



VAIKŲ APSAUGOS INTERNETE GAIRĒS PASLAUGŲ TEIKĒJAMS

Lietuvos Respublikos ryšių reguliavimo tarnyba (RRT) pristato Vaikų apsaugos internete gaires, skirtas informacijos ir ryšių technologijų (IRT) pramonės šalims, elektroninės informacijos prieglobos paslaugų teikėjams ir kitoms suinteresuotoms grupėms. Išsamiose gairėse, kurias parengė Tarptautinė telekomunikacijų sąjunga (ITU) kartu su darbo grupe, pateiktos gerosios praktikos rekomendacijos sprendžiant vaikams kylančios rizikos skaitmeniniame pasaulyje klausimus bei kaip elgtis siekiant vaikams sukurti saugią aplinką internete. Gairėse gausu patarimų, kaip pramonė gali padėti užtikrinti vaikų saugumą naudojant IRT, internetą ar bet kurią susijusią technologiją ar įrenginį, įskaitant mobiliuosius telefonus, žaidimų konsoles, prie interneto prijungiamus žaislus, laikrodžius, daiktų internetą ir dirbtiniu intelektu pagrįstas sistemas.

Padėkos

Šias gaires parengė Tarptautinė telekomunikacijų sąjunga (ITU) ir darbo grupė, sudaryta iš autorių iš pirmaujančių institucijų, veikiančių informacinių ir ryšių technologijų (IRT) bei vaikų apsaugos srityje, įskaitant EBU, Pasaulinę partnerystę smurtui prieš vaikus sustabdyti, GSMA, Tarptautinį neįgaliųjų aljansą, Interneto stebėjimo fondą (IWF), „Privately SA“ ir UNICEF. Darbo grupei pirmininkavo Anjan Bose (UNICEF), o ją koordinavo Fanny Rotino (ITU).

Šios ITU gairės nebūtų įmanomos be autorių paaukoto laiko, entuziazmo ir atsidavimo. Taip pat ypatingai prisidėjo „e-Worldwide Group“ („e-WWG“), „Facebook“, „Tencent Games“, „Twitter“, „Walt Disney Company“ ir kitos suinteresuotos šalys, kurių bendras tikslas - padaryti internetą geresne ir saugesne vieta vaikams ir jaunimui. ITU yra dėkinga šiems partneriams, kurie skyrė savo brangų laiką ir įžvalgas (išvardyti organizacijų abėcėlės tvarka):

- Giacomo Mazzone (EBU)
- Salma Abbasi (e-WWG)
- David Miles ir Caroline Hurst (Facebook)
- Amy Crocker ir Serena Tommasino (Pasaulinė partnerystė smurtui prieš vaikus sustabdyti)
- Jenny Jones (GSMA)
- Lucy Richardson (Tarptautinis neįgaliųjų aljansas)
- Fanny Rotino (ITU)
- Tess Leyland (IWF)
- Deepak Tewari („Privately SA“)
- Adam Liu („Tencent Games“)
- Katy Minshall („Twitter“)
- Anjan Bose, Daniel Kardefelt Winther, Emma Day, Josianne Galea Baron, Sarah Jacobstein ir Steven Edwin Vosloo (UNICEF)
- Amy E. Cunningham („Walt Disney Company“)

Įžanga

Spartus skaitmeninių technologijų augimas sukūrė precedento neturinčias galimybes vaikams ir jaunimui bendrauti, dalytis, mokytis, naudotis informacija ir reikšti savo nuomonę poveikį jų gyvenimui ir jų bendruomenėms turinčiais klausimais.

Tačiau platesnė ir lengviau prieinama interneto paslaugų prieiga taip pat kelia didelių iššūkių vaikų saugumui - tiek internete, tiek ir už jo ribų. Šiandienos vaikai susiduria su daugybe rimtų pavojų: nuo pavojaus privatumui, bendraamžių smurto ir žalingo bei (arba) netinkamo turinio jų amžiui, iki interneto sukčių ir nusikaltimų prieš vaikus, pavyzdžiui, viliojimo internete, seksualinės prievartos ir išnaudojimo. Grėsmių daugėja, o smurtautojai vis dažniau vienu metu veikia iš kelių valstybių, todėl juos sunku surasti ir dar sunkiau nubausti. Be to, pasaulinės COVID-19 pandemijos metu padaugėjo vaikų, kurie pirmą kartą turėjo prisijungti prie internetinio pasaulio dėl nuotolinio mokymo bei socialinių ryšių. Virusą nustatyti apribojimai reiškė ne tik tai, kad daugelis jaunesnių vaikų pradėjo bendrauti internete daug anksčiau, nei galbūt planavo jų tėvai, bet ir tai, kad dėl darbinių įsipareigojimų daugelis tėvų negalėjo prižiūrėti savo vaikų, todėl jauniems žmonėms iškilo grėsmė pasiekti netinkamą turinį ar susidurti nusikaltėliais, kuriančiais vaikų seksualinio išnaudojimo medžiagą (CSAM).

Nusikaltėliai naudojami technologijų pažanga, tokia kaip mobiliųjų programėlių ir žaidimų susijungimas, greitas dalinimasis failais, tiesioginės transliacijos, kriptovaliutos, tamsusis internetas (Dark Web) ir stipraus šifravimo programinė įranga. Tačiau jie taip pat naudojami tuo, kad technologijų sektoriaus veiksmams, turintys padėti veiksmingai kovoti su šia problema, dažnai yra nekoordinuoti ir pavėluoti.

Naujos technologijos gali būti sprendimo dalis. Pavyzdžiui, Interpolo dirbtiniu intelektu pagrįsta vaikų seksualinės prievartos duomenų bazė, kurioje naudojama vaizdų ir vaizdo įrašų palyginimo programinė įranga, kad būtų galima greitai nustatyti ryšius tarp aukų, smurtautojų ir veikimo vietų. Tačiau vien technologija problemos neišspręs.

Siekiant sumažinti skaitmeninės revoliucijos riziką, tuo pačiu leidžiant vis daugiau jaunų žmonių pasinaudoti jos teikiamais pranašumais, bendradarbiavimas su suinteresuotosiomis šalimis kaip niekada svarbus. Vyriausybės, pilietinė visuomenė, vietos bendruomenės, tarptautinės organizacijos ir kitos šios pramonės suinteresuotosios šalys turi susivienyti dėl bendro tikslo.

Tai pripažindamos, 2018 m. ITU valstybės narės paprašė išsamiai atnaujinti mūsų gaires dėl [vaikų apsaugos internete](#). Šios naujos ITU gairės buvo permąstytos, perrašytos ir pertvarkytos, kad atspindėtų reikšmingiausias pokyčius skaitmeniniame pasaulyje, kuriame atsiduria šios kartos vaikai. Šis naujasis leidimas ne tik atspindi naujus skaitmeninių technologijų ir platformų pokyčius, bet ir atkreipia dėmesį į svarbią spragą: situaciją, su kuria susiduria neįgalūs vaikai, kuriems internetinis pasaulis suteikia ypač svarbų įrankį visaverčiam ir prasmingam gyvenimui - dalyvavimą socialiniame gyvenime.

Technologijų pramonė turi atlikti svarbų ir aktyvų vaidmenį kuriant pagrindus saugesniam interneto paslaugų ir kitų technologijų naudojimui šiandienos vaikams ir ateities kartoms.

Verslas vis dažniau turi skirti svarbesnį vaidmenį vaikų interesams, ypatingą dėmesį sutelkiant į jaunų vartotojų asmens duomenų privatumo apsaugą, jų teisės į saviraiškos laisvę išsaugojimą, kovoti su vis didėjančia CSAM rykšte ir užtikrinti, kad būtų sukurtos sistemos vaiko teisių pažeidimams veiksmingai spręsti.

Ten, kur šalies įstatymai dar neatitinka tarptautinės teisės, verslas turi galimybę ir atsakomybę suderinti savo veiklos sistemas su aukščiausiais standartais ir geriausia praktika.

Tikimės, kad paslaugų teikėjams šios gairės bus tvirtas pagrindas kuriant verslo politiką ir naujoviškus sprendimus. Atsižvelgdamas į tikrąją ITU, kaip pasaulinio vienytojo, dvasią, aš didžiuojuosi, kad šios gairės yra pasaulinio bendradarbiavimo rezultatas ir kad jos buvo parašytos bendromis plačios tarptautinės bendruomenės ekspertų pastangomis.

Taip pat džiaugiuosi galėdama pristatyti mūsų naująjį COP (Child Online Protection) talismaną Sango: draugišką, atkaklų ir bebaimį personažą, kurį grupė vaikų sukūrė pagal ITU naują tarptautinę jaunimo informavimo programą.

Amžiuje, kai vis daugiau jaunų žmonių prisijungia prie interneto, ITU vaikų apsaugos gairės yra svarbesnės nei bet kada. Pramonė, vyriausybės, tėvai ir pedagogai, taip pat patys vaikai vaidina ypač svarbų vaidmenį. Esu dėkinga, kaip visada, už jūsų paramą ir tikiuosi tęsti glaudų bendradarbiavimą šiuo kritiniu klausimu.



Doreen Bogdan-Martin
Direktorė

Telekomunikacijų plėtros biuras, ITU

1. Apžvalga

Šiuo dokumentu tikimasi padėti suinteresuotosioms IRT pramonės šalims sukurti vaikų apsaugos internete (COP) priemones. Šių gairių, skirtų vaikų apsaugai internete, tikslas yra pateikti naudingą, lanksčią ir patogią sistemą įmonėms ir jų atsakomybei apsaugoti vartotojus. Jos taip pat skirtos sukurti saugesnio interneto paslaugų ir susijusių technologijų naudojimo pagrindą vaikams ir ateities kartoms.

Šiomis gairėmis taip pat siekiama padėti verslui suteikiant įrankius didelėms ir mažoms įmonėms bei suinteresuotosioms šalims sukurti ir išlaikyti patrauklų ir tvarų verslo modelį, kartu suprantant teisinę ir moralinę atsakomybę dėl vaikų ir visuomenės.

Reaguodami į didelę pažangą technologijų ir konvergencijos srityje, ITU, UNICEF ir vaikų apsaugos internete partneriai sukūrė ir atnaujino gaires įvairiausioms įmonėms, kurios kuria, teikia ar naudoja telekomunikacijas ar užsiima susijusia veikla teikdamos produktus ir paslaugas.

Naujos gairės vaikų apsaugai internete yra konsultacijų su COP iniciatyvos nariais, taip pat platesnių konsultacijų su pilietinės visuomenės, verslo, akademinės bendruomenės atstovais, vyriausybėmis, žiniasklaida, tarptautinėmis organizacijomis ir jaunimu rezultatas.

Šio dokumento tikslas yra:

- nustatyti bendrą informacinių ir ryšių technologijų bei interneto pramonės ir atitinkamų suinteresuotųjų šalių atskaitos tašką ir gaires;
- teikti įmonėms gaires, kaip atpažinti, užkirsti kelią ir sumažinti bet kokį neigiamą jų produktų ir paslaugų poveikį vaikų teisėms;
- teikti įmonėms gaires, kaip jos gali apsaugoti vaikų teises ir skatinti atsakingą skaitmeninį vaikų pilietiškumą;
- pasiūlyti bendrus principus, kurie sudarytų nacionalinius ar regioninius įsipareigojimus visose susijusiose pramonės šakose, suprantant, kad skirtingų tipų įmonės naudos skirtingus įgyvendinimo modelius.

Taikymo sritis

Vaikų apsauga internete yra didelis iššūkis, apimantis įvairius valdymo, politikos, veiklos, techninius ir teisinius aspektus. Šiose gairėse, remiantis esamais ir gerai pripažintais modeliais, sistemomis ir kitomis nuorodomis, bandoma atkreipti dėmesį į daugelį šių sričių, jas sutvarkyti ir nustatyti prioritetus.

Gairėse daugiausia dėmesio skiriama vaikų apsaugai visose srityse ir nuo bet kokio skaitmeninio pasaulio pavojaus, todėl pabrėžiama pramonės suinteresuotųjų šalių geroji praktika, kuria galima remtis rengiant, kuriant ir valdant įmonės COP politiką. Jos teikia pramonės subjektams rekomendacijas ne tik apie tai, kaip valdyti ir apriboti neteisėtą veiklą internete, prieš kurią jie įsipareigoja kovoti (pvz., prieš vaikų seksualinio išnaudojimo medžiagą (CSAM) internete) naudodamiesi savo teikiamomis paslaugomis, bet ir sutelkti dėmesį į kitus klausimus, kurie visais atvejais negali būti apibrėžiami kaip nusikaltimai visose jurisdikcijose. Tai apima smurtą tarp bendraamžių, elektronines patyčias ir priekabiavimą internete, taip pat klausimus, susijusius su privatumu ar bendra gerove, sukčiavimu ar kitomis grėsmėmis, kurios gali būti žalingos vaikams tik tam tikrais atvejais.

Šiuo tikslu šiose gairėse pateikiamos gerosios praktikos rekomendacijos sprendžiant vaikams kylančios rizikos skaitmeniniame pasaulyje klausimus bei kaip elgtis siekiant vaikams sukurti saugią aplinką internete. Šiose gairėse pateikiami patarimai, kaip pramonė gali padėti užtikrinti vaikų saugumą naudojant IRT, internetą ar bet kurią susijusią

technologiją ar įrenginį, įskaitant mobiliuosius telefonus, žaidimų konsoles, prie interneto prijungiamus žaislus, laikrodžius, daiktų internetą ir dirbtiniu intelektu pagrįstas sistemas. Todėl šiose gairėse pateikiami pagrindiniai klausimai ir iššūkiai, susiję su vaikų apsauga internete ir pasiūlymai įmonėms ir suinteresuotosioms šalims dėl veiksmų kuriant vietinę ir vidaus politiką. Šios gairės neapima tokių aspektų kaip faktinis kūrimo procesas ar tekstas, kuris galėtų būti įtrauktas į vaikų apsaugos internete taisykles.

Struktūra

1 skyrius – apžvalga: šiame skyriuje pabrėžiamas šių gairių tikslas, taikymo sritis ir tikslinė auditorija.

2 skyrius – įvadas į vaikų apsaugą internete: šiame skyriuje pateikiama vaikų apsaugos internete apžvalga, tam tikra pagrindinė informacija, įskaitant išskirtinę neįgalių vaikų situaciją. Be to, jame pateikiami esamų tarptautinių ir nacionalinių vaikų apsaugos internete modelių pavyzdžiai, kaip galimos suinteresuotų asmenų intervencijos sritys.

3 skyrius – pagrindinės vaikų teisių apsaugos sritys: šiame skyriuje pateikiamos penkios pagrindinės sritys, kuriose įmonės gali imtis veiksmų, kad vaikai galėtų saugiai ir teigiamai naudoti IRT.

4 skyrius – bendrosios gairės: šiame skyriuje pateikiamos rekomendacijos visoms pramonės suinteresuotosioms šalims dėl vaikų saugumo naudojant IRT ir teigiamo IRT naudojimo, įskaitant atsakingą vaikų skaitmeninį pilietiškumą, skatinimo.

