePROTECT Global Alliance[74]. Istilah ini lebih tepat untuk menggambarkan konten. Pornografi mengacu pada industri yang sah dan dikomersialkan, dan sebagaimana dinyatakan dalam Luxembourg Guidelines yang menyatakan penggunaan istilah tersebut:

"mungkin (secara sengaja maupun tidak sengaja) berkontribusi untuk mengurangi kegawatani, meremehkan, atau bahkan melegitimasi hal-hal yang sebenarnya merupakan pelecehan seksual dan/atau eksploitasi seksual terhadap anak-anak […] istilah 'pornografi anak' berisiko menyiratkan seakan-akan tindakan tersebut dilakukan dengan persetujuan anak, dan mewakili materi seksual yang sah"[75].

Istilah CSAM mengacu pada materi yang mewakili tindakan pelecehan seksual dan/atau eksploitatif terhadap anak. Ini termasuk, namun tidak terbatas pada, materi yang merekam pelecehan seksual terhadap anak oleh orang dewasa; gambar anak-anak yang termasuk dalam perilaku seksual eksplisit; organ seksual anak-anak ketika gambar tersebut diproduksi atau digunakan terutama untuk tujuan seksual.

---

71 OHCHR; UNICEF and ITU, *Guidelines for Industry on Child Online Protection*.

72 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

73 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse"; UNICEF, "Global Kids Online Comparative Report (2019)."

74 WePROTECT Global Alliance, "Preventing and Tackling Child Sexual Exploitation and Absue (CSEA): A Model National Response.," 2016, https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf; Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)."

75 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

Anak-anak dan remaja

Menjelaskan semua orang di bawah usia 18 tahun dimana anak-anak, juga disebut sebagai anak-anak yang lebih muda dalam pedoman, mencakup semua orang di bawah usia 15 tahun dan remaja terdiri dari kelompok usia 15 sampai 18 tahun.

Connected toys

Connected toys 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 *connected toys* mencapai USD 2,8 miliar dan diprediksi akan meningkat menjadi USD 11 miliar pada tahun 2020. *Toys* ini mengumpulkan dan menyimpan informasi pribadi dari anak-anak termasuk nama, geolokasi, alamat, foto, audio, dan rekaman video[76].

Perundungan di dunia maya, juga disebut sebagai perundungan di dunia maya

Hukum internasional tidak mendefinisikan perundungan di dunia maya. Untuk tujuan dokumen ini, perundungan di dunia maya digambarkan sebagai tindakan agresif yang disengaja yang dilakukan berulang kali oleh sekelompok atau individu dengan menggunakan teknologi digital dan menargetkan korban yang tidak dapat dengan mudah membela diri[77]. Biasanya ini melibatkan "penggunaan teknologi digital dan internet untuk memposting informasi yang menyakitkan tentang seseorang, dengan sengaja membagikan informasi pribadi, foto, atau video pribadi dengan cara yang menyakitkan, mengirim pesan yang mengancam atau menghina (melalui email, pesan instan, obrolan, teks), menyebarkan desas-desus dan informasi palsu tentang korban atau dengan sengaja mengecualikan mereka dari komunikasi online"[78]. Ini mungkin melibatkan secara langsung (seperti obrolan atau pesan teks), semi-publik (seperti memposting pesan yang melecehkan pada daftar email) atau komunikasi publik (seperti membuat situs web yang ditujukan untuk mengolok-olok korban).

Ujaran kebencian dunia maya, diskriminasi, dan ekstremisme kekerasan

"Kebencian dunia maya, diskriminasi, dan ekstremisme kekerasan adalah bentuk-bentuk berbeda dari kekerasan dunia maya karena menargetkan identitas kolektif, bukan individu [...] sering kali berkaitan dengan ras, orientasi seksual, agama, kebangsaan atau status imigrasi, jenis kelamin/gender, dan politik"[79].

Kewarganegaraan digital

Kewarganegaraan digital mengacu pada kemampuan untuk terlibat secara positif, kritis dan kompeten dalam lingkungan digital, memanfaatkan keterampilan komunikasi dan kreasi yang efektif, untuk mempraktikkan bentuk-bentuk partisipasi sosial yang menghormati hak asasi dan martabat manusia melalui penggunaan teknologi yang bertanggung jawab[80].

---

[76] Jeremy Greenberg, "Dangerous Games: Connected Toys, COPPA, and Bad Security," Georgetown Law Technology Review, 4 Desember 2017, https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/.

[77] Anna Costanza Baldry, Anna Sorrentino, dan David P. Farrington, "Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities," Children and Youth Services Review 96 (Januari 2019): 302–7, https://doi.org/10.1016/j.childyouth.2018.11.058.

[78] UNICEF, "Global Kids Online Comparative Report (2019)"; "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

[79] UNICEF, "Global Kids Online Comparative Report (2019)."