5 skyrius – su ypatybėmis susiję kontroliniai sąrašai: šiame skyriuje suinteresuotoms šalims pateikiamos konkrečios rekomendacijos dėl veiksmų saugant vaikų teises, įtraukiant šias ypatybes:

- Ypatybė A: teikti ryšio, duomenų saugojimo ir informacijos prieglobos paslaugas
- Ypatybė B: prižiūrimo skaitmeninio turinio pasiūla
- Ypatybė C: talpinti vartotojų sukurtą turinį ir sujungti vartotojus
- Ypatybė D: dirbtiniu intelektu valdomos sistemos

Tikslinė auditorija

Remiantis Jungtinių Tautų verslo ir žmogaus teisių pagrindiniais principais¹, vaiko teisės ir verslo principai ragina įmones vykdyti savo pareigą gerbti vaikų teises, vengiant bet kokio neigiamo poveikio, susijusio su jų veikla, produktais ar paslaugomis. Šie principai taip pat aiškiai nurodo skirtumą tarp pagarbos (minimalaus pagarbos lygio, reikalingo verslui, kad nebūtų padaryta žala vaikams) ir paramos (pavyzdžiui, imantis savanoriškų veiksmų, kuriais siekiama skatinti vaiko teisių apsaugą). Verslas turi užtikrinti vaikų teisę į apsaugą internete, prieigą prie informacijos ir saviraiškos laisvę, kartu skatinant teigiamą vaikų naudojimąsi IRT. Tradiciniai skirtumai tarp skirtingų telekomunikacijų ir mobiliųjų telefonų pramonės dalių bei interneto bendrovių ir transliuotojų greitai nyksta ir tampa neryškūs. Konvergencija sujungia šiuos anksčiau skirtingus skaitmeninius srautus į vieną srovę, pasiekiančią milijardus žmonių visose pasaulio vietose. Bendradarbiavimas ir partnerystė yra raktai, kuriant saugesnio interneto ir susijusių technologijų naudojimo pagrindus. Vyriausybės, privatus sektorius, politikos formuotojai, pedagogai, pilietinė visuomenė, tėvai ir globėjai atlieka svarbų vaidmenį siekiant šio tikslo. Pramonė gali veikti penkiose pagrindinėse srityse, kaip aprašyta 3 skyriuje.

¹ Jungtinių Tautų verslo ir žmogaus teisių pagrindiniai principai.

2. Kas yra vaikų apsauga internete?

Per pastaruosius 10 metų interneto naudojimas ir vaidmuo žmonių gyvenime labai pasikeitė. Dėl išmaniųjų telefonų ir planšetinių kompiuterių paplitimo, „Wi-Fi“ ir 4G technologijų prieinamumo bei socialinės žiniasklaidos platformų ir programėlių plėtros, daugėja priežasčių interneto naudojimui.

2019 m. daugiau nei pusė pasaulio gyventojų naudojami internetu. Didžiausia interneto vartotojų dalis yra jaunesni nei 44 metų žmonės, o interneto naudojimas vienodai didelis tarp 16–24 metų ir 35–44 metų žmonių. Pasauliniu lygiu kas trečias interneto vartotojas yra vaikas (0–18 metų), o UNICEF skaičiavimais, 71 proc. jaunų žmonių yra pastoviai prisijungę prie interneto². Interneto prieigos taškų gausa, mobiliosios technologijos ir didėjantis interneto prieinamų įrenginių asortimentas kartu su didžiuliais ištekliais, kuriuos galima rasti virtualioje erdvėje, suteikia neregėtas galimybes mokytis, dalytis ir bendrauti.

IRT naudojimas suteikia geresnę prieigą prie informacijos apie socialines paslaugas, švietimo išteklius ir sveikatos patarimus. Kai vaikai, jaunimas ar šeimos naudojami internetu bei mobiliaisiais telefonais ieškodami informacijos ir pagalbos bei pranešdami apie piktnaudžiavimo atvejus, šios technologijos gali padėti apsaugoti vaikus ir jaunimą nuo smurto ir išnaudojimo. Vaikų apsaugos paslaugų teikėjai taip pat naudojami IRT rinkti ir perduoti duomenis, taip palengvindami gimimo registravimą, bylų valdymą, šeimos narių paiešką, duomenų rinkimą ir smurto žemėlapij.

Be to, internetas padidino prieigą prie informacijos visuose pasaulio kampeliuose, suteikdamas vaikams ir jaunimui galimybę tyrinėti beveik bet kurią dominančią temą, naudotis pasaulio žiniasklaida, siekti profesinių perspektyvų ir įgyvendinti idėjas. IRT naudojimas suteikia vaikams ir jaunimui galimybę ginti savo teises ir pareikšti savo nuomonę, taip pat leidžia jiems užmegzti ryšius ir bendrauti su savo šeima ir draugais. IRT taip pat yra svarbiausias kultūrinių mainų būdas ir pramogų šaltinis.

Nepaisant didžiulės interneto naudos, vaikai ir jaunimas, naudodamiesi IRT, taip pat gali susidurti su daugybe pavojų. Jie gali būti paveikti netinkamo turinio, įskaitant potencialius seksualinius prievartautojus. Jie gali neigiamai paveikti savo reputaciją paskelbdami asmeninę informaciją internete arba rašydami seksualinio turinio žinutes (angl. sexting), dažnai nesuvokdami savo veiksmų pasekmių bei išliekančių „skaitmeninių pėdsakų“. Jie taip pat susiduria su privatumo internete rizika, kylančia dėl jų asmeninės informacijos rinkimo.

Vaiko teisių konvencija, kuri yra plačiausiai ratifikuota tarptautinė žmogaus teisių sutartis,³ nustato pilietines, politines, ekonomines, socialines ir kultūrines vaikų teises. Ji nustato, kad visi vaikai ir jaunimas turi teisę į mokslą, laisvalaikį, žaidimus ir kultūrą, tinkamą informaciją, minties ir saviraiškos laisvę, privatumą bei gali išreikšti savo nuomonę jiems aktualiais klausimais, atsižvelgiant į jų besikeičiančius gebėjimus. Konvencija taip pat apsaugo vaikus ir jaunimą nuo bet kokio smurto, išnaudojimo, prievartos ir bet kokios rūšies diskriminacijos, o be to nurodo, kad, sprendžiant bet kokią su vaikais susijusį klausimą, pirmiausia turi būti atsižvelgiama į vaiko interesus. Tėvai, globėjai, pedagogai ir bendruomenės nariai, įskaitant bendruomenės vadovus ir pilietinės visuomenės veikėjus, yra atsakingi už vaikų ir jaunimo auklėjimą ir pagalbos jiems suteikimą sulaukus pilnametystės. Vyriausybės vaidina svarbų vaidmenį užtikrinant, kad visi suinteresuoti subjektai atliktų šį vaidmenį.

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

³ Jungtinių Tautų vaiko teisių konvencija. Visos šalys, išskyrus tris, (Somalis, Pietų Sudanas ir JAV) ratifikavo Vaiko teisių konvenciją.

Saugodamos vaikų teises internete, įvairių pramoninių atstovai turi bendradarbiauti, kad būtų užtikrinta vaikų teisių apsauga ir pusiausvyra tarp jų teisės gauti informaciją bei saviraiškos laisvės. Todėl įstaigos turėtų teikti pirmenybę vaikų ir jaunimo apsaugos internete priemonėms, kurios yra tikslingos ir nėra pernelyg ribojančios nei vaiką, nei kitus vartotojus. Be to, vis labiau sutariama, kad skatinti skaitmeninį vaikų ir jaunimo pilietiškumą ir kurti produktus bei platformas, palengvinančias teigiamą vaikų naudojimąsi IRT, turėtų būti privataus sektoriaus prioritetas.

Nors internetinės technologijos suteikia daug galimybių vaikų ir jaunimo bendravimui, naujų įgūdžių įgijimui, skatina kūrybiškumą ir prisideda prie visuomenės gerinimo, jos taip pat gali kelti pavojų vaikų ir jaunimo saugumui. IRT priemonės gali sukelti riziką vaikams ir jauniems žmonėms dėl privatumo, neteisėto turinio, priekabiavimo, elektroninių patyčių, netinkamo asmens duomenų naudojimo ar viliojimo seksualiniais tikslais ir netgi vaikų seksualinio išnaudojimo klausimais. Taip pat gali būti padaryta žala vaikų reputacijai, įskaitant „keršto pornografiją“, susijusią su neskelbtinos asmeninės informacijos, tokios kaip seksualinio pobūdžio pranešimų, nuotraukų ar vaizdo įrašų pavišimu internete. Jie taip pat susiduria su rizika dėl privatumo internete. Vaikai pagal savo amžių ir besiformuojančią brandą dažnai negali iki galo suvokti su internetiniu pasauliu susijusios rizikos ir galimo neigiamo netinkamo jų elgesio pasekmių sau ir kitiems.

Nepaisant privalumų, yra ir naujų bei pažangesnių technologijų naudojimo trūkumų. Dirbtinio intelekto ir automatizuoto mokymosi, virtualios ir papildytos realybės, didžiųjų duomenų, robotikos ir daiktų interneto plėtra turėtų dar labiau pakeisti vaikų ir jaunimo interneto priemonių naudojimą. Nors šios technologijos daugiausia kuriamos siekiant išplėsti paslaugų teikimo sritį ir padidinti patogumą (pvz.: teikiant pagalbą balsu, gerinant prieinamumą ir naujas skaitmeninio formos), kai kurios tokios technologijos gali turėti nenumatytą poveikį ir netgi gali būti panaudotos vaikų prievartautojų. Norint sukurti saugią aplinką vaikams ir jaunimui internete, reikia veiksmingo vyriausybės, privataus sektoriaus ir visų suinteresuotųjų subjektų dalyvavimo. Dėmesys skaitmeniniams tėvų ir pedagogų įgūdžiams ir raštingumui taip pat turi būti vienas iš pirmųjų tikslų, kurį įgyvendinant pramonė gali atlikti gyvybiškai svarbų ir tvarų vaidmenį.

Kai kurie vaikai gerai supranta riziką internete ir elgiasi atitinkamai. Tačiau to negalima pasakyti apie visus vaikus, ypač tarp pažeidžiamų grupių. Pagal Jungtinių Tautų darnaus vystymosi tikslų 16.2 punktą, kurio tikslas - nutraukti prievartą, išnaudojimą, prekybą žmonėmis ir visų formų smurtą ir kankinimus prieš vaikus, vaikų apsauga internete yra ypatingai svarbi.

Nuo 2009 m. ITU sukurta tarptautinė įvairių suinteresuotųjų šalių iniciatyva „COP Initiative“ skirta informuoti apie vaikams internete kylančią riziką ir kaip su ja kovoti. Iniciatyva suburia partnerius iš visų pasaulinės bendruomenės sektorių, kad vaikams užtikrintų saugų interneto naudojimą. Įgyvendindama šią iniciatyvą, 2009 m. ITU paskelbė COP gairių rinkinį keturioms grupėms: vaikams; tėvams, globėjams ir pedagogams; pramonei; ir politikos formuotojams. Vaikų apsauga šiose gairėse suprantama kaip viską apimantis būdas reaguoti į visas galimas grėsmes ir žalą, su kuria vaikai ir jaunimas gali susidurti tiek internete, tiek dėl kitų internetinių technologijų. Šiame dokumente vaikų apsauga internete taip pat apima žalą vaikams, daromą vaikams už interneto ribų, tačiau susijusią su smurtu ir prievarta patiriama internete. Be to, kad atsižvelgiama į vaikų elgesį ir veiklą internete, vaikų apsauga internete taip pat nurodo ne tik vaikų, bet ir kitų asmenų netinkamą technologijų naudojimą siekiant išnaudoti vaikus.

Visos susijusios suinteresuotos šalys turi padėti vaikams ir jaunimui pasinaudoti interneto teikiamomis galimybėmis bei įgyti skaitmeninio raštingumo ir atsparumo pavojams, kylantiems jų gerovei ir apsaugai internete.

Vaikų ir jaunimo apsauga yra bendra visų suinteresuotųjų šalių atsakomybė. Kad tai įvyktų, politikos formuotojai, pramonės atstovai, tėvai, globėjai, pedagogai ir kiti suinteresuotieji subjektai turi užtikrinti, kad vaikai ir jaunimas galėtų išnaudoti savo galimybes tiek internete, tiek ir už jo ribų.

Nors nėra visuotinio apibrėžimo, vaikų apsauga internete laikosi holistinio požiūrio kuriant saugią, amžių atitinkančią ir įtraukiančią skaitmeninę vaikų ir jaunimo erdvę, kuriai būdinga:

- reagavimas, pagalba ir gebėjimas padėti sau iškilus grėsmei;
- žalos prevencija;
- dinamiška pusiausvyra tarp apsaugos užtikrinimo ir galimybės vaikams tapti skaitmeniniais piliečiais suteikimo;
- vaikų ir visuomenės teisių bei pareigų laikymasis.

Be to, dėl sparčios technologijų ir visuomenės pažangos bei interneto sienų nebuvimo, norint, kad vaikų apsauga internete būtų veiksminga, ji turi būti greitai prisitaikanti. Technologinių priemonių naujovės sukuria naujus iššūkius, o kiekviename regione jie yra skirtingi. Geriausias būdas tai išspręsti yra pasaulinės bendruomenės bendradarbiavimas, nes tai leistų sprendimus rasti greičiau.

2.1 Papildoma informacija

Kadangi internetas yra visiškai integruotas į vaikų ir jaunimo gyvenimą, negalima į skaitmeninį ir fizinį pasaulį žiūrėti atskirai.

Toks ryšys suteikė nepaprastą įgalinimą. Internetinis pasaulis leidžia vaikams ir jauniems žmonėms įveikti trūkumus ir negalią, o be to jis sukūrė naują pramogų, švietimo, dalyvavimo ir santykių kūrimo aplinką. Dabartinės skaitmeninės platformos naudojamos įvairiai veiklai ir dažnai yra daugialypės.

Manoma, kad prieiga prie šių technologijų ir sugebėjimas jomis naudotis yra labai svarbūs veiksniai jaunimo vystymuisi. Kadangi IRT pirmą kartą panaudojamos dar ankstyvame amžiuje, yra labai svarbu žinoti, kad vaikai ir jaunimas dažnai pradeda naudotis platformomis ir paslaugomis dar nepasiekę nustatyto minimalaus amžiaus, kurį turi taikyti technologijų pramonė, todėl švietimas turėtų būti integruotas į visas vaikų naudojamas paslaugas internete.

2.1.1 Vaikai skaitmeniniame pasaulyje

Prieiga prie interneto

2019 m. daugiau nei pusė pasaulio gyventojų naudojami internetu (53,6 proc.) - apytiksliai 4,1 milijardo vartotojų. Pasauliniu lygiu, kas trečias interneto vartotojas yra vaikas iki 18 metų amžiaus⁴. UNICEF duomenimis, visame pasaulyje 71 proc. jaunų žmonių jau naudojami

⁴ Livingstone, S., Carr, J., ir 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>.

internetu⁵. Nepaisant minimalaus amžiaus, „Ofcom“ (Jungtinės Karalystės komunikacijų reguliavimo tarnyba) skaičiuoja, kad beveik 50 procentų vaikų nuo 10 iki 12 metų jau turi paskyras socialiniuose tinkluose.⁶ Dabar vaikai ir jaunimas internete užima didelį, svarbų ir pastovų vaidmenį. Internetas tarnauja kitiems socialiniams, ekonominiams ir politiniams tikslams ir tapo šeimos ar kitų vartotojų produktu ar paslauga, neatsiejama nuo šeimos, vaikų ir jaunimo gyvenimų.

2017 m. regioniniu lygiu vaikų ir jaunimo galimybė naudotis internetu buvo glaudžiai susijusi su nacionalinių pajamų lygiu. Šalyse, kurių gyventojai gauna mažas pajamas, interneto vartotojų yra mažiau nei šalyse, kuriose pajamos didelės. Daugumos šalių vaikai ir jaunuoliai internete daugiau laiko praleidžia savaitgaliais nei darbo dienomis, o 15–17 metų paaugliai internete praleidžia ilgiausiai laiko – 2.5–5.3 valandos, priklausomai nuo šalies.

Interneto naudojimas

Tarp vaikų ir jaunimo populiariausias priegys prie interneto prietaisas yra mobilusis telefonas, po kurio seka stacionarūs ir nešiojamieji kompiuteriai. Vaikai ir jaunimas vidutiniškai per savaitę internete praleidžia dvi valandas per vieną darbo dieną ir keturias valandas kiekvieną savaitgalio dieną. Nors kai kurie prie interneto yra prisijungę nuolatos, daug kitų savo namuose vis dar neturi priegys prie interneto. Praktiškai dauguma vaikų ir jaunuolių, kurie naudojami internetu, prie jo prisijungia naudodami daugiau nei vieną įrenginį, o tie, kurie prisijungia bent kas savaitę, dažnai naudojami ne daugiau kaip trimis skirtingais įrenginiais. Vyresni ir iš turtingesnių šalių kilę vaikai prietaisų paprastai naudoja daugiau, o berniukai naudoja šiek tiek daugiau prietaisų nei mergaitės kiekvienoje apklaustoje šalyje.

Populiariausia mergaičių ir berniukų veikla yra vaizdo įrašų žiūrėjimas. Daugiau nei trys ketvirtadaliai internetu besinaudojančių vaikų ir jaunuolių teigia, kad bent kartą per savaitę žiūri vaizdo įrašus internete vieni ar su kitais savo šeimos nariais. Daugelį vaikų ir jaunuolių galima laikyti „aktyviais socialiais veikėjais“, naudojančiais keletą socialinės žiniasklaidos platformų, tokių kaip „Facebook“, „Twitter“, „Tik tok“ ar „Instagram“. Vaikai ir jaunimas taip pat internete dalyvauja politikoje ir pateikia savo nuomones rašydami tinklaraščius.

Bendras dalyvavimo internetiniuose žaidimuose lygis įvairiose šalyse atitinkamai priklauso nuo vaikų ir jaunimo priegys prie interneto. Tačiau internetinių žaidimų prieinamumas greitai keičiasi, o vaikų ir jaunimo, pirmą kartą prisijungusių prie internetinių žaidimų, amžius jaunėja.

Kas savaitę 10–30 proc. internetu besinaudojančių apklaustų vaikų ir jaunuolių užsiima kūrybine veikla internete.⁷ Švietimo tikslais daugelis bet kokio amžiaus vaikų ir jaunuolių kas savaitę naudojami internetu atlikdami namų darbus ar netgi norėdami pasivyti bendraamžius dėl praleistų pamokų ar internete tiesiog ieško informacijos apie sveikatą. Panašu, kad vyresni vaikai informacijos ieško dažniau nei jaunesni.

⁵ Plačiajuosčio ryšio komisija, „Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019),“ *Broadband Commission for Sustainable Development*, 2019 m. spalio, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf

⁶ BBC, „Under-age social media use ‘on the rise’, says Ofcom“.

⁷ Livingstone, S., Kardefelt Winther, D., and Hussein, M. (2019). „Global Kids Online“ lyginamoji ataskaita, „Innocenti“ tyrimų ataskaita. UNICEF tyrimų biuras - Innocenti, Florencija, <https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html>.

Vaikų seksualinis išnaudojimas ir prievarta internete

Vaikų seksualinis išnaudojimas ir prievarta (CSEA) internete auga stulbinančiai. Prieš dešimtmetį buvo užfiksuota mažiau nei milijonas bylų dėl prievartos prieš vaikus. 2019 m. šis skaičius išaugo iki 70 mln. (nuo 2018 m. jis padidėjo beveik 50 procentų). Be to, pirmą kartą išnaudojimo vaizdo įrašų skaičius pralenkė valdžios institucijoms skirtuose pranešimuose pateiktų nuotraukų skaičių, o tai rodo poreikį imtis naujų priemonių, reikalingų šiai tendencijai pašalinti. CSEA internete aukos patenka į visas amžiaus grupes, tačiau amžius vis jaunėja. 2018 m. interneto karštųjų linijų tinklas [INHOPE](#) atkreipė dėmesį į aukų profilių pasikeitimą iš paauglių į mažamečius. Be to, 2018 m. ECPAT International ir INTERPOL tyrimai parodė, kad vis jaunesni vaikai kenčia nuo smurto, įskaitant kankinimus, prievartavimą ar sadizmą. Tai apima kelių dienų, savaitių ar mėnesių amžiaus kūdikius. Nors mergaitės yra labiau paveiktos, berniukų prievarta gali būti sunkesnė. Ta pati ataskaita rodo, kad 80 proc. aukų, nurodytų ataskaitose, buvo mergaitės, o 17 proc. - berniukai. Abiejų lyčių vaikai buvo paminėti 3-uose procentuose įvertintų pranešimų.⁸

Momentinė duomenų nuotrauka⁹

- Kas trečias interneto vartotojas visame pasaulyje yra vaikas.
- Kas pusę sekundės vaikas pirmą kartą prisijungia prie interneto.
- 800 milijonų vaikų naudojami socialiniais tinklais.
- Apskaičiuota, kad vienu metu internete 750 000 asmenų seksualiniais tikslais bando susisiekti su vaikais.
- EUROPOL saugykloje yra daugiau nei 46 milijonai unikalių vaikų seksualinio išnaudojimo (CSAM) vaizdų ar vaizdo įrašų.
- Daugiau nei 89 procentai aukų yra nuo 3 iki 13 metų amžiaus.

Norėdami gauti daugiau informacijos apie mastą ir atsaką į CSEA internete, apsilankykite [WePROTECT Global Alliance](#).

2.1.2 Įvairių platformų įtaka vaikų skaitmeninei patirčiai

Internetas ir skaitmeninės technologijos vaikams ir jaunimui ne tik suteikia galimybes, bet ir kelia riziką. Toliau pateikiame kelis pavyzdžius.

Kai vaikai naudojami socialiniais tinklais, jie išnaudoja puikias galimybes tyrinėti, mokytis, bendrauti ir lavinti pagrindinius įgūdžius. Vaikai socialinius tinklus laiko platformomis, leidžiančiomis saugioje aplinkoje tyrinėti savo asmeninę tapatybę. Jaunimui svarbu turėti atitinkamų įgūdžių ir žinoti, kaip spręsti problemas, susijusias su privatumu ir reputacija.

“Žinau, kad viskas, ką skelbiame internete, išlieka ir tai gali turėti įtakos mūsų gyvenimui ateityje”, 14-metis berniukas, Čilė.

Tačiau, atlikus apklausas, kurios rodo, kad dauguma vaikų naudoja socialinius tinklus dar nesulaukę 13 metų amžiaus, o tinkamo amžiaus užtikrinimo galimybės yra menkos arba jų visai nėra, rizika, su kuria susiduria vaikai, gali būti labai rimta. Be to, nors vaikai nori išmokti skaitmeninių įgūdžių, tapti skaitmeniniais piliečiais ir kontroliuoti savo privatumą, jie linkę

⁸ ECPAT and Interpol, “Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: summary report”, 2018.

⁹ End Violence Against Children, “Safe Online”.

savo privatumą saugoti savo draugų ir pažįstamų tarpe - „Ką gali matyti mano draugai?“ – nepagalvodami apie svetimus žmones bei trečiuosius asmenis. Tai, kartu su natūraliu vaikų smalsumu ir paprastai didesne jiems kylančia rizika, gali padaryti juos pažeidžiamus viliojimui, išnaudojimui, patyčioms ar kitokio pobūdžio žalingam turiniui.

Plačiai paplitęs dalijimasis nuotraukomis ir vaizdo įrašais per mobiliąsias programas, ypač vaikams naudojant tiesioginės transliacijos platformas, kelia papildomų problemų ir pavojų privatumui. Kai kurie vaikai kuria savo, draugų ir brolių bei seserų seksualines nuotraukas ir jomis dalijasi internete. 2019 m. beveik trečdalyje (29 proc.) visų interneto svetainių, kurias įtraukė IWF, buvo tokių nuotraukų. Iš jų 76 proc. sudarė 11–13 metų mergaičių nuotraukos, kurių dauguma buvo fotografuojama miegamuosiuose ar kituose namų kambariuose. Vieniems, ypač vyresniems vaikams, tai gali būti laikoma natūraliu seksualumo ir seksualinės tapatybės tyrinėjimu, o kitiems, ypač jaunesniems, tai dažnai yra prievarta iš suaugusio asmens ar kito vaiko. Kad ir kaip bebūtų, daugelyje šalių toks turinys yra neteisėtas ir gali kelti vaiko patraukimo baudžiamojon atsakomybėn riziką arba būti naudojamas tolesniam vaiko išnaudojimui, prievartavimui ar šantažui.

Internetiniai žaidimai suteikia vaikams panašią galimybę įgyvendinti jų teisę žaisti, taip pat kurti tinklus, leisti laiką su draugais ir susitikti su naujais žmonėmis bei lavinti pagrindinius įgūdžius. Nors tai neabejotinai gali turėti teigiamą poveikį, kai kuriais atvejais žaidimų platformos taip pat gali vaikams kelti riziką, jei jos neprižiūrimos ir nepalaikomos atsakingų suaugusių asmenų. Tai apima didelę finansinę riziką, susijusią su žaidimuose siūlomais pirkiniais, pramonės subjektų renkamais vaikų asmens duomenimis, elektronines patyčias, neapykantos kurstymą, smurtą ir netinkamo elgesio ar turinio naudojimą, viliojimą, o taip pat tikrų, kompiuteriu sukurtų ar net virtualių nuotraukų ar vaizdo įrašų naudojimą, siekiant parodyti ir normalizuoti smurtą prieš vaikus. Ši rizika būdinga ne tik žaidimų platformoms, bet ir kitoms skaitmeninėms vaikų naudojamoms aplinkoms.

Be to, dėl technologijų raidos atsirado „daiktų internetas“, kur vis daugiau ir daugiau prie interneto prijungtų įrenginių gali užmegzti ryšį internetu. Tai apima žaislus, kūdikių monitorius ir dirbtinio intelekto valdomus prietaisus, kurie gali kelti riziką privatumui ir suteikti galimybes nepageidaujamiems asmenims susisiekti su vaikais.

Geroji praktika: tyrimai

Internetinių ar elektroninių patyčių kontekste „Microsoft“ atliko skaitmeninio saugumo ir elektroninių patyčių tyrimus. 2012 m. apklausė 8–17 metų vaikus 25 šalyse dėl žalingo elgesio internete. Rezultatai parodė, kad vidutiniškai 54 procentai dalyvių nurodė, kad jie nerimauja dėl to, kad susidurs su patyčiomis internete; 37 proc. nurodė, kad jie jau nukentėjo nuo tokių patyčių; 24 proc. atskleidė, kad jie tyčiojosi iš kitų. Ta pati apklausa parodė, kad mažiau nei trys iš dešimties tėvų aptarė patyčias internete su savo vaikais. Nuo 2016 m. „Microsoft“ reguliariai atlieka rizikos internete tyrimus teikdama kasmetines „Digital Civility Index“ ataskaitas. „FACES“ yra daugialypės terpės programa, kurią sukūrė „NHK Japan“ ir įvairių viešųjų transliuotojų sąjunga, o šioje programoje tradicinių bei patyčių internete aukos dalijasi savo pasakojimais. Juose paaugliai paaiškina, kaip jie reagavo į išpuolius internete. Pasakojimus, kurie taip pat pateikiami kaip dviejų minučių trukmės vaizdo klipai, naudoja „Facebook“, UNESCO ir Europos Taryba. Jie yra prieinami daugeliu kalbų.

2019 m. UNICEF paskelbė diskusijų dokumentą „Vaiko teisės ir internetiniai žaidimai: vaikų ir pramonės galimybės ir iššūkiai“, kuriuo siekiama atkreipti dėmesį į vaikų galimybes ir iššūkius vienoje iš sparčiausiai augančių pramogų industrijų. Straipsnyje nagrinėjamos šios temos:

- Vaikų teisė žaisti ir teisė į saviraišką (žaidimo laikas ir poveikis sveikatai);
- Diskriminacijos užkirtimas, dalyvavimas ir apsauga nuo prievartos (socialinė sąveika ir įtrauktis, žalinga aplinka, amžiaus ribos ir jų laikymosi užtikrinimas, apsauga nuo viliojimo ir seksualinės prievartos);
- Teisė į privatumą ir apsauga nuo ekonominio išnaudojimo („duomenys už prieigą“ verslo modeliai, nemokami žaidimai ir apmokestinimas, komercinio turinio skaidrumo trūkumas).

Geroji praktika: technologijos

„Google“ virtualios realybės veiksmų laboratorija tiria, kaip virtuali realybė gali paskatinti jaunimą tapti kovotojais prieš patyčias realiame gyvenime ir internete.¹⁰

2019 m. rugsėjo mėn. BBC išleido mobiliąją programėlę „Own IT“ - gerovės programėlę, skirtą 8–13 metų vaikams, gavusiems pirmąjį išmanųjį telefoną. Programa yra dalis BBC įsipareigojimo remti jaunimą kintančioje žiniasklaidos aplinkoje ir yra sėkmingo 2018 m. „Own IT“ tinklalapio atidarymo tęsinys. Programėlė sujungia pažangiausias kompiuterio mokymosi technologijas, kad būtų galima stebėti vaikų aktyvumą išmaniajame telefone ir galimybę patiems vaikams pranešti apie savo emocinę būseną. Šią informaciją programėlė naudoja pritaikyti turinį ir intervencijas, kad vaikai internete galėtų išlikti laimingi ir sveiki, pasiūlydama draugiškus ir gelbstinčius patarimus, kai vaikų elgesys nukrypsta nuo normos. Vartotojai gali naudoti programėlę pagalbos paieškai, tačiau ji taip pat gali suteikti greitus patarimus ekrane, naudojant specialiai pritaikytą klaviatūrą. Įranga atlieka šias funkcijas:

- Primena vartotojams gerai pagalvoti prieš dalinant asmeninę informaciją socialiniuose tinkluose (pvz., mobiliaisiais numeriais).
- Padeda suprasti, kaip pranešimus gali suvokti kiti, kol pranešimas dar neišsiųstas.
- Stebi vartotojo nuotaiką laikui bėgant ir teikia pasiūlymus, kaip, prireikus, galima pagerinti situaciją.
- Teikia informaciją tokiomis temomis kaip telefonų naudojimas vėlai vakare ir poveikis vartotojų gerovei.