[80] Council of Europe, "Digital Citizenship and Digital Citizenship Education," Digital Citizenship Education, diakses pada 16 Januari 2020, https://www.coe.int/en/web/digital-citizenship-education/home.

Literasi digital

Literasi digital berarti memiliki keterampilan yang dibutuhkan seseorang untuk hidup, belajar, dan bekerja dalam masyarakat di mana komunikasi dan akses informasi semakin meningkat melalui teknologi digital seperti platform internet, media sosial, dan perangkat seluler[81]. Hal ini mencakup komunikasi yang jelas, keterampilan teknis, dan pemikiran kritis.

Ketahanan digital

Istilah ini menggambarkan kemampuan seorang anak untuk secara emosional mengatasi bahaya yang dihadapi secara online. Ketahanan digital termasuk memiliki sumber daya emosional yang diperlukan untuk memahami saat anak berada dalam risiko online, mengetahui apa yang harus dilakukan untuk mencari bantuan, belajar dari pengalaman, dan memulihkan diri saat terjadi kesalahan[82].

Pendidik

Pendidik adalah seseorang yang secara sistematis bekerja untuk meningkatkan pemahaman orang lain tentang mata pelajaran tertentu. Peran pendidik meliputi mereka yang mengajar di ruang kelas dan pendidik yang lebih informal yang, misalnya, mereka yang menggunakan platform dan layanan situs jejaring sosial untuk memberikan informasi keamanan online atau menjalankan kursus berbasis komunitas atau sekolah untuk memungkinkan anak-anak dan remaja untuk tetap aman saat online.

Pekerjaan pendidik akan bervariasi tergantung pada konteks di mana mereka bekerja dan kelompok usia anak-anak dan remaja (atau orang dewasa) yang ingin mereka didik.

Grooming/grooming online

Grooming/*grooming* online sebagaimana didefinisikan dalam Luxembourg Guidelines, mengacu pada proses menjalin/membangun hubungan dengan seorang anak baik secara langsung atau melalui penggunaan Internet atau teknologi digital lainnya untuk memfasilitasi kontak seksual secara offline atau online dengan orang tersebut membujuk anak untuk melakukan hubungan seksual[83]. Suatu proses yang dimaksudkan untuk memikat anak-anak ke dalam perilaku atau percakapan seksual dengan atau tanpa sepengetahuan mereka, atau suatu proses yang melibatkan komunikasi dan sosialisasi antara pelaku dan anak untuk membuatnya lebih rentan terhadap pelecehan seksual. Istilah *grooming* belum didefinisikan dalam hukum internasional; beberapa yurisdiksi, termasuk Kanada, menggunakan istilah '*luring*' (memancing).

Teknologi informasi dan komunikasi (TIK)

Teknologi informasi dan komunikasi menggambarkan semua teknologi informasi yang menekankan aspek komunikasi. Ini mencakup semua layanan dan perangkat yang terhubung ke Internet seperti antara lain komputer, laptop, tablet, *smartphone*, konsol game, televisi, dan jam tangan[84]. Ini lebih lanjut mencakup layanan seperti radio serta antara lain *broadband*, perangkat keras jaringan dan sistem satelit.

---

[81] Western Sydney University-Claire Urbach, "What Is Digital Literacy?," diakses pada 16 Januari 2020, https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy.

[82] Dr. Andrew K. Przybylski, et al., "A Shared Responsibility. Building Children's' Online Resilience Report" (ParentZone, University of Oxford and Virgin Media, 2014), https://parentzone.org.uk/sites/default/files/Building%20Online%20Resilience%20Report.pdf.

[83] "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

[84] UNICEF and ITU, *Guidelines for Industry on Child Online Protection.*

Internet dan teknologi terkait

Sekarang dimungkinkan untuk terhubung ke Internet menggunakan berbagai perangkat yang berbeda, misalnya, *smartphone*, tablet, konsol game, TV dan laptop serta komputer yang lebih tradisional. Jadi, kecuali jika konteksnya menunjukkan sebaliknya, referensi apa pun ke Internet harus dipahami mencakup semua metode yang berbeda ini. Untuk mencakup permadani Internet yang kaya dan kompleks, 'Internet dan teknologi terkait', 'TIK dan industri online' dan 'layanan berbasis Internet' digunakan secara bergantian.

Notice dan takedown

Operator dan penyedia layanan terkadang diberi tahu tentang konten yang mencurigakan secara online oleh pelanggan, anggota masyarakat, penegak hukum, atau organisasi hotline. Prosedur *notice* dan *takedown* mengacu pada proses perusahaan untuk penghapusan cepat (*'takedown'*) konten ilegal (konten ilegal didefinisikan menurut yurisdiksi) segera setelah mereka diberi tahu (*'notice'*) keberadaannya di layanan mereka.

Online gaming

'Game online' didefinisikan sebagai memainkan semua jenis game digital komersial yang satu pemain tunggal atau multipemain melalui perangkat apa pun yang terhubung ke Internet, termasuk konsol khusus, komputer desktop, laptop, tablet, dan ponsel.

'Ekosistem game online' didefinisikan untuk mencakup menonton orang lain bermain video game melalui platform e-sports, *streaming*, atau *video-sharing*, yang biasanya memberikan opsi bagi pemirsa untuk mengomentari atau berinteraksi dengan pemain dan audiens lainnya.[85].

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 semacam itu dapat membatasi akses ke jenis/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 maju dapat merekam semua teks yang dikirim atau diterima dari perangkat. Program ini biasanya akan dilindungi kata sandi[86].

Orang tua, pengasuh, wali

Beberapa situs Internet merujuk pada orang tua dengan cara yang umum (seperti pada "halaman orang tua" dan merujuk pada "kontrol orang tua"). Oleh karena itu, penting untuk mendefinisikan orang-orang yang idealnya harus memberdayakan anak-anak untuk memaksimalkan peluang yang tersedia secara online, memastikan bahwa anak-anak dan remaja menggunakan situs Internet dengan aman dan bertanggung jawab dan memberikan persetujuan mereka untuk memiliki akses ke situs Internet tertentu. Dalam dokumen ini, istilah "orang tua" mengacu pada siapa saja (tidak termasuk pendidik) yang memiliki tanggung jawab hukum atas seorang anak. Tanggung jawab orang tua akan bervariasi dari satu negara ke negara lain seperti halnya hak orang tua yang sah.

---

85 UNICEF, "Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry," DISCUSSION PAPER SERIES: Children's Rights and Business in a Digital World, 2019, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

86 UNICEF and ITU, *Guidelines for Industry on Child Online Protection.*

Informasi pribadi

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

Privasi

Privasi sering diukur dalam hal berbagi informasi pribadi secara online, memiliki profil media sosial publik, berbagi informasi dengan orang yang mereka kenal secara online, menggunakan pengaturan privasi, berbagi kata sandi dengan teman, memperhatikan privasi[87].

Sexting

Sexting umumnya didefinisikan sebagai pengiriman, penerimaan, atau pertukaran konten seksual yang diproduksi sendiri termasuk gambar, pesan, atau video melalui ponsel dan/atau Internet[88]. Pembuatan, distribusi, dan kepemilikan gambar seksual anak-anak adalah ilegal di sebagian besar negara. Jika gambar seksual anak-anak diungkapkan, orang dewasa tidak boleh melihatnya. Berbagi gambar seksual oleh orang dewasa kepada anak merupakan tindakan kriminal maupun di antara anak-anak dapat terjadi bahaya dan diperlukan pelaporan serta tindakan untuk menghapus gambar yang dibagikan.

Pemerasan seksual terhadap anak-anak

Pemerasan seksual (juga disebut sebagai "pemaksaan dan pemerasan seksual online")[89] menggambarkan "pemerasan seseorang dengan bantuan gambar yang dibuat sendiri dari orang tersebut untuk memeras keuntungan seksual, uang, atau keuntungan lain darinya di bawah ancaman membagikan materi di luar persetujuan orang yang digambarkan (misalnya, memposting gambar di media sosial)"[90].

Internet of Things(IoT)

Internet of Things mewakili langkah selanjutnya menuju digitalisasi masyarakat dan ekonomi, di mana objek dan orang saling terhubung melalui jaringan komunikasi dan melaporkan tentang status mereka dan/atau lingkungan sekitarnya[91].

URL

Merupakan singkatan dari *'uniform resource locator'*, sebutan untuk alamat halaman Internet[92].

87 "Children's Online Privacy Protection Act," Pub. L. No. 15 U.S.C. 6501-6505 (1998), https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

88 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

89 Europol, "Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective" (European Cybercrime Centre, Mei 2017), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

90 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

91 Ntantko, The Internet of Things, 1 Oktober 2013, Digital Single Market - European Commission, https://ec.europa.eu/digital-single-market/en/internet-of-things.

92 UNICEF and ITU, *Guidelines for Industry on Child Online Protection.*

Virtual reality

Virtual reality adalah penggunaan teknologi komputer untuk menciptakan efek dunia tiga dimensi interaktif di mana objek memiliki rasa kehadiran spasial[93].

Wi-Fi

Wi-Fi (*Wireless Fidelity*) adalah sekelompok standar teknis yang memungkinkan transmisi data melalui jaringan nirkabel [94].

[93] NASA, "Virtual Reality," nas.nasa.gov, diakses pada 16 Januari 2020, https://www.nas.nasa.gov/Software/VWT/ vr.html.

[94] Children's Online Privacy Protection Act.

Lampiran 2 : Kontak pelanggaran terhadap anak-anak dan remaja

Anak-anak dan remaja dapat terkena berbagai kontak yang tidak diinginkan atau tidak pantas di Internet yang dapat memiliki konsekuensi yang mengerikan bagi mereka. Beberapa dari kontak ini mungkin bersifat seksual.