Programėlėje pateikiamas specialus turinys iš BBC. Joje pateikiama naudinga medžiaga ir išteklių, padedantys jauniems žmonėms kuo geriau išnaudoti laiką internete ir sukurti sveiką elgesį ir įpročius internete. Tai padeda jauniems žmonėms ir tėvams konstruktyviau kalbėtis apie savo patirtį internete, tačiau neteikia ataskaitų ar atsiliepimų tėvams ir jokie duomenys nepalieka vartotojų įrenginių. Programėlė nerenka jokių vartotojo sukurtų asmens duomenų ar turinio, nes visas kompiuterinis mokymasis vyksta programėlėje ir vartotojo įrenginyje. Įrenginiai yra pritaikomi pagal mokymo duomenis, kad būtų užtikrinta, jog privatumas nebus pažeistas.

2.1.3 Išskirtinė neįgalių vaikų situacija ¹¹

Negalią turintys vaikai ir jaunuoliai internete susiduria ne tik su visiems kylančia rizika, tačiau, be to, jie gali susidurti su specifine rizika dėl jų negalios. Neįgalūs vaikai ir jaunimas

¹⁰ Daugiau informacijos žr. Alexa Hasse ir kt., "Youth and Cyberbullying: Another Look", „Berkman Klein“ interneto ir visuomenės centras, 2019.

¹¹ Žr. Europos Tarybos pranešimą - "Two clicks forward and one click back: report on children with disabilities in the digital environment", 2019.

dažnai susiduria su atskirtimi, stigmatizacija ir kliūtimis (fizinėmis, ekonominėmis, visuomenės ir požiūrio sąlygomis) dalyvauti savo bendruomenėse. Šie išgyvenimai gali turėti neigiamos įtakos neįgaliam vaikui ir paskatinti jį ieškoti socialinių santykių ir draugystės interneto erdvėse. Nors tokia sąveika gali būti teigiama padedant ugdyti savigarbą ir kuriant pagalbos tinklus, tačiau tokiems vaikams taip pat gali kilti didesnė verbavimo internete ir (arba) seksualinio priekabiavimo rizika. Tyrimai rodo, kad vaikams ir jaunuoliams, patiriantiems sunkumų bei turintiems psichosocialinių problemų realiame gyvenime, kyla didesnė rizika.¹²

Bendrai kalbant, tikėtina, kad realiame gyvenime viktimizuojami vaikai taip pat bus viktimizuojami ir internete. Tai neįgaliesiems vaikams kelia dar didesnę riziką, tačiau būtent šios grupės vaikams prieiga prie interneto yra labai reikalinga. Tyrimai rodo, kad neįgalūs vaikai dažniau patiria prievartą,¹³ o ypač seksualinę.¹⁴ Viktimizacija gali apimti patyčias, priekabiavimą, atskirtį ir diskriminaciją dėl faktinės ar tariamos vaiko negalios arba su jo negalia susijusių aspektų, pavyzdžiui, elgesio ar kalbėjimo būdo ar naudojamos įrangos ar paslaugų.

Vilioti ir (arba) seksualiai priekabiauti prie neįgalių vaikų ir jaunimo internete gali išskirtinai negalią turinčių vaikų ir jaunuolių ieškantys išnaudotojai. Tarp tokių pažeidėjų gali būti „aistruoliai“ – negalios neturintys asmenys, kuriuos seksualiai traukia neįgalieji (dažniausiai galūnes praradę žmonės ir asmenys, naudojantys pagalbines judėjimo priemones), o kai kurie iš jų net ir patys apsimeta neįgaliaisiais.¹⁵ Tokių žmonių veiksmai gali apimti neįgalių vaikų ir jaunimo nuotraukų ir vaizdo įrašų atsisiuntimą (nežalingo pobūdžio) ir (arba) pasidalijimą jais per tam skirtus forumus ar socialinių tinklų paskyras. Pranešimų įrankiai forumuose ir socialiniuose tinkluose dažnai neturi tinkamų priemonių kovoti su tokia problema.

Kyla susirūpinimas, kad „sharenting“ (kai tėvai internete dalijasi savo vaikų bei jaunimo informacija bei nuotraukomis) gali pažeisti vaiko privatumą, sukelti patyčias ir priversti jausti gėdą arba turėti neigiamų pasekmių vėliau gyvenime.¹⁶ Kai kurie neįgalių vaikų tėvai gali dalytis savo vaiko informacija ar nuotraukomis siekdami pagalbos ar patarimų, o dėl to gali kilti pavojus vaiko privatumo pažeidimui. Tokie tėvai taip pat rizikuoja būti įtakoti nepakankamai informuotų ar kenkėjiškų paskatų vedamų žmonių, siūlančių gydymo būdus, terapiją ar netgi greitą vaiko negalios išgydymą. Kai kurie neįgalių vaikų ir jaunuolių tėvai taip pat gali būti pernelyg atsargūs, nes jiems trūksta žinių, kaip geriausiai kontroliuoti vaiko naudojimąsi internetu arba apsaugoti nuo patyčių ar priekabiavimo.¹⁷

Kai kurie neįgalūs vaikai ir jaunuoliai gali susidurti su sunkumais naudodamiesi internetu ar net būti iš jo išstumti dėl nepasiekiamo dizaino (pvz., programėlių, neleidžiančių padidinti teksto dydžio), negauti pageidaujamų pagalbinių priemonių (pvz., ekrano skaitytuvo

¹² Andrew Schrock ir kt., „[Solicitation, Harassment, and Problematic Content](#)“, „Berkman Klein“ interneto ir visuomenės centras, 2008.

¹³ UNICEF, „[State of the World's Children Report: Children with Disabilities](#),” 2013.

¹⁴ Katrin Mueller-Johnson ir kt., „[Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors](#)“, Tarpasmeninio smurto žurnalas, 2014.

¹⁵ Richard L Bruno, „[Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder](#)“, Seksualumas ir negalia, 1997.

¹⁶ UNICEF, „[Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy](#)“, „Innocenti“ diskusijų straipsnis 2017-03 .

¹⁷ UNICEF, „[Is there a ladder of children's online participation?](#)“, „Innocenti“ tyrimų apžvalga, 2019.

programinės įrangos neregiams ar kitų pritaikomųjų kompiuterinių programų) arba tinkamos pagalbos (pvz., instruktažo, kaip naudotis įranga, individualios pagalbos socialinėse sąveikose).¹⁸

2.2 Esami nacionaliniai ir tarptautiniai vaikų apsaugos internete modeliai

Vaikų ir jaunimo apsaugai internete pasauliniu lygiu yra taikomi keli modeliai. Suinteresuotieji pramonės subjektai turėtų tai laikyti tarptautinių iniciatyvų gairėmis ir struktūra, užtikrinančia, kad jie netaupytų pastangų vaikų ir jaunimo apsaugai internete. Interneto pramonė yra įvairi ir sudėtinga erdvė, sudaryta iš skirtingų dydžių ir funkcijų įmonių. Labai svarbu, kad vaikų apsauga būtų užtikrinama ne tik turinį siūlančiose platformose ir paslaugose, bet ir tose, kurios palaiko interneto infrastruktūrą.

Reikia pažymėti, kad pramonės pajėgumas įgyvendinti visapusišką vaikų apsaugos politiką ribojamas turimų išteklių. Todėl šiose gairėse pramonės įmonėms rekomenduojama bendradarbiauti diegiant paslaugas vartotojų apsaugai. Išteklių ir inžinerinės patirties dalijimasis pramonės įmonėse galėtų efektyviau sukurti „saugias erdves“, kad būtų išvengta piktnaudžiavimo.

Pramonės bendradarbiavimas

[Technologijų koalicija](#) yra sėkmingo pramonės suinteresuotųjų šalių bendradarbiavimo kovojant su CSEA internete pavyzdys.

Tarptautiniai modeliai

Pramonės įmonės turėtų į savo struktūrinę programą įtraukti atitinkamas tarptautines gaires, taip pat laikytis visų atitinkamų nacionalinių ar tarptautinių jų veiklos šalyse taikomų teisės aktų. Pramonės atstovai turėtų atsižvelgti ne tik į veiksmus, kurių turi imtis teisiniu lygmeniu, bet ir į tai, kokią veiklą jie gali atlikti, ir, jei įmanoma, siekti įgyvendinti iniciatyvas visame pasaulyje. Kai kurie modeliai, kurie pateikia tokių iniciatyvų principus, yra:

- Penki šalies ministerijų [principai, skirti kovai su CSEA internete](#) (2020);
- Plačiajuosčio ryšio komisija tvariam vystymuisi: [Vaikų saugumas internete: smurto, prievartos ir išnaudojimo internete rizikos mažinimas](#) (2019);
- „WePROTECT Global Alliance“: [Pasaulinis strateginis atsakas į vaikų seksualinį išnaudojimą ir prievartą internete](#) (2019);
- Visuotinė partnerystė siekiant panaikinti smurtą prieš vaikus: [Saugus mokymasis: raginimas veikti](#);
- Vaiko orumas skaitmeniniame pasaulyje: [Vaiko orumo aljansas: technologijų darbo grupės ataskaita](#) (2018 m.);
- [Europos Parlamento ir Tarybos direktyva \(ES\) 2018/1808: garso ir vaizdo žiniasklaidos paslaugų direktyva](#);
- [Europos Komisijos bendrasis duomenų apsaugos reglamentas](#) (2018 m.);
- [OECD rekomendacija dėl vaikų apsaugos internete](#) (2012).

Nacionaliniai modeliai

¹⁸ Šių teisių gaires rasite [Jungtinių Tautų neįgalųjų teisių konvencijoje ir fakultatyviniame protokole](#), ypač 9 straipsnyje apie prieinamumą ir 21 straipsnyje apie saviraiškos ir nuomonės laisves bei galimybes naudotis informacija.

Yra daugybė nacionalinių ir tarptautinių modelių, kurie nustato aiškų technologijų pramonės vaidmenį ir atsakomybę sprendžiant vaikų apsaugos internete klausimus. Kai kurie iš jų nėra skirti būtent vaikų apsaugai, tačiau gali būti taikomi jiems, kaip interneto vartotojams. Šie modeliai teikia bendrąsias gaires pramonei dėl reguliavimo politikos, standartų ir bendradarbiavimo su kitais sektoriais. Šiame dokumente pabrėžiami pagrindiniai tokių modelių principai, taikomi IRT pramonei.

Amžių atitinkančio modelio kodeksas, Jungtinė Karalystė

2019 m. pradžioje Informacijos komisaro biuras paskelbė pasiūlymus amžiui tinkamo modelio kodeksui dėl vaikų duomenų apsaugos. Siūlomas kodeksas grindžiamas vaiko interesais, kaip nustatyta Jungtinių Tautų vaiko teisių konvencijoje, ir pateikia keletą lūkesčių pramonei. Kodeksas susideda iš penkiolikos standartų, įskaitant vietos nustatymo paslaugų išjungimą pagal numatytuosius nustatymus vaikams, pramonei rinkti ir saugoti tik mažiausią vaikų asmens duomenų kiekį ir tik tam, kad kuriami produktai būtų asmeniniai, o paaiškinimai atitiktų vartotojų amžių ir būtų prieinami.

Žalingo skaitmeninio ryšio įstatymas, Naujoji Zelandija

2015 m. įstatymas patyčias internete įvardino kaip nusikaltimą ir daugiausia dėmesio skiria įvairiai patyčių internete sukeliamai žalai ir keršto pornografijai. Juo siekiama sustabdyti žalingą bendravimą internete arba jį sumažinti, todėl skelbti bendravimo įrašus internete ketinant sukelti emocinę žalą yra draudžiama, o tam nustatoma 10 bendravimo principų. Tai suteikia vartotojams teisę skųstis nepriklausomai organizacijai, jei šie principai pažeidžiami, arba kreiptis dėl teismo sprendimo prieš viešintoją, jei problema neišspręsta.

Internetinio saugumo komisaras, Australija

2015 m. įkurtas Australijos **internetinio saugumo komisaras** yra pirmoji pasaulyje vyriausybinių agentūra, skirta kovoti su piktnaudžiavimu internetu ir saugoti savo piliečius internete. Ši agentūra, kaip nacionalinė nepriklausoma interneto saugumo reguliuotoja, turi galingą funkcijų derinį. Tai apima prevenciją, informuotumo didinimą, švietimą, mokslinius tyrimus ir geriausios praktikos gaires, ankstyvą įsikišimą ir žalos taisymą pasitelkiant įvairias įstatymų numatytas reguliavimo schemas, suteikiančias internetinio saugumo komisarui galimybę greitai sustabdyti patyčias internete, piktnaudžiavimą vaizdais ir neteisėtą turinį internete. Ši plati kompetencija leidžia agentūrai iš anksto įvairiapusiškai ir holistiškai užkirsti kelią internetu daromai žalai.

2018 m. „eSafety“ sukūrė iniciatyvą „Safety by Design“ (SbD), kurioje vartotojų apsauga ir teisės yra svarbiausi kuriant, plėtojant ir diegiant produktus ir paslaugas internete. Iniciatyvos centre yra apsaugos taisyklių rinkinys pagal projektavimo principus, kuriuose pramonės įmonėms nustatomos realistiškos, veiksmingos ir įgyvendinamos priemonės, kurių imamasi siekiant geriau apsaugoti piliečius internete. Trys pagrindinės taisyklės yra:

- 1) Paslaugų teikėjo atsakomybė:** saugos našta niekada neturėtų tekti tik galutiniam vartotojui. Gali būti imamasi prevencinių veiksmų siekiant užtikrinti, kad žinomos ir numatomos žalos būtų įvertintos kuriant ir teikiant internetinę paslaugą, taip pat veiksmų, kad paslaugos mažiau palengvintų, pakurstytų ar paskatintų neteisėtą ir netinkamą elgesį.
- 2) Vartotojo įgalinimas ir autonomija:** vartotojų orumas ir jų interesai yra labai svarbūs. Žmogaus atstovavimas ir autonomija turėtų būti palaikomi ir stiprinami kuriant paslaugas, leidžiančias vartotojams geriau kontroliuoti ir valdyti savo patirtį.
- 3) Skaidrumas ir atskaitomybė:** tai yra tvirto požiūrio į saugumą bruožai, užtikrinantys, kad paslaugos veikia pagal skelbiamus saugos tikslus, o taip pat informuojantys visuomenę apie veiksmus, kurių galima imtis sprendžiant saugos problemas.

„WePROTECT“ pasaulinis aljansas

„WePROTECT“ pasaulinio aljanso strategijos esmė yra pagalba šalims parengti koordinuotas įvairių suinteresuotųjų šalių priemones kovai su vaikų seksualiniu išnaudojimu internete, vadovaujantis jo pavyzdiniu nacionaliniu atsaku (angl. Model National Response), kuris veikia kaip nacionalinių veiksmų planas. Jis suteikia šalims modelį kovai su vaikų seksualiniu išnaudojimu internete. Nacionalinis pavyzdinis „WePROTECT“ atsakas turi aiškius IRT įmonių įsipareigojimus, susijusius su:

- pranešimo apie draudžiamą turinį ir jo pašalinimo (angl. notice and takedown) procedūromis;
- pranešimais apie vaikų seksualinį išnaudojimą ir prievartą (CSEA) internete;
- technologinių sprendimų kūrimu; ir
- investicijomis į veiksmingas COP prevencines programas ir reagavimo paslaugas.

Pasaulinė partnerystė ir fondas, skirtas nutraukti smurtą prieš vaikus

Visuotinę partnerystę ir fondą, skirtą nutraukti smurtą prieš vaikus, 2016 m. įkūrė Jungtinių Tautų generalinis sekretorius, siekdamas vieno tikslo: paskatinti ir paremti veiksmus, kad iki 2030 m. būtų panaikintas visų formų smurtas prieš vaikus, sujungiant daugiau nei 400 partnerių iš visų sektorių.

Pagrindinis dėmesys skiriamas aukų gelbėjimui ir paramai, technologiniams sprendimams, leidžiantiems nustatyti ir užkirsti kelią nusikaltimams, teisėsaugos, įstatymų leidybos ir politikos reformų palaikymui, duomenų ir įrodymų apie CSEA internete mastą ir pobūdį rinkimui bei vaikų mąstymo suvokimui.¹⁹

3. Pagrindinės vaikų teisių apsaugos ir propagavimo sritys

Šiame skyriuje pateikiamos penkios pagrindinės sritys, kuriose įmonės gali imtis veiksmų, siekdamas apsaugoti vaikus ir jaunimą internete, ir skatinti teigiamą IRT naudojimą.

3.1 Vaiko teisių aspektų integravimas į įmonės politiką ir valdymo procesus

Vaiko teisių aspektų integravimas reikalauja, kad įmonės imtųsi tinkamų priemonių, kad nustatytų, užkirstų kelią, sušvelnintų ir prireikus ištaisytų galimą ir faktinį neigiamą poveikį vaiko teisėms. Jungtinių Tautų verslo ir žmogaus teisių pagrindiniai principai kviečia visus verslo subjektus ir pramonės įmones nustatyti tinkamą politiką ir procesus, užtikrinančius žmogaus teises.

¹⁹ Daugiau informacijos žr. End Violence Against Children, “Grantees of the End Violence Fund”.

Pramonės atstovai turėtų atkreipti ypatingą dėmesį į vaikus ir jaunimą kaip į pažeidžiamą grupę, atsižvelgdami į jų duomenų apsaugą ir saviraiškos laisvę. [Jungtinių Tautų Generalinės Asamblėjos rezoliucija 68/167](#) dėl teisės į privatumą skaitmeniniame amžiuje dar kartą patvirtina teisę į privatumą ir saviraiškos laisvę, o taip pat draudžia bet kokį neteisėtą teisių pažeidimą. Be to, [Jungtinių Tautų Žmogaus teisių tarybos rezoliucijoje 32/13](#) dėl žmogaus teisių į internetą skatinimo ir apsaugos pripažįstamas globalus ir atviras interneto pobūdis, kaip varomoji jėga spartinant pažangą ir patvirtinama, kad realiame gyvenime turimos žmonių teisės turi būti išlaikomos ir internete. Valstybėse, kuriose nėra tinkamos teisinės sistemos vaikų ir jaunimo teisėms į privatumą ir saviraiškos laisvei apsaugoti, įmonės turėtų ypatingai rūpintis, kad politika ir praktika atitiktų tarptautinę teisę. Kadangi ryšių internete dėka jaunimo pilietinis aktyvumas ir toliau didėja, įmonės turi didesnę atsakomybę apsaugoti vaikų ir jaunimo teises, net jei vietos įstatymai dar neatitinka tarptautinių standartų.

Bendrovės turėtų įdiegti operatyvinio lygio skundų mechanizmą, kuris suteiktų nukentėjusiems asmenims galimybę pareikšti susirūpinimą dėl galimų pažeidimų. Operatyvinio lygio mechanizmai turėtų būti prieinami vaikams, jų šeimoms ir tiems, kurie atstovauja jų interesams. Verslo ir žmogaus teisių pagrindinių principų 31-ame punkte paaiškinama, kad tokie mechanizmai turėtų būti teisėti, prieinami, žinomi, teisingi, skaidrūs, suderinami su teisėmis, o taip pat būti nuolatinio mokymosi šaltiniai ir pagrįsti įsitraukimu bei dialogu. Kartu su vidiniais procesais, siekiant pašalinti neigiamą poveikį, skundų nagrinėjimo mechanizmai turėtų užtikrinti, kad įmonėse būtų sukurtos sistemos, užtikrinančios tinkamą vaikų ir jaunimo teisių apsaugą.

Kai įmonės laikosi reikalavimų, susijusių su IRT sauga, daugiausia dėmesio skiriant nacionalinių įstatymų laikymuisi, tarptautinėms rekomendacijoms, kai nėra atitinkamų nacionalinių teisės aktų, ir siekiant išvengti vaikų ir jaunimo teisių pažeidimo, tuomet įmonės aktyviai skatina vaikų ir jaunimo raidą ir gerovę savanoriškais veiksmais užtikrinamos vaikų ir jaunimo teises į informaciją, saviraišką, dalyvavimą, švietimą ir kultūrą.

Geroji praktika: politika ir amžiui tinkamas modelis

Programėlių kūrėjas „Toca Boca“ gamina skaitmeninius žaislus, remdamasis vaikų perspektyva. Šios įmonės [privatumo politika](#) orientuota į įmonės surinktos informacijos ir jos panaudojimo principų dalijimąsi. „Toca Boca, Inc“ yra „[PRIVO Kids Privacy Assured COPPA Safe Harbor](#)“ [sertifikavimo programos narė](#).

„LEGO® Life“ yra saugios socialinės žiniasklaidos platformos, skirtos vaikams iki 13 metų, pavyzdys, kaip saugiai galima dalytis savo „LEGO“ kūriniais, surasti įkvėpimą ir bendrauti. Paskyros sukūrimui iš vaikų neprašoma pateikti jokios asmeninės informacijos, o jos sukūrimas galimas tik nurodžius tėvų ar globėjų el. pašto adresą. Programėlė suteikia galimybę vaikams ir šeimoms aptarti saugumą ir privatumą internete teigiamoje aplinkoje.

Amžiui tinkamo modelio pavyzdžiai yra kai kurių pagrindinių viešųjų paslaugų transliuotojų tam tikroms amžiaus grupėms skirti pasiūlymai: pavyzdžiui, Vokietijos ARD („Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland - Das Erste“) ir ZDF („Zweites Deutsches Fernsehen“) tikslinė auditorija yra nuo 14 metų amžiaus, siūlant pritaikytą turinį per interneto kanalą [funk.net](#). BBC (British Broadcasting Corporation) sukūrė „[CBeebies](#)“, skirtą jaunesniems nei 6 metų vaikams. Svetainės turinys yra specialiai pritaikytas atitinkamoms amžiaus grupėms.

Geroji praktika: politika ir technologijos

„Twitter“ nuolat investuoja į patentuotas technologijas, kurios sumažino žmonių poreikį pranešti apie žalingas žinutes.²⁰ Tiksliau kalbant, daugiau nei 50 proc. žinučių (angl. Tweets), palyginti su 20 proc. 2018 m., dėl kurių daromos žalos „Twitter“ imasi veiksmų, šiuo metu yra aktyviai nustatoma naudojant technologijas, o ne pasikliaujant „Twitter“ vartotojų pranešimais. Naujoji technologija naudojama privačios informacijos, neskelbtino turinio, neapykantos skleidimo, piktnaudžiavimo ir apsimetinėjimo politikos sričių problemoms spręsti.

3.2 Standartinių procesų, skirtų kovai su vaikų seksualinio išnaudojimo medžiaga (CSAM), kūrimas

2019 m. IWF patvirtino, kad 132 676 patikrintose interneto svetainėse buvo aptikta vaikų seksualinio išnaudojimo medžiaga.²¹ Bet kokia interneto svetainė gali turėti šimtus ar net tūkstančius nuotraukų ir vaizdo įrašų. Iš visų IWF patikrintų nuotraukų, 45 proc. jų buvo nufotografuoti 10 metų ar jaunesni vaikai. 1 609 interneto svetainėse buvo aptikta medžiaga, kurioje buvo užfiksuoti 0–2 metų vaikai, o 71 proc. iš jų vaizdavo sunkiausio laipsnio seksualinę prievartą, pavyzdžiui, išžaginimą ir seksualinį kankinimą. Šie nerimą keliantys faktai pabrėžia pramonės, vyriausybės, teisėsaugos ir pilietinės visuomenės bendradarbiavimo svarbą kovojant su seksualine vaikų prievarta.

Nors daugelis vyriausybių kovoja su seksualine vaikų prievarta ir jos įrašų platinimu priimdamos teisės aktus, persekiodamos smurtautojus ir keldamos baudžiamąsias bylas, didindamos sąmoningumą ir padėdamos vaikams ir jaunimui atsigauti nuo prievartos ar išnaudojimo, yra daug šalių, kurios dar neturi tinkamų sistemų. Kiekvienoje šalyje reikalingi mechanizmai, kad plačioji visuomenė galėtų pranešti apie tokio pobūdžio piktnaudžiavimą ir išnaudojimą. Pramonė, teisėsauga, vyriausybės ir pilietinė visuomenė turi dirbti kartu, kad būtų užtikrinta tinkama teisinė sistema, atitinkanti tarptautinius standartus. Tokios sistemos turėtų būti drausti visas seksualinio vaikų išnaudojimo formas ir apsaugoti vaikus, kurie yra tokios prievartos ar išnaudojimo aukos. Šios sistemos turi užtikrinti, kad pranešimų teikimo, tyrimų ir turinio pašalinimo procesai veiktų kuo efektyviau.

Pramonė turėtų pateikti nuorodas į nacionalines interneto karštąsias linijas ar kitas vietoje pasiekiamas interneto karštąsias linijas, tokias kaip IWF portalai kai kuriose šalyse, o, jei vietinių galimybių nėra, pateikti nuorodas į kitas tarptautines interneto karštąsias linijas, tokias, kaip, pavyzdžiui, **Jungtinių Valstijų nacionalinis dingusių ir išnaudotų vaikų centras (NCMEC)** arba **Tarptautinė interneto karštųjų linijų asociacija (INHOPE)**, kur pranešimui pateikti gali būti naudojama bet kuri tarptautinė interneto karštoji linija.

Atsakingos įmonės imasi daugybės veiksmų, kad jų tinklai ir paslaugos nebūtų naudojami seksualinės vaikų prievartos turinio platinimui. Tai įtraukiama į vartojimo sąlygas ir elgesio kodeksus, kurie aiškiai draudžia tokį turinį ar elgesį;²² patikimų pranešimo apie draudžiamą turinį ir jo pašalinimo (angl. notice and takedown) procesų kūrimą; bendradarbiavimą su nacionalinėmis interneto karštosiomis linijomis.

²⁰ Twitter, „15th Transparency Report: Increase in proactive enforcement on accounts“.

²¹ IWF, „The why. The how. The who. And the results. Annual Report 2019“.

²² Pažymėtina, kad netinkamas vartotojo elgesys neapsiriboja CSAM ir kad bet kokio pobūdžio netinkamą elgesį ar turinį įmonė turėtų reaguoti atitinkamai.

Be to, kai kurios įmonės taiko technines priemones, kad būtų išvengta piktnaudžiavimo jų paslaugomis ar tinklais dalijantis jau žinoma medžiaga apie seksualinę vaikų prievartą. Pavyzdžiui, kai kurie interneto paslaugų teikėjai blokuoja prieigą prie tam tikrų puslapių, kuriuose atitinkamos institucijos patvirtina kaip turinčius tokios medžiagos arba jei svetainė patalpinta šalyje, kurioje nėra procesų, užtikrinančių, kad ji bus greitai panaikinta. Kiti taiko maišos (angl. hashing) technologijas, kad automatiškai aptiktų ir pašalintų seksualinės prievartos prieš vaikus vaizdus, kurie jau žinomi teisėsaugai ar interneto karštosioms linijoms. Pramonės atstovai turėtų apsvarstyti ir į savo veiklą įtraukti visas atitinkamas priemones, kad būtų išvengta seksualinės prievartos prieš vaikus sklaidos.

Pramonės subjektai turėtų įsipareigoti paskirstyti atitinkamus išteklius ir toliau kurti bei dalytis, pageidautina, atvirojo kodo technologiniais sprendimais, kad būtų galima nustatyti ir pašalinti vaikų seksualinio išnaudojimo medžiagą (CSAM).

Geroji praktika: technologijos

„Microsoft“ taiko keturių krypčių metodą, skatindama atsakingą ir saugų technologijų naudojimą, daugiausia dėmesio skirdama pačiai technologijai, savivaldai, partnerystėms ir vartotojų švietimui bei informavimui. „Microsoft“ taip pat turi įterptų funkcijų, kurios padeda žmonėms veiksmingiau valdyti jų saugumą internete. „Šeimos sauga“ (angl. „Family Safety“) yra viena iš tokių savybių, leidžiančių tėvams ir globėjams stebėti jų vaikų veiklą internete.

„Microsoft“ įgyvendina politiką prieš priekabiavimą savo platformose, o vartotojams, kurie piktnaudžiauja šiomis taisyklėmis, gresia paskyros panaikinimas arba, jei būtų nustatyti rimtesni pažeidimai, teisėsaugos priemonės.

Microsoft PhotoDNA yra įrankis, kuris sukuria vaizdų maišas (angl. hashes) ir lygina jų reikšmes su jau identifikuotų ir patvirtintų vaikų seksualinio išnaudojimo medžiagos (CSAM) maišų reikšmių duomenų baze. Jei jis randa atitikimą, vaizdas užblokuojamas. Šis įrankis leido turinio tiekėjams iš interneto pašalinti milijonus neteisėtų nuotraukų; padėjo nuteisti vaikų prievartautojus; ir kai kuriais atvejais padėjo teisėsaugai išgelbėti potencialias aukas, užkertant kelią nusikaltimams, prieš jiems įvykstant. „Microsoft“ jau seniai yra įsipareigojusi apsaugoti savo klientus nuo neteisėto jos gaminių ir paslaugų turinio bei taiko savo sukurtą technologiją kovai su tokiu nelegalių vaizdo įrašų platinimu. Tačiau šiame įrankyje nenaudojama veido atpažinimo technologija, todėl negalima nustatyti paveikslėlyje esančio asmens ar objekto. Bet išradus „PhotoDNA for Video“ viskas pasisuko nauja linkme. „PhotoDNA for Video“ padalina vaizdo įrašą į smulkias dalis ir, iš esmės, sukuria tų vaizdų maišas. Lygiai taip pat, kaip „PhotoDNA“ gali nustatyti, kad nuotrauka buvo pakeista, siekiant išvengti aptikimo, „PhotoDNA for Video“ gali surasti pakeistą ar į, atrodytų, eilinį vaizdo įrašą įterptą vaikų seksualinio išnaudojimo turinį.

Be to, „Microsoft“ neseniai sukūrė naują įrankį, leidžiantį identifikuoti vaikų prievartautojus, bandančius suvilioti vaikus pokalbiais internete. Projektas „Artemis“, sukurtas bendradarbiaujant su „The Meet Group“, „Roblox“, „Kik“ ir „Thorn“, remiasi „Microsoft“ užpatentuota technologija ir bus laisvai prieinamas per „Thorn“ kvalifikuotoms interneto paslaugų įmonėms, siūlančioms internetinio pokalbio funkciją. „Project Artemis“ yra technologinė priemonė, perspėjanti administratorius, kai pokalbiuose reikia įsikišimo. Taikant šią viliojimo aptikimo techniką bus galima nustatyti ir pranešti apie prievartautojus, bandančius privilioti vaikus seksualiniais tikslais.