Penelitian telah menunjukkan bahwa 22 persen telah dirundung[95], dilecehkan atau dikuntit secara online; 24 persen telah menerima komentar seksual yang tidak diinginkan;[96] 8 persen telah bertemu orang-orang dalam kehidupan nyata yang sebelumnya hanya mereka kenal secara online[97]. Meskipun angkanya berbeda-beda di setiap negara dan wilayah, angka-angka ini menunjukkan bahwa risikonya nyata[98]. Satu studi Internet di Amerika Serikat[99] menemukan bahwa 32 persen remaja online telah dihubungi oleh orang yang sama sekali tidak dikenal, 23 persen dari mereka mengatakan bahwa mereka merasa takut dan tidak nyaman selama kontak; dan 4 persen telah menerima ajakan seksual agresif.

Predator seksual menggunakan Internet untuk menghubungi anak-anak dan remaja untuk tujuan seksual, sering kali menggunakan teknik yang dikenal sebagai *grooming* di mana mereka mendapatkan kepercayaan anak dengan menarik minatnya. Mereka sering memperkenalkan topik seksual, foto dan bahasa eksplisit untuk menghilangkan kepekaan, meningkatkan kesadaran seksual dan melunakkan keinginan korban muda mereka. Hadiah, uang, dan bahkan tiket transportasi digunakan untuk membujuk dan memikat anak atau remaja ke tempat di mana si predator dapat mengeksploitasinya secara seksual. Pertemuan-pertemuan ini bahkan dapat difoto atau direkam. Anak-anak dan remaja sering kali tidak memiliki kedewasaan emosional dan harga diri, yang membuat mereka rentan terhadap manipulasi dan perundungan. Mereka juga ragu-ragu untuk memberitahu orang dewasa tentang pertemuan mereka karena takut malu atau kehilangan akses ke Internet. Dalam beberapa kasus, mereka diancam oleh predator dan disuruh merahasiakan hubungannya. Predator seksual juga belajar dari satu sama lain melalui forum Internet dan *chat room*.

[95] U-report (2019), http://www.ureport.in/v2/.
[96] Project deSHAME (2017), https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf.
[97] Lenhardt, A., Anderson, M., Smith, A. (2015), Teens, Technology and Romantic Relationships, https://www.pewresearch.org/internet/2015/10/01/teens-technology-and-romantic-relationships/
[98] Livingstone, S., Haddon, L., Görzig, A., dan Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of Europeanchildren. Fullfindings*. LSE,London: EUKids Online, http://eprints.lse.ac.uk/33731/.
[99] Amanda Lenhart et al., "The Use of Social Media Gains a Greater Foothold in Teen Life as They Embrace the Conversational Nature of Interactive Online Media.," *Pew Internet and American Life Project*, 2007, 44, https://www.pewinternet.org/wpcontent/uploads/sites/9/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf.

Lampiran 3: The WeProtect Global Alliance

Model Respon Nasional WePROTECT

Strategi WePROTECT Global Alliance mendukung negara-negara untuk mengembangkan tanggapan *multi-stakeholdrs* yang terkoordinasi untuk mengatasi eksploitasi seksual anak secara online, dipandu oleh Model Respon Nasional (MNR). Model Respon Nasional WPGA berfungsi sebagai cetak biru untuk aksi nasional. Model ini memberikan kerangka kerja bagi negara-negara untuk mengatasi eksploitasi seksual anak secara online (OCSE). Model ini dimaksudkan untuk membantu suatu negara untuk:

- mengevaluasi responnya saat ini terhadap OCSE dan mengidentifikasi kesenjangan;
- memprioritaskan upaya nasional untuk mengisi kesenjangan;
- meningkatkan pemahaman dan kerjasama internasional.

Model tersebut tidak berusaha untuk meresepkan kegiatan atau menetapkan pendekatan tunggal. Tujuannya adalah untuk menggambarkan kemampuan yang dibutuhkan untuk perlindungan anak yang efektif dan untuk mendukung negara-negara untuk mengembangkan atau meningkatkan kemampuan mereka yang ada. Ini juga mencantumkan sejumlah faktor pendukung yang, jika ada dan efektif, akan mempercepat dan meningkatkan hasil. MNR mencakup dua puluh satu kemampuan, dibagi menjadi enam bagian: kebijakan dan tata kelola, peradilan pidana, korban, masyarakat, industri, serta media dan komunikasi. WPGA percaya bahwa tindakan di keenam bidang akan memberikan respon nasional yang lengkap terhadap kejahatan ini.

Model ini akan memungkinkan suatu negara – terlepas dari titik awalnya – untuk mengidentifikasi setiap kesenjangan dalam kemampuan dan mulai merencanakan untuk mengisi kesenjangan tersebut. Meskipun negara-negara akan mengembangkan pendekatan mereka masing-masing, dengan melakukannya dalam konteks kerangka kerja yang disepakati dan pemahaman bersama atas kapabilitas, diharapkan komunikasi dan kerja sama di antara para pemangku kepentingan di tingkat nasional dan internasional dapat lebih ditingkatkan.

Respon Strategis Global WePROTECT

Respon Strategis Global (GSR) WePROTECT Global Alliance adalah pendekatan terkoordinasi untuk memerangi eksploitasi seksual anak secara online dengan menyertakan wawasan global yang lebih besar, harmonisasi internasional pendekatan nasional, dan solusi global, di atas dan melampaui respons yang dipimpin di tingkat nasional. GSR pada dasarnya adalah pelengkap dari Model Respon Nasional (MNR); sementara MNR difokuskan pada kapabilitas yang dibutuhkan untuk menangani OCSE di tingkat nasional, GSR difokuskan pada bidang-bidang prioritas untuk kerjasama dan peningkatan kapasitas internasional.

GSR mencakup enam bidang tematik, dengan kapabilitas terkait yang diperlukan dan hasil yang diharapkan untuk masing-masing bidang, serta mitra yang harus bekerja sama lintas batas untuk mewujudkannya.

Kebijakan dan undang-undang

Mengembangkan *political will* untuk bertindak dan undang-undang untuk secara efektif menyelaraskan pendekatan terhadap tindak pidana akan menghasilkan pembaruan komitmen tingkat tinggi di tingkat nasional dan internasional untuk memerangi eksploitasi seksual anak secara online.

Peradilan pidana

Berbagi informasi, termasuk akses bersama ke basis data internasional melalui kerangka kerja berbagi data formal yang dikombinasikan dengan petugas hukum dan jaksa khusus dan terlatih dengan keahlian dalam bidang eksploitasi seksual anak secara online adalah cara terbaik untuk mengidentifikasi, mengejar, dan menangkap pelaku, termasuk melalui investigasi dan hukuman bersama yang berhasil.

Dampak dan layanan korban

Dukungan yang efektif dan tepat waktu bagi para korban, termasuk perlindungan identitas mereka dan memberi mereka suara, membantu memastikan bahwa para korban dapat mengakses dukungan yang mereka butuhkan, saat mereka membutuhkannya.

Teknologi

Penggunaan solusi teknis, termasuk kecerdasan buatan, untuk mendeteksi, memblokir, dan mencegah materi berbahaya, *live streaming*, dan *grooming* online, yang harus mencakup kepatuhan yang luas dan konsisten di antara sektor teknologi, akan memungkinkan platform tersebut untuk tidak digunakan sebagai alat untuk eksploitasi seksual anak secara online.

Masyarakat

Terdapat sejumlah kapabilitas yang dapat dimanfaatkan bersama dalam masyarakat luas untuk memberdayakan anak-anak untuk melindungi diri mereka dari eksploitasi seksual anak secara online, di mana pun mereka tinggal. Dengan memastikan bahwa pengembangan budaya digital sejak awal didesain agar lebih aman (yaitu, memiliki fitur keamanan bawaan), dan adanya pendekatan etis dan konsisten terhadap pelaporan media, paparan konten ilegal secara online akan dibatasi. Sementara itu, pendidikan dan penjangkauan untuk anak-anak dan orang tua, pengasuh, dan profesional, dan intervensi yang ditargetkan untuk pelaku, semuanya berupaya untuk mencegah atau mengurangi terjadinya eksploitasi seksual anak secara online.

Riset dan wawasan

Terakhir, penilaian ancaman (seperti Global Threat Assessment 2019), penelitian pelaku, dan upaya untuk memahami trauma korban jangka panjang akan memberikan pemahaman yang jelas kepada pemerintah, penegak hukum, masyarakat sipil, akademisi, dan industri tentang ancaman terbaru.

Lampiran 4: Contoh tanggapan terhadap bahaya online

Contoh-contoh yang disertakan di sini disusun oleh penulis dan kontributor pedoman pembuat kebijakan ITU.

Mendidik anak-anak melawan bahaya online

Aplikasi Own IT BBC – sebuah aplikasi kesejahteraan yang ditujukan untuk anak-anak berusia 8-13 tahun yang menerima *smartphone* pertama mereka. Menggabungkan teknologi pembelajaran mesin canggih untuk melacak aktivitas anak-anak di *smartphone* mereka dengan kemampuan bagi anak-anak untuk melaporkan sendiri keadaan emosi mereka, menggunakan informasi ini untuk memberikan konten dan intervensi yang disesuaikan untuk membantu anak-anak agar tetap bahagia dan sehat secara online.