IWF teikia įvairias paslaugas pramonės atstovams, kad jie galėtų apsaugoti savo vartotojus nuo vaikų seksualinio išnaudojimo. Tai apima:

- Dinamišką, kokybišką blokuojamų puslapių sąrašą;
- Žinomos nusikalstamos vaikų seksualinio išnaudojimo medžiagos maišos reikšmių (angl. hashes) sąrašą;
- Unikalių kriptinių terminų ir raktinių žodžių sąrašą, kuris, yra susijęs su vaikų seksualiniu išnaudojimu (CSAM);
- Domenų pavadinimų, žinomų dėl seksualinės vaikų prievartos turinio talpinimo, sąrašą, kad būtų galima greitai pašalinti neteisėtą turinį talpinančius domenus.

3.3 Saugesnės ir amžių atitinkančios interneto aplinkos kūrimas

Labai nedaugelį dalykų gyvenime galima laikyti absoliučiai saugiais ir nerizikingais. Net miestuose, kur eismo judėjimas yra labai reguliuojamas ir atidžiai kontroliuojamas, vis tiek įvyksta avarijos. Lygiai taip pat, virtuali erdvė yra rizikinga, ypač vaikams ir jaunimui. Jiems kylančią riziką galima suskirstyti į keturias sritis:²³

- *Netinkamas turinys* – vaikai ir jaunimas gali atsitiktinai surasti netinkamą ir neteisėtą turinį ieškodami ko nors kito, spustelėdami tariamai nekenksmingą nuorodą pranešime, tinklaraštyje ar dalindamiesi failais. Jie taip pat gali ieškoti netinkamos ar pagal amžių jautrios medžiagos. Tai, kas laikoma žalingu turiniu, skiriasi kiekvienoje šalyje; pavyzdžiai apima turinį, kuriame skatinamas piktnaudžiavimas narkotinėmis medžiagomis, rasinė neapykanta, rizikingas elgesys, savižudybės, anoreksija ar smurtas.
- *Netinkamas elgesys* – vaikai ir suaugusieji gali naudoti internetą priekabiavimui ar net kitų žmonių išnaudojimui. Vaikai kartais gali rašyti skaudžius komentarus ar rodyti nepadorius vaizdus, gali pavogti turinį ar pažeisti autorių teises.
- *Netinkamos pažintys* – tiek suaugusieji, tiek jaunimas gali naudotis internetu vaikų ar kitų pažeidžiamų jaunų žmonių paieškai. Dažnai jų tikslas yra įtikinti auką, kad jie sukūrė prasmingus santykius, tačiau pagrindinis tikslas yra manipuliuojantis. Jie gali bandyti įtikinti vaiką atlikti seksualinius ar kitokius žalingus veiksmus internete, naudodamiesi internetine kamera ar kitu įrašymo įrenginiu, arba bandyti suorganizuoti asmeninį susitikimą. Šis procesas dažnai vadinamas viliojimu (angl. „grooming“).
- *Komercinė rizika* – Ši kategorija nurodo duomenų privatumo riziką, susijusią su vaikų duomenų rinkimu ir naudojimu, taip pat su skaitmenine rinkodara. Sauga internete yra bendruomenės iššūkis ir galimybė pramonei, vyriausybėms ir pilietinei visuomenei bendradarbiauti nustatant saugos principus ir praktiką. Pramonė gali pasiūlyti daugybę techninių metodų, įrankių ir paslaugų tėvams, vaikams ir jaunimui. Pirmiausia, ji turėtų sukurti lengvai naudojamus, saugaus dizaino ir amžių atitinkančius produktus plačiajam vartotojų ratui. Papildomi metodai apima priemones, skirtas sukurti tinkamas amžiaus patikros sistemas, kuriose būtų atsižvelgiama į vaikų teises, į privatumą ir prienamumą, arba apriboti vaikų ir jaunimo prieigą prie jų amžiui netinkamo turinio, arba apriboti žmones, su kuriais vaikai gali bendrauti, arba, tiesiog, vaikų praleidžiamą laiką internete. Svarbiausia, kad į „inovacijų ir gaminio projektavimo procesus“ turi būti įtrauktos „saugaus

²³ Sonia Livingstone ir kt., „EU Kids Online: Final Report“, Londono ekonomikos mokykla, 2009.

projektavimo“²⁴ sistemos, įskaitant privatumą. Vaikų saugumas ir atsakingas technologijų naudojimas turi būti kruopščiai apsvarstytas iš anksto.

Kai kurios programos leidžia tėvams matyti žinutes ir kitus pranešimus, kuriuos siunčia ir gauna jų vaikai ir kitas jaunimas. Jei norite naudoti tokio tipo programas, svarbu, kad apie tai būtų atvirai aptarta su vaiku, kitaip toks elgesys gali būti suvokiamas kaip „šnipinėjimas“ ir gali pakenkti pasitikėjimui šeimoje.

Priimtino naudojimo politika yra vienas iš būdų, kaip įmonės gali nustatyti, kokio tipo elgesį skatina tiek suaugusieji, tiek vaikai, kokia veikla yra nepriimtina ir kokios šios politikos pažeidimų pasekmės. Dėl turinio ir elgesio nerimąjantiems vartotojams, pranešimų teikimo mechanizmai turėtų būti prieinami, aiškūs ir skaidrūs. Be to, reikia tinkamai vykdyti pranešimų teikimą laiku pateikiant informaciją apie pranešimo būklę. Nors įmonės gali keisti savo tolesnių veiksmų mechanizmus priklausomai nuo kiekvieno atvejo, būtina nustatyti aiškų pranešimų pateikimo laiką, pranešti apie dėl pranešimo priimtą sprendimą ir pasiūlyti tolesnių veiksmų planą, jei vartotojas nėra patenkintas atsakymu.

Geroji praktika: pranešimų teikimas

„Facebook“, siekdama pažaboti seksualinį priekabiavimą skaitmeninėse platformose, kartu su Europos Sąjunga, finansavo projektą „deSHAME“, kurio metu „Childnet“, „Gelbėkit vaikus“, „Kek Vonal“ ir „UCLan“ bendradarbiaus siekdamas bendrų tikslų. Šiuo projektu siekiama paskatinti pranešimų apie nepilnamečių seksualinį išnaudojimą internete teikimą ir pagerinti daugiasektorinį bendradarbiavimą užkertant kelią tokiam elgesiui.

Kadangi vienas pagrindinių projekto tikslų yra skatinti vartotojus pranešti apie netinkamą turinį, „Facebook“ bendruomenės standartai taip pat nurodo, ką daryti „Facebook“ leidžia ir ko - ne. Jie taip pat nurodo vartotojų tipus, kuriems skelbti pranešimus yra draudžiama. „Facebook“ taip pat sukūrė saugos funkcijas, tokias kaip „Ar pažįsti šį asmenį?“ funkciją; pašto dėžutę pavadinimu „kiti“, kurioje renkami nauji pranešimai iš vartotojui nepažįstamų žmonių; ir iššokantį langą, kuris pasirodo naujienu sraute, jei atrodo, kad su nepilnamečiu susisiekiama nepažįstamas suaugęs žmogus.

Turinio ir paslaugų internete teikėjai taip pat gali apibūdinti savo teikiamo turinio ar paslaugų pobūdį ir numatomą tikslinę amžiaus grupę. Šie aprašymai turėtų būti suderinti su jau egzistuojančiais nacionaliniais ir tarptautiniais standartais, atitinkamais reglamentais ir patarimais dėl rinkodaros ir reklamos vaikams, kuriuos pateikia atitinkamos klasifikavimo įstaigos. Tačiau šis procesas tampa sunkesnis, nes didėja interaktyvių paslaugų, leidžiančių publikuoti vartotojo sukurtą turinį, pavyzdžiui, per pranešimų lentas, pokalbių kambarius ir socialinių tinklų paslaugas, asortimentas. Kai įmonės specialiai taikosi į vaikus ir jaunimą, o taip pat kai paslaugos yra stipriai nukreiptos į jaunesnes auditorijas, kyla daug didesni lūkesčiai dėl vartotojams pateikiamo **patogaus, lengvai suprantamo ir prieinamo turinio** ir saugumo.

Įmonės taip pat raginamos laikytis aukščiausių privatumo standartų, kai reikia rinkti, tvarkyti ir saugoti iš vaikų ir jaunuolių gaunamus duomenis, nes vaikams ir jaunimui gali trūkti brandos įvertinti platesnes socialines ir asmenines pasekmes atskleidus savo asmeninę informaciją arba ją naudojant komerciniais tikslais. Vaikų ir jaunimo auditorijai skirtos ar juos įtraukiančios paslaugos turi atsižvelgti į jiems kylančią riziką dėl asmeninės informacijos (įskaitant informaciją apie vietą) rinkimo ir naudojimo, o taip pat užtikrinti, kad ši rizika būtų

²⁴ eSafety Commissioner, [Safety by Design Overview](#), 2019

tinkamai pašalinta, o vartotojai - informuoti. Visų pirma, įmonės turėtų užtikrinti, kad reklamose naudojama kalba ir bet kokia medžiaga būtų tinkama, suteikti prieigą prie paslaugų, iš kurių gaunama informacija apie šiuos asmenis, o taip pat padėti vartotojams suprasti ir valdyti jų privatumą, suprantamai paaiškinant su kuo jie sutinka.

Geroji praktika: naujovės

2018–2019 m. UNICEF Rytų Azijos ir Ramiojo vandenyno regioninis biuras surengė penkis suinteresuotųjų šalių apvaliuosius stalus, kad pasidalintų perspektyvia pramonės praktika, kaip kovoti su seksualiniu vaikų išnaudojimu internete. Apskritojo stalo dalyviai buvo pagrindinės privataus sektoriaus įmonės, tokios kaip „Google“, „Facebook“, „Microsoft“, „Telenor“, „Ericsson“, „MobiCom“ (Mongolija) „Mobifone +“ (Vietnamas), „Globe Telecom“ (Filipinai), „True“ (Tailandas), GSMA ir pilietinės visuomenės partneriai, įskaitant INHOPE, ECPAT International ir Child Helpline International organizacijas.

Vykdydama tą patį projektą, 2020 m. vasario mėn., UNICEF įsteigė idėjų grupę (angl. „Think Tank“), siekdama paspartinti pramonės lyderystę Rytų Azijos ir Ramiojo vandenyno regione, kad būtų išvengta smurto prieš vaikus internete. „Think Tank“ yra idėjų ir inovacijų inkubatorius, besiremiantis unikalia pramonės dalyvių (produktų kūrimo, rinkodaros ir kt.) perspektyva, kuriant veiksmingą mokomąją medžiagą ir nustatant efektyviausias pateikimo platformas, taip pat kuriant vertinimo sistemą, siekiant išmatuoti šios mokomosios medžiagos ir vaikams skirtų pranešimų poveikį. Idėjų grupę sudaro „Facebook“, „Telenor“, akademiniai ekspertai, Jungtinių Tautų agentūros, tokios kaip ITU, UNESCO ir UNODC, ir kitos, tokios kaip Australijos internetinio saugumo komisaras, ECPAT International, ICMEC, INTERPOL ir pasaulinis fondas kovai prieš vaikų patiriamą smurtą. „Think Tank“ steigiamasis susitikimas, vykęs kartu su ASEAN regionine vaikų apsaugos internete konferencija, subūrė ekspertus, įskaitant ir „Microsoft“, siekiant ištirti technologijas ir tyrimų galimybes, kaip geriau stebėti elgesio internete pokyčius, remiantis interneto saugos medžiagos ir pranešimų naudojimu.

3.4 Vaikų, tėvų, globėjų ir pedagogų švietimas dėl vaikų saugumo internete ir interneto atsakingo naudojimo

Techninės priemonės gali būti svarbus veiksnys, užtikrinant vaikų ir jaunimo apsaugą nuo galimos rizikos internete, tačiau tai tik vienas iš elementų. Tėvų kontrolės priemonės, sąmoningumo ugdymas ir švietimas taip pat yra svarbūs komponentai, kurie padės įgalinti ir informuoti bet kokio amžiaus vaikus ir jaunimą, o taip pat tėvus, globėjus bei pedagogus. Nors įmonės vaidina svarbų vaidmenį skatinant vaikus ir jaunimą atsakingai ir saugiai naudotis IRT, ši atsakomybė tenka tėvams, mokykloms, vaikams ir jaunimui.

Daug įmonių investuoja į švietimo programas, suteikiančias vartotojams informaciją, reikalingą priimti sprendimus dėl interneto turinio ir paslaugų. Įmonės padeda tėvams, globėjams ir pedagogams nukreipti vaikus ir jaunuolius į saugesnes, atsakingesnes ir tinkamesnes interneto ir mobiliojo telefono paslaugas. Tai apima įspėjimus dėl amžiaus cenzos ir tai, kad informacija apie produktų kainas, prenumeratos sąlygas ar jos atšaukimą būtų aiški. Esant galimybei, visos šalys skatinamos įvesti interneto turiniui atitinkamą amžiaus cenzą socialiniuose tinkluose, taip padedant apsaugoti vaikus nuo žalingo turinio. Labai svarbu paminėti, kad su tuo susijęs asmens duomenų rinkimas gali sukelti poreikį apriboti šios informacijos rinkimą, saugojimą bei jos tvarkymą.

Taip pat svarbu tiesiogiai informuoti vaikus ir jaunimą apie saugesnį IRT naudojimą ir teigiamą bei atsakingą elgesį. Be informuotumo apie saugumo didinimą, įmonės gali

palengvinti teigiamą patirtį, kurdamos turinį vaikams ir jaunimui apie pagarbą, geraširdiškumą ir atvirumą naudojant IRT ir saugant draugus. Įmonės gali suteikti informacijos apie veiksmus, kurių reikia imtis, jei vaikai susiduria su neigiama patirtimi, pvz., patyčiomis internete ar viliojimu, taip palengvindami pranešimą apie tokius įvykius ir suteikdami funkciją atsisakyti anoniminių pranešimų gavimo.

Tėvai kartais internetu bei mobiliaisiais įrenginiais moka naudotis prasčiau nei vaikai ir jaunimas. Be to, mobiliųjų įrenginių ir interneto paslaugų persipynimas tėvams apsunkina priežiūrą. Pramonė gali bendradarbiauti su vyriausybe ir pedagogais, kad būtų galima tėvams suteikti tinkamą kompetenciją auklėti vaikus dėl saugumo ir atsparumo internete. Tikslas nėra perduoti atsakomybę už vaikų ir jaunimo IKT naudojimą tik tėvams, o pripažinti, kad tėvai turi geresnes galimybes nuspręsti, kas tinka jų vaikams, ir kad tėvai turėtų žinoti apie visą kylančią riziką, jog galėtų tinkamai apsaugoti savo vaikus.

Informacija gali būti perduodama realiame gyvenime ir internetu keliais kanalais, atsižvelgiant į tai, kad kai kurie tėvai nesinaudoja interneto paslaugomis. Svarbu bendradarbiauti su mokyklomis, kad tėvams būtų suteikiama mokymo programa ir mokomoji medžiaga dėl vaikų ir jaunimo saugumo internete ir atsakingo IKT naudojimo. Pavyzdžiui, galima pristatyti paslaugas ir įrankius vaikų veiklos internete stebėjimui ar veiksmus, kurių reikia imtis, jei vaikas patiria patyčias internete ar viliojimą, o be to ir kaip išvengti šlamšto ir tvarkyti privatumo nustatymus, bei, galiausiai, kaip kalbėti su skirtingų amžiaus grupių berniukais ir mergaitėmis apie jautrias problemas. Bendravimas yra dvipusis procesas ir daugelis įmonių teikia klientams galimybes susisiekti su jomis pranešimams apie problemas.

Kadangi turinys ir paslaugos tampa vis turtingesni, visiems vartotojams bus labai naudinga gauti patarimų ir priminimų apie konkrečios paslaugos pobūdį ir kaip ja saugiai naudotis. Nors svarbu mokyti vaikus apie atsakingą interneto naudojimą, mes žinome, kad vaikai mėgsta eksperimentuoti, rizikuoti, yra iš esmės smalsūs ir ne visada gali priimti geriausius sprendimus. Galimybė išreikšti save prisideda prie jų augimo ir yra sveikas būdas padėti jiems ugdyti savarankiškumą ir atsparumą tol, kol nepadaroma per didelė žala. Nors vaikams turi būti leista prisiimti tam tikrą riziką interneto aplinkoje, labai svarbu, kad tėvai ir įmonės galėtų jiems padėti, jei įvyktų kas nors blogo, nes tai gali padėti susitvarkyti su neigiamomis jų veiksmų pasekmėmis ir padaryti tai naudinga pamoka.

Geroji praktika: švietimas

„NHK Japan“ „Twitter“ organizuoja [savižudybės prevencijos kampaniją](#) jaunimui: Japonijoje paauglių savižudybių skaičius būna didžiausias, kai jie grįžta į mokyklą po vasaros atostogų. Teigiama, kad grįžimas į realybę yra piko priežastis. „NHK Heart Net TV“ („NHK Japan“) gamybos komanda kuria daugialypės terpės programą [#Rugpjūčio 31-osios naktį](#) (angl. #On the Night of August 31st). Sujungdama televiziją, tiesiogines transliacijas ir socialinius tinklus, NKH sėkmingai sukūrė „vietą“, kurioje paaugliai gali be baimės pasidalinti savo jausmais.

Geroji praktika: švietimas

„Twitter“ taip pat išleido [socialinių tinklų naudojimo raštingumo vadovėlį pedagogams](#). UNESCO parengtas vadovėlis pirmiausia skirtas padėti pedagogams suteikti jaunosioms kartoms socialinių tinklų priemonių naudojimo raštingumo įgūdžius. Kitas „Twitter“ saugos darbo aspektas yra susijęs su jų [informacijos operacijų atskleidimu](#). Tai valstybės remiamų informacijos operacijų archyvas, kuriuo „Twitter“ dalijasi viešai. Inicijatyva buvo pradėta

siekiant padėti akademinei bendruomenei ir visuomenei suprasti su šia tema susijusias kampanijas visame pasaulyje ir paskatinti nepriklausomą, kritinį šios „Twitter“ platformos taktikos vertinimą iš trečiųjų šalių.

Projektas „deSHAME“, bendrai finansuojamas „Facebook“ ir Europos Sąjungos, taip pat padeda kurti išteklius įvairiausioms amžiaus grupėms, ypatingą dėmesį skiriant 9–13 metų vaikams. Vykdamas projektą buvo sukurtas įrankių rinkinys **„Step Up, Speak Up!“** suteikiantis įvairią švietimo, mokymo ir sąmoningumo ugdymo medžiagą, taip pat praktines daugiasektorių prevencijos ir reagavimo strategijų priemones. Projektas suteikia šią mokymosi medžiagą kitoms Europos šalims ir partneriams visame pasaulyje, taip siekiant apginti jaunimo teises į internetą.

„Google“ sukūrė daugybę švietimo iniciatyvų, išteklių ir įrankių, padedančių užtikrinti jaunimo saugumą internete. Viena iš tokių iniciatyvų - **„Be Internet Awesome“** kampanija apie skaitmeninę pilietybę, sukurta bendradarbiaujant su tokiomis organizacijomis kaip „ConnectSafely“, „Family Online Safety Institute“ ir „Internet Keep Safe Coalition“. Ši kampanija skirta 8–11 metų vaikams. Jame yra internetinis žaidimas jaunimui („Interland“), kuriame mokoma skaitmeninių saugos pagrindų, ir ištekliai pedagogams, tokie kaip skaitmeninis pilietiškumas (angl. Digital Citizenship) ir saugumo mokymo programos (angl. Safety Curriculum). Saugumo programoje siūlomi penkių pagrindinių kampanijos teminių sričių pamokų planai, iš kurių vienas orientuotas į patyčias internete. Be to, „Google“ sukūrė skaitmeninio pilietiškumo internete ir saugumo kursą bet kokio amžiaus mokinių pedagogams, suteikdama papildomą pagalbą skaitmeninio pilietiškumo ir saugumo integravimui klasėje. „Google“ taip pat siūlo keletą programų, padedančių tiesiogiai įtraukti jaunus žmones į saugumo internete ir skaitmeninio pilietiškumo programas. Visuotinė „Web Rangers“ iniciatyva yra viena iš tokių programų, mokanti jaunus žmones apie saugumą internete ir skatinanti juos rengti savo kampanijas apie teigiamą ir saugų interneto naudojimą. Taip pat yra konkrečių šalių jaunimui skirtų programų, tokių kaip „Google“ sukurtos „Internet Citizens“ ir „Internet Legends“ programos Jungtinėje Karalystėje.

„Eurovizijos“ jaunimo žinių mainuose, „Eurovizijos“ jaunimo žinių mainuose Europos transliuotojų sąjunga suburia 15 Europos televizijos transliuotojų dalytis programomis, formatais ir sprendimais tiek internete, tiek ir realiame gyvenime. Pastaraisiais metais jų programose svarbiausiu jų akcentu tapo skaitmeninio raštingumo mokymas ir vaikų švietimas apie riziką internete. Tarp sėkmingiausių pastarųjų metų iniciatyvų yra socialinių tinklų reklamos ir vaikams tinkamos naujienų programos, kurias, Norvegijos visuomeninio transliuotojo NRK iniciatyva, sukūrė „Super“ ir „Ultra nytt“.

Geroji patirtis: strateginės partnerystės

Vykdydama projektą **„Sustabdyti smurtą prieš vaikus“** 2018 m. **„Capital Humano y Social Alternativo“** užmezgė partnerystę su didžiausiu Peru interneto, televizijos ir telefoninių paslaugų teikėju „Telefónica“, turinčiu 14,4 mln. klientų, įskaitant daugiau nei 8 milijonus „Movistar“ mobiliojo ryšio vartotojų.

Pagal šią vaisingą partnerystę buvo vykdomos keletas veiklų:

- „Telefónica“, su technine „Capital Humano y Social Alternativo“ pagalba, sukūrė **virtualių kursų vaikų saugumui internete**. Kursas dabar yra atvirai prieinamas „Telefónica“ svetainėje, o žmonė stebi, kiek žmonių į jį užsiregistravo ir sėkmingai baigė. Peru švietimo ministerija sutiko savo oficialioje svetainėje įtraukti prieigą prie šio virtualaus kurso.

- „Capital Humano y Social Alternativo“ sukūrė **brošiūrą apie saugumą internete**, o „Telefónica“ ją išplatino daugiau nei 300 savo mobiliųjų prekybos centrų. Tikslas yra padidinti „Telefónica“ klientų supratimą apie saugumą internete ir rizikas, susijusias su smurtu prieš vaikus internete.
- „Telefónica“, naudodama techninę „Capital Humano y Social Alternativo“ pagalbą, sukūrė Interaktyvų žaidimą apie seksualinį išnaudojimą ir smurtą prieš vaikus (CSEA) internete, kurį jos klientai gali žaisti laukdami savo eilės „Telefónica“ parduotuvėse.

Matydama „Telefónica“ sėkmę, „Capital Humano y Social Alternativo“ pradėjo bendradarbiavimą su interneto ir televizijos paslaugų teikėju „Econocable“, apimančiu atokias ir skurdžias Peru teritorijas.

3.5 Skaitmeninės technologijos, kaip priemonė skatinti pilietinį aktyvumą

Jungtinių Tautų vaiko teisių konvencijos 13 straipsnyje teigiama, kad „vaikas turi teisę laisvai reikšti savo nuomonę; todėl ši teisė apima laisvę ieškoti, gauti ir perduoti bet kokio pobūdžio informaciją ir idėjas nepaisant sienų žodine: rašytine arba spausdinta forma, meno kūriniais arba kitais vaiko pasirinktais būdais“. Įmonės gali vykdyti savo pareigą gerbti vaikų ir jaunimo pilietines ir politines teises užtikrindamos, kad technologijos, o taip pat vaikų ir jaunimo saugumui internete sukurtų teisės aktų ir politikos taikymas nesukeltų nenumatytų pasekmių, apribojančių vaikų dalyvavimo ir išraiškos teises ar neleistų jiems naudotis jų gerovei svarbia informacija. Būtina užtikrinti, kad amžiaus tikrinimo sistemos nepakenktų konkrečių amžiaus grupių poreikiui pasiekti jų vystymuisi svarbų turinį.

Įmonės ir pramonės atstovai gali skatinti vaikų ir jaunimo teises, pateikdami mechanizmus ir priemones, skatinančias jaunimo įsitraukimą. Jie gali pabrėžti interneto teikiamą naudą palengvinant teigiamą įsitraukimą į platesnį pilietinį gyvenimą, socialinės pažangos skatinimą ir bendruomenių tvarumo ir atsparumo didinimą, pavyzdžiui, dalyvaujant socialinėse ir aplinkosauginėse kampanijose ir prisiimant atsakomybę už atitinkamus asmenis. Turėdami tinkamas priemones ir informaciją, vaikai ir jaunimas gali geriau naudotis sveikatos priežiūros, švietimo ir užimtumo galimybėmis bei pareikšti savo nuomonę ir poreikius mokyklose, bendruomenėse bei savo šalyse. Jie įgalinami gauti informaciją apie savo teises ir ieškoti informacijos apie asmeniškai jiems aktualius klausimus, pvz., jų seksualinę sveikatą ir apie politinę bei vyriausybės atskaitomybę.

Įmonės taip pat gali investuoti į vaikams, jaunimui ir šeimoms tinkamo turinio internete kūrimą. Jos gali prisidėti prie vaikų ir jaunimą mokyti bei kurti sprendimus skatinančių technologijų ir turinio plėtros. Jos visada turėtų atsižvelgti į savo produktų saugumą.

Be to, įmonės gali aktyviai remti vaikų ir jaunimo teises, stengdamosi panaikinti skaitmeninę atskirtį. Vaikų ir jaunimo dalyvavimui reikalingas skaitmeninis raštingumas - gebėjimas suprasti ir bendrauti skaitmeniniame pasaulyje. Neturėdami šių galimybių, piliečiai negali dalyvauti daugelyje skaitmenizuotų socialinių veiklų, įskaitant mokesčių mokėjimą, politinių kandidatų palaikymą, internetinių peticijų pasirašymą, gimimo registravimą ar tiesiog priegią prie komercinės, sveikatos, švietimo ar kultūrinės informacijos. Nesiimant veiksmų, atotrūkis tarp šias funkcijas naudojančių ir to negalinčių daryti piliečių ir toliau didės, o pastarųjų situacija tik blogės. Įmonės gali prisidėti prie daugialypės terpės iniciatyvų, skirtų ugdyti

skaitmeninius įgūdžius, reikalingus, kad vaikai ir jaunimas pasitikėtų savimi, palaikytų ryšį ir būtų aktyvūs piliečiai.²⁵ Daugelyje šalių skaitmeninių ir socialinių tinklų priemonių naudojimo raštingumas ir pastangos panaikinti skaitmeninę atskirtį pastaraisiais metais tapo viešosios žiniasklaidos misijos dalimi. Pavyzdžiui, Italijos parlamentas pasiūlė, kad nacionalinio transliuotojo prioritetai būtų skaitmeninės atskirties mažinimas ir vaikų saugumo užtikrinimas tiek internete, tiek ir realiame gyvenime. Tokiu pavyzdžiu galėtų sekti ir kitos šalys.

Geroji patirtis: įmonių bendradarbiavimas

Neseniai „Microsoft“ prisijungė prie organizacijos „No Bully“ pasaulinės kampanijos „Power of ZERO“, kurios tikslas - padėti mažiems vaikams ir jais besirūpinantiems suaugusiems išmokyti gerai naudotis skaitmeninėmis technologijomis ir skatinti nuomonės išreiškimą, užuojautą ir įtrauktį, nes tai yra skaitmeninio pilietiškumo pagrindas. Inicijatyva, mažamečių vaikų pedagogams (kampanija skirta 8 metų ir jaunesniems vaikams) ir šeimoms, siūlo nemokamą mokomąją medžiagą, skirtą padėti mažiems vaikams ugdyti „12 įgūdžių gerumui“ („Power of ZERO“ 12 gyvenimo įgūdžių arba „galių“, kad vaikai galėtų sėkmingai tyrinėti interneto ir realų pasaulį, įskaitant atsparumą, pagarbą, įtrauktį ir kūrybiškumą) ir sukurti jiems tvirtą pagrindą ankstyvame amžiuje.

4. Bendrosios pramonės gairės

1 lentelėje pateikiamos plačios pramonės gairės, kaip nustatyti, užkirsti kelią ir sumažinti bet kokį neigiamą produktų ir paslaugų poveikį vaikų ir jaunimo teisėms ir skatinti teigiamą vaikų ir jaunimo naudojimąsi IRT.

Atkreipkite dėmesį, kad ne visi 1-oje lentelėje išvardyti veiksmai bus tinkami visoms įmonėms ir tarnyboms, o taip pat šioje lentelėje pateikiami ne visi būtini veiksmai. Bendrąsias pramonės gaires papildo konkrečioms funkcijoms reikalingi veiksmai (žr. 5 skyrių) ir atvirkščiai. 2–5 lentelėse konkrečioms funkcijoms pateikiami individualių paslaugų teikimui svarbūs veiksmai. Atminkite, kad konkrečių funkcijų veiksmai gali sutapti, ir kad daugiau nei vienas veiksmas gali būti susijęs su ta pačia paslauga.

1 lentelė. Bendrosios pramonės gairės

Vaiko teisių aspektų integravimas į tinkamą įmonės politiką ir valdymo procesus	Pramonė gali nustatyti, užkirsti kelią ir sušvelninti neigiamą IRT poveikį vaikų ir jaunimo teisėms, o taip pat nustatyti galimybes paremti vaikų ir jaunimo teisių gynimą. Tam galima atlikti šiuos veiksmus:
	Užtikrinti, kad būtų paskirtas konkretus asmuo ir (arba) komanda, atsakinga už šį procesą ir kad jis/ji turėtų prieigą prie būtinų vidaus ir išorės suinteresuotųjų šalių. Įgaliokite šį asmenį ar komandą imtis iniciatyvos didinant vaikų saugumo internete skatinimą visoje įmonėje.

²⁵ Mobilios bendruomenės jaunimo dalyvavimo pavyzdžius žr. čia.