Menampilkan konten berkomisi khusus dari seluruh BBC, aplikasi ini menyediakan materi dan sumber yang berguna untuk membantu remaja memanfaatkan waktu online mereka secara maksimal dan membangun perilaku dan kebiasaan online yang sehat, membantu remaja dan orang tua melakukan percakapan yang lebih konstruktif tentang pengalaman mereka secara online. Aplikasi ini tidak mengumpulkan data atau konten pribadi apa pun yang dihasilkan dari pengguna karena seluruh pembelajaran mesin berjalan di dalam aplikasi/di dalam perangkat pengguna.

Project Evolve – Kerangka kerja pendidikan kompetensi digital dengan sumber daya penuh, mengidentifikasi keterampilan digital untuk setiap dan semua usia anak untuk membantu orang tua dan guru memahami kompetensi yang harus dimiliki anak-anak mereka, bersama dengan sumber daya dan kegiatan yang akan memberi mereka keterampilan tertentu.

360 degree safe – Sebuah alat tinjauan mandiri online untuk sekolah dalam mempertimbangkan dan menilai seluruh ketentuan keamanan online mereka yang memberikan panduan dan dukungan untuk mendapatkan standar yang ditentukan.

DQ Institute – Data dikumpulkan dari 145.426 anak-anak dan remaja di 30 negara dari 2017-2019 sebagai bagian dari #DQEveryChild, gerakan kewarganegaraan digital global yang diperjuangkan oleh DQ Institute, yang dimulai di Singapura dengan dukungan Singtel dan dengan cepat berkembang melalui kolaborasi dengan World Economic Forum untuk melibatkan lebih dari 100 organisasi mitra. Gerakan ini bertujuan untuk memberdayakan anak-anak dengan kompetensi kewarganegaraan digital yang komprehensif sejak awal kehidupan digital mereka menggunakan program pendidikan dan penilaian online DQ World. Data dari gerakan ini digunakan untuk membuat Indeks Keamanan Online Anak (COSI) 2020. Kerangka kerja COSI menilai dan memberi peringkat keamanan online anak di 30 negara berdasarkan 24 area yang dikelompokkan menjadi enam pilar yang memengaruhi keamanan online anak.

Paket Kesiapan Keluarga DQ Pro dan DQ World memberikan kesempatan bagi orang tua untuk menilai kesiapan digital anak mereka dan, melalui materi pendidikan, meningkatkan kompetensi digital seperti kewarganegaraan digital, manajemen waktu layar, manajemen perundungan di dunia maya, manajemen keamanan dunia maya, empati digital, manajemen jejak digital, berpikir kritis, dan manajemen privasi eSafety Toolkit for Schools milik Australia adalah sumber daya yang dirancang untuk mendukung sekolah dalam menciptakan lingkungan online yang lebih aman. *Toolkit* ini mencerminkan pendekatan multifaset untuk pendidikan keselamatan online, dan telah dikategorikan ke dalam empat elemen, dengan sumber daya yang:

- mempersiapkan sekolah untuk menilai kesiapan mereka untuk menangani masalah keamanan online dan memberikan saran untuk meningkatkan praktik mereka saat ini;
- melibatkan seluruh komunitas sekolah untuk berkomitmen dan terlibat dalam menciptakan lingkungan online yang aman;
- mendidik dengan menyoroti praktik terbaik dalam pendidikan keamanan online dan mendukung sekolah untuk mengembangkan kemampuan keamanan online bagi komunitas sekolah;
- merespon insiden secara efektif sambil mendukung keselamatan dan kesejahteraan.

Kampanye pendidikan I Click Sensible oleh Kantor Komunikasi Elektronik Polandia-UKE mendidik anak-anak dan orang tua tentang bagaimana cara menjelajahi dunia maya secara lebih aman dan bagaimana mengenali serta mengelola risiko.

ChildFund Viet Nam membentuk inisiatif Swipe Safe . Program ini mendidik anak-anak tentang potensi risiko online, seperti penipuan dunia maya, perundungan, atau pelecehan seksual, dan memberikan saran tentang metode untuk tetap aman.

Laporan Broadband Commission tentang *Teknologi, Broadband dan Pendidikan: memajukan pendidikan untuk semua agenda*, 2013.

Pengalaman Anak-Anak Online: Membangun Pemahaman dan Tindakan Global, UNICEF, 2019.

Penelitian Online Anak Global yang mencakup banyak informasi tentang respons praktik yang baik terhadap bahaya online.

Contoh industri yang terlibat

eSafety Commissioner Australia membangun kemitraan yang kuat dan bekerja dengan industri untuk memberdayakan semua warga Australia agar mendapatkan pengalaman online yang lebih aman dan positif. Contohnya adalah pekerjaan eSafety tentang keselamatan sejak desain awal. Sebagai bagian dari inisiatif, eSafety melakukan proses konsultasi terperinci dengan industri, badan dan organisasi perdagangan yang bertanggung jawab untuk melindungi pengguna, serta orang tua, pengasuh, dan remaja. Inisiatif Safety by Design dirancang untuk mendorong dan membantu industri memastikan keamanan pengguna tertanam dalam desain, pengembangan, dan penerapan layanan dan platform online. eSafety juga mengelola tiga skema pelaporan dan pengaduan: skema perundungan di dunia maya, skema pelecehan berbasis gambar dan skema konten online. eSafety dapat secara resmi mengarahkan penyedia layanan online tertentu untuk menghapus konten dari layanan mereka. Sementara skema sebagian besar beroperasi sebagai model kerja sama antara pemerintah dan industri, kekuatan yang tersedia untuk eSafety untuk memaksa penghapusan materi memberikan jaring pengaman penting dan mendorong industri untuk proaktif dalam mengatasi bahaya online.

Perusahaan Telia bertanggung jawab untuk memahami dan mengelola dampak negatif dari konektivitas dan untuk sepenuhnya transparan dan akuntabel di tingkat Dewan. Mereka juga peduli dengan anak-anak dan remaja karena mereka mengakui bahwa itulah pengguna aktif dari layanan mereka.

Kantor Komunikasi Elektronik Polandia-UKE melibatkan masyarakat sipil dan anak-anak dalam kampanye advokasi mereka untuk membuat mereka menyadari apa yang mereka tanda tangani secara online.

Internet Watch Foundation adalah organisasi kemitraan yang menyatukan industri, pemerintah, penegak hukum dan LSM untuk menghapus pelecehan seksual anak. Pada tahun 2020, IWF memiliki 152 Anggota di seluruh platform dan layanan infrastruktur dan menawarkan berbagai layanan kepada Anggotanya untuk mencegah penyebaran citra kriminal di platform mereka.

Cakupan undang-undang

Ekspresikan kemauan politik untuk memprioritaskan COP dengan menandatangani Child Online Safety Universal Declaration (Broadband Commission).

Peraturan

Outof theShadows: menyoroti respons terhadap indeks pelecehan dan eksploitasi seksual anak (2019) dari The Economist Intelligence Unit adalah satu-satunya alat tolok ukur yang menganalisis respons negara-negara terhadap pelecehan dan eksploitasi seksual anak, termasuk ruang digital dan respons industri TIK untuk itu.

Identifikasi pelecehan anak secara online

Berikut ini adalah contoh praktik yang baik dalam mengidentifikasi pelecehan anak secara online.

INHOPE: Jaringan INHOPE dibentuk pada tahun 1999 untuk memerangi CSAM online dalam menanggapi visi bersama tentang Internet yang bebas dari materi pelecehan seksual anak. Dalam kurun waktu 20 tahun, INHOPE telah berkembang dengan sukses untuk memerangi pertumbuhan, penyebaran geografis, dan keparahan CSAM online. Saat ini hotline INHOPE bekerja di lapangan di setiap benua, menerima laporan dan dengan cepat menghapus CSAM dari Internet, dan berbagi data dengan penegak hukum.

Microsoft PhotoDNA membuat *hash* gambar dan membandingkannya dengan basis data hash yang telah diidentifikasi dan dikonfirmasi sebagai CSAM. Jika menemukan kecocokan, gambar tersebut akan diblokir. Namun, alat ini tidak menggunakan teknologi pengenalan wajah, juga tidak dapat mengidentifikasi seseorang atau objek dalam gambar. Namun, dengan penemuan PhotoDNA for Video, segalanya dapat berubah.

PhotoDNA for 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 for Video dapat menemukan konten eksploitasi seksual anak yang telah diedit atau digabungkan menjadi video yang mungkin tampak tidak berbahaya.

Microsoft telah merilis alat baru untuk mengidentifikasi predator anak yang mempersiapkan anak-anak untuk pelecehan dalam obrolan online. Project Artemis, yang dikembangkan bekerja sama dengan The Meet Group, Roblox, Kik and Thorn, dibangun di atas teknologi yang dipatenkan Microsoft dan akan tersedia secara gratis melalui Thorn untuk perusahaan layanan online yang menawarkan fungsi obrolan. Project Artemis adalah alat teknologi yang membantu memberi peringatan kepada Administrator ketika moderasi diperlukan di *chat room*. Teknik deteksi *grooming* ini akan dapat mendeteksi, mengatasi, dan melaporkan predator yang mencoba memikat anak-anak untuk tujuan seksual.

Thorn telah mengembangkan iklan pencegahan yang ditujukan bagi mereka yang mencari materi pelecehan seksual terhadap anak, yang telah ditayangkan jutaan kali di empat mesin pencari selama tiga tahun. Selain itu, iklan itu telah melihat rasio klik-tayang 3 persen dari orang-orang yang mencari bantuan setelah mencari materi eksploitatif.

Thorn's Safer, sebuah alat yang dapat digunakan langsung ke platform perusahaan swasta untuk mengidentifikasi, menghapus, dan melaporkan CSAM.