	<p>Parengti vaikų apsaugos taisykles ir (arba) atsižvelgti į vaikų ir jaunimo teisėms kylančią specifinę riziką bei galimybes ir integruoti visa tai į visos įmonės politinius įsipareigojimus (pvz., žmogaus teisės, privatumas, rinkodara ir atitinkami elgesio kodeksai).</p>
	<p>Integruoti atsakingą vaikų saugumo internete klausimo sprendimą į esamas žmogaus teisių ar rizikos vertinimo sistemas (įmonių, produktų ar technologijų ir (arba) šalies lygmeniu), siekiant nustatyti, ar verslas arba pramonė savo veikla gali sukelti neigiamą poveikį ar prisidėti prie jo, ar neigiamas poveikis gali būti tiesiogiai siejamas su jo/jos veikla, produktais ar paslaugomis arba verslo santykiais.</p>
	<p>Nustatyti daromą poveikį įvairių amžiaus grupių vaikų teisėms dėl įmonės veiklos ir produktų bei paslaugų kūrimo, tobulinimo ir pristatymo, o taip pat galimybes saugoti vaikų ir jaunimo teises.</p>

<p>Vaiko teisių integravimas į tinkamą įmonės politiką ir valdymo procesus (tęsinys)</p>	<p>Priimti įgalinimu ir švietimu pagrįstą požiūrį į vaikų apsaugą. Apsvarstykite vaikų duomenų apsaugos teises, jų teisę į privatumą ir žodžio laisvę, kartu teikdami švietimą ir konsultacijas per įmonės paslaugas.</p> <p>Pasinaudokite vidine ir išorine patirtimi ir pasikonsultuokite su pagrindinėmis suinteresuotosiomis šalimis, įskaitant vaikus ir jaunimą, apie vaikų saugos mechanizmus internete, kad gautumėte nuolatinį grįžtamąjį ryšį ir rekomendacijas apie įmonės požiūrį.</p>
	<p>Valstybėse, kuriose nėra tinkamos teisinės sistemos, skirtos apsaugoti vaikų ir jaunimo teises į privatumą ir žodžio laisvę, įmonės turėtų užtikrinti, kad politika ir praktika atitiktų tarptautinius standartus. Žr. Jungtinių Tautų Generalinės asamblėjos rezoliuciją 68/167 dėl teisės į privatumą skaitmeniniame amžiuje.</p>
	<p>Užtikrinti prieigą prie teisių gynimo priemonių, nustatant mechanizmus operacinio lygmens skundams ir pranešimams apie bet kokius vaiko teisių pažeidimus (pvz., seksualinį smurtą prieš vaikus, netinkamą turinį ar asmenis arba privatumo pažeidimus).</p>
	<p>Paskirti vaikų apsaugos politikos vadovą ar kitą paskirtą asmenį, į kurį galima kreiptis dėl su vaikų saugumu susijusių problemų. Jei vaikui kyla grėsmė, vaikų apsaugos politikos vadovas turėtų nedelsdamas įspėti atitinkamas institucijas.</p> <p>Pavyzdžiui, BBC redakcinėse gairėse (2019 m.) nurodomas vaikų apsaugos politikos vadovo paskyrimas, kuris laikomas privalomu valstybinėje žiniasklaidoje.</p>
<p>Pramonės standartų kūrimas siekiant apsaugoti vaikus internete</p>	<p>Sukurti ir įgyvendinti įmonės ir pramonės standartus, skirtus vaikų ir jaunimo apsaugai, atsižvelgiant į specifinę pramonę ir ypatybes.</p>

<p>Standartinių procesų kūrimas kovojant su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu</p>	<p>Bendradarbiaujant su vyriausybe, teisėsaugos institucijomis, pilietine visuomene ir interneto karštųjų linijų organizacijomis, pramonė turi atlikti svarbų vaidmenį kovojant su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu, imdamasi šių veiksmų:</p> <p>Uždrausti įkelti, skelbti, perduoti ar padaryti prieinamą turinį, kuris pažeidžia bet kurios šalies teises arba bet kokius vietos, valstybės, nacionalinius ar tarptautinius įstatymus.</p> <p>Bendrauti su nacionalinėmis teisėsaugos agentūromis arba nacionaline (-ėmis) interneto karštąja (-iomis) linija (-omis), perduodant vaikų seksualinio išnaudojimo medžiagos (CSAM) pranešimus.</p> <p>Parengti vidaus procedūras, kad būtų laikomasi vietos ir tarptautiniuose įstatymuose nustatytos pareigos teikti CSAM pranešimus.</p> <p>Jei įmonė veikia mažiau teisinio reguliavimo ir teisėsaugos kontrolės klausimais išsivysčiusioje rinkoje, ji norinčius pranešti žmones gali nukreipti į Tarptautinę interneto karštųjų linijų asociaciją (INHOPE), kur pranešimus galima pateikti bet kuriai tarptautinei interneto karštajai linijai.</p>
<p>Standartinių procesų kūrimas kovai su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu (tęsinys)</p>	<p>Nustatyti vidaus procedūras, užtikrinančias, kad būtų laikomasi vietinių ir tarptautinių kovos su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu įstatymų.</p> <p>Įsteigti poziciją ar komandą, skirtą integruoti šias procedūras į organizaciją. Pramonės nariai savo metinėje įmonės ataskaitoje turėtų pranešti apie šio asmens ar šios grupės veiksmus ir pasiektus rezultatus.</p> <p>Kai nacionaliniai teisės aktai nesuteikia pakankamos apsaugos, įmonės turėtų gerbti, bet viršyti nacionalinius įstatymus ir pasistengti paskatinti teisės aktų pakeitimus, kad pramonė galėtų kovoti su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu.</p> <p>Organizacijoje turėtų būti įsteigta pozicija ar grupė, skirta integruoti šias procedūras ir stebėti atliekamus veiksmus. Tai turėtų būti skaidriai atspindėta metinėse įmonės ataskaitose ir paskelbta visuomenei.</p> <p>Nurodyti, kad įmonė visapusiškai bendradarbiaus su teisėsaugos tyrimais, jei bus pranešta apie neteisėtą turinį arba jis bus aptiktas, ir pateikti išsamią informaciją apie atitinkamas nuobaudas, tokias kaip baudos ar aptarnavimo paslaugų nutraukimas.</p> <p>Apibrėžti sutarties sąlygas ir (arba) priimtina naudojimo politiką, kad aiškiai nurodytumėte įmonės poziciją dėl netinkamo jos paslaugų naudojimo vaikų seksualinio išnaudojimo medžiagos (CSAM) saugojimui ar dalijimuisi juo ir piktnaudžiavimo pasekmėmis.</p> <p>Sukurti pranešimo apie draudžiamą turinį ir jo pašalinimo (angl. notice and takedown) procesus, leidžiančius vartotojams informuoti apie vaikų seksualinio išnaudojimo medžiagą (CSAM) internete ar netinkamus asmenis bei konkrečią paskyrą / vietą, kurioje CSAM buvo aptiktas.</p>

	<p>Nustatykite tolesnius pranešimų (angl. notice and takedown) procesus, susitarkite dėl įrodymų surinkimo procedūrų ir nedelsdami pašalinkite arba blokuokite prieigą prie vaikų seksualinio išnaudojimo medžiagos.</p> <p>Užtikrinti, kad prireikus paslaugų teikėjai, prieš sunaikindami neteisėtą turinį, paprašytų ekspertų (pvz., Nacionalinių vaikų saugumo internete įstaigų) nuomonės.</p> <p>Užtikrinti, kad atitinkamos trečiosios šalys – partnerės - taip pat turėtų gerus informavimo ir panaikinimo procesus.</p>
	<p>Būti pasirengus susidurti su vaikų seksualinio išnaudojimo medžiaga (CSAM) ir pranešti apie tokius atvejus atitinkamoms institucijoms. Jei santykiai su teisėsauga ir nacionaline interneto karštąja linija dar nėra užmegzti, bendradarbiaukite su jais ir procesus plėtokite kartu.</p>
	<p>Dirbti su vidinėmis funkcijomis, tokiomis kaip klientų aptarnavimas, sukčiavimo prevencija ir saugumas, kad įmonė tiesiogiai galėtų pranešti apie įtariamą neteisėtą turinį teisėsaugai ir karštosioms linijoms. Geriausia, kad tai būtų daroma taip, jog įmonės darbuotojai nesusidurtų su žalingu turiniu, o vaikai dėl to nenukentėtų dar kartą. Sukurkite politiką ar programą, skirtą skatinti darbuotojų atsparumą, saugą ir gerovę, jei jiems tektų susidurti su žalingu turiniu.</p>
<p>Standartinių procesų kūrimas kovai su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu (tęsinys)</p>	<p>Įtraukti duomenų saugojimo politiką, kuri padėtų teisėsaugai, jai atliekant nusikalstamos veikos tyrimą ir renkant įrodymus. Dokumentuoti įmonės praktiką susidūrus su vaikų seksualinio išnaudojimo medžiaga (CSAM), pradedant stebėjimu ir baigiant galutiniu turinio perdavimu bei sunaikinimu. Į dokumentaciją įtraukite visų darbuotojų, atsakingų už medžiagos tvarkymą, sąrašą.</p> <p>Skatinti vaikų seksualinio išnaudojimo medžiagos (CSAM) pranešimų teikimo mechanizmus ir įsitikinti, kad klientai žino, kaip pranešti, jei aptinka tokį turinį. Jei yra nacionalinė interneto karštoji linija, skelbkite interneto karštosios linijos nuorodą savo įmonės interneto svetainėje ir kitur, priklausomai nuo atitinkamų paslaugų, kurias reklamuoja bendrovė.</p> <p>Prižiūrėti visas siūlomas paslaugas / duomenų rinkinius, kad būtų išvengta žinomo vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimo šių paslaugų ar platformų pagalba.</p> <p>Reguliariai aktyviai peržiūrėti visą įmonės serveriuose saugomą turinį, įskaitant komercinį (firminį ar sutartinį iš trečiųjų šalių turinio teikėjų). Apsvarstyti galimybę naudoti įrankius, pvz., žinomų vaikų seksualinio išnaudojimo vaizdų maišų reikšmes (angl. hashes), vaizdo atpažinimo programinę įrangą ar URL blokavimą.</p>
<p>Saugesnės ir amžių atitinkančios</p>	<p>Pramonė gali padėti sukurti saugesnę, malonesnę skaitmeninę aplinką bet kokio amžiaus vaikams ir jaunimui atlikdama šiuos veiksmus:</p>

<p>interneto aplinkos kūrimas</p>	<p>Įmonės technologijoms ir paslaugoms taikyti saugos ir privatumo principus ir pirmenybę teikti sprendimams, kurie sumažina su vaikais susijusių duomenų kiekį iki minimalaus.</p> <p>Siūlomoms paslaugoms pritaikyti amžių atitinkantį dizainą.</p> <p>Pateikti vaikams tinkamą kiekį informacijos apie svetainės taisykles suprantamai ir pagal atitinkamą amžių.</p> <p>Be amžiui atitinkamų ir prieinamų sąlygų, pramonė taip pat turėtų aiškiai perduoti informaciją, pvz., taisykles ir pagrindinę politiką. Tai turėtų pabrėžti priimtina ir nepriimtina elgesį, bet kokių taisyklių pažeidimo pasekmes, paslaugos specifiką ir tai, su kuo vartotojas sutinka. Tokia informacija visų pirma turėtų būti skirta jauniems vartotojams, jų tėvams ir globėjams.</p> <p>Naudoti paslaugų teikimo sąlygas, kad būtų atkreipiamas vartotojų dėmesys į įmonės interneto paslaugų turinį, kuris gali būti netinkamas tam tikroms amžiaus grupėms. Sąlygose taip pat turėtų būti numatyti aiškūs pranešimo apie tokių taisyklių pažeidimus ir jų sprendimo būdai.</p>
<p>Saugesnės ir amžių atitinkančios interneto aplinkos kūrimas (tęsinys)</p>	<p>Apsvarstyti galimybę parengti tokius mechanizmus kaip tėvų kontrolės programinė įranga ir kiti įrankiai, leidžiantys tėvams ir globėjams valdyti savo vaikų prieigą prie interneto išteklių, kartu pateikiant tėvams gaires, kaip juos tinkamai naudoti, kad nebūtų pažeistos vaikų teisės. Tai apima blokavimo / leidimo sąrašus, turinio filtravimo priemones, naudojimo stebėjimą, kontaktų valdymą ir laiko / programos apribojimus.</p> <p>Pasiūlyti lengvai naudojamas tėvų kontrolės parinktį, leidžiančią tėvams ir globėjams apriboti tam tikras paslaugas ir turinį, kurį vaikai gali pasiekti naudodamiesi elektroniniais prietaisais. Šie apribojimai gali apimti tinklo, įrenginių bei programų valdiklius. Atsižvelgiant į tai, kad tai daro didžiulę įtaką vaiko gebėjimui tobulinti savo skaitmeninius įgūdžius ir kenkia jų galimybėms internete, šios kontrolės priemonės turėtų būti sukurtos mažamečiams vaikams, atsižvelgiant į jų raidos aplinkybes su atitinkamomis rekomendacijomis tėvams.</p> <p>Jei įmanoma, skatinti nacionalines paramos paslaugas, kurias tėvai ir globėjai gali naudoti pranešdami apie pažeidimus ir kreiptis pagalbos piktnaudžiavimo ar išnaudojimo atveju.</p> <p>Vengti žalingo ar netinkamo reklaminio turinio internete ir nustatyti turinio teikimo įsipareigojimus paslaugų teikėjams, kai turinys skirtas suaugusiesiems ir gali būti žalingas vaikams ir jaunimui. Žalinga reklama taip pat gali apimti maisto ir gėrimų, kuriuose yra daug riebalų, cukraus ar druskos, reklamą.</p> <p>Verslo praktiką suderinti su reglamentais ir patarimais, susijusiais su rinkodara ir reklama, skirta vaikams ir jaunimui. Stebėti, kur, kada ir kaip</p>

	<p>vaikai ir jaunimas gali susidurti su potencialiai žalingais reklaminiais pranešimais, skirtais kitam rinkos segmentui.</p> <p>Užtikrinti, kad duomenų rinkimo politika atitiktų įstatymus, susijusius su vaikų ir jaunimo privatumu, įskaitant ir tai, ar komercinė įmonė turi gauti tėvų sutikimą asmeninės vaiko informacijos rinkimui.</p> <p>Pritaikyti ir įgyvendinti išplėstinius numatytuosius privatumo nustatymus, skirtus rinkti, tvarkyti, saugoti, perduoti ir skelbti asmens duomenis, įskaitant informaciją apie vietą ir naršymo tendencijas, surinktus iš jaunesnių nei 18 metų žmonių. Numatytieji privatumo nustatymai ir informacija apie privatumo svarbą turėtų atitikti vartotojų amžių ir paslaugos pobūdį.</p> <p>Taikyti technines priemones, pvz., tinkamas tėvų kontrolės priemones, saugumą užtikrinantį dizainą, amžių atitinkančią prieigą, slaptažodžiu apsaugotą turinį, blokavimo / leidimo sąrašus, pirkimo / laiko valdymą, atsisakymo funkcijas, filtravimą ir moderavimą, kad būtų išvengta nepilnamečių prieigos prie netinkamo turinio ar paslaugų.</p> <p>Įdiegti technologiją, pagal kurią galima nustatyti vartotojų amžių ir pateikti jiems pritaikytą