Thorn Spotlight, sebuah perangkat lunak yang memberikan penegakan hukum di 50 negara bagian di Amerika Serikat dan Kanada kemampuan untuk mempercepat identifikasi korban dan mengurangi waktu investigasi lebih dari 60 persen.

Geebo, sebuah situs rahasia yang berkomitmen untuk menjauhkan eksploitasi seksual dari platformnya, tidak pernah memiliki kasus yang melibatkan eksploitasi seksual anak. Mereka berhasil melakukan ini sebagian karena proses pra-penyaringan mereka.

Google AI classifier dapat digunakan untuk mendeteksi materi pelecehan seksual terhadap anak di jaringan, layanan, dan di platform. Alat ini tersedia secara gratis melalui Google Content Safety API, yang merupakan alat yang meningkatkan kapasitas untuk meninjau konten dengan cara yang membutuhkan lebih sedikit orang untuk diekspos. Alat ini akan membantu pakar manusia meninjau materi ke skala yang lebih besar dan mengikuti pelaku, dengan menargetkan citra yang sebelumnya tidak ditandai sebagai materi ilegal. Berbagi teknologi ini akan mempercepat identifikasi gambar.

Pada tahun 2015, Google memperluas pekerjaan mereka pada hash dengan memperkenalkan sidik jari pertama dan teknologi pencocokan untuk video di YouTube, yang memindai dan mengidentifikasi video yang diunggah yang berisi materi pelecehan seksual anak yang diketahui.

Selama Child Safety Hackathon tahun 2019, Facebook mengumumkan dua teknologi *open-source* yang mendeteksi foto dan video yang identik dan hampir identik. Kedua algoritma ini tersedia di GitHub yang memungkinkan sistem berbagi hash untuk berbicara satu sama lain, membuat sistem jauh lebih kuat.

Hotline IWF tetap waspada, tidak hanya menindaklanjuti ribuan laporan dari anggota masyarakat, yang mungkin menemukan gambar pelecehan seksual anak secara online, tetapi juga melakukan peran proaktif yang unik dalam mencari konten ilegal ini di web. Dengan memberdayakan hotline untuk memanfaatkan informasi dan sumber daya fokus mereka, lebih banyak konten dapat diidentifikasi dan dihapus. Selain itu, IWF terus bekerja sama dengan Google, Microsoft, dan Facebook serta perusahaan lain dalam keanggotaannya untuk terus mendorong batasan teknis. 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.

IWF berkolaborasi dengan yayasan amal pendukung korban Marie Collins Foundation yang bertujuan untuk membuat kampanye baru yang menyerukan kepada remaja pria untuk melaporkan gambar atau video seksual yang dibuat sendiri dari anak-anak di bawah 18 tahun yang mungkin mereka temukan saat menjelajahi dunia maya.

Interpol telah membuat basis data gambar dan video International Child Sexual Exploitation (ICSE), yang merupakan alat intelijen dan investigasi, yang memungkinkan penyelidik khusus dari lebih dari 50 negara untuk berbagi data tentang kasus pelecehan seksual anak. Dengan menganalisis konten digital, visual dan audio dari foto dan video, ahli identifikasi korban dapat mengambil petunjuk, mengidentifikasi setiap tumpang tindih dalam kasus dan menggabungkan upaya mereka untuk menemukan korban pelecehan seksual anak. Saat ini, basis data Eksploitasi Seksual Anak Interpol menyimpan lebih dari 1,5 juta gambar dan video dan telah membantu mengidentifikasi 19.400 korban di seluruh dunia.

NetClean ProActive adalah software berbasis pencocokan tanda tangan dan algoritma deteksi lainnya yang secara otomatis mendeteksi gambar dan video pelecehan seksual anak di lingkungan perusahaan.

Griffeye Brain menggunakan kecerdasan buatan untuk memindai konten yang sebelumnya tidak diklasifikasikan, membandingkannya dengan atribut konten CSAM yang diketahui, dan menandai item yang dicurigai untuk ditinjau oleh seorang agen.

RAINN membuat dan mengoperasikan National Sexual Assault Hotline dengan bermitra dengan lebih dari 1.000 penyedia layanan laporan kekerasan seksual lokal di seluruh negeri dan mengoperasikan DoD Safe Helpline untuk Departemen Pertahanan. RAINN juga menjalankan program untuk mencegah kekerasan seksual, membantu para penyintas, dan memastikan pelakunya diadili.

Safehorizon adalah organisasi nirlaba asistensi korban yang telah berdiri bersama para korban kekerasan dan pelecehan di New York City sejak 1978. Safehorizon menawarkan layanan hotline kepada korban kekerasan.

Project Arachnid adalah alat inovatif yang dioperasikan oleh Canadian Centre, Project Arachnid untuk memerangi proliferasi materi pelecehan seksual anak (CSAM) di Internet yang semakin meningkat.

[i] http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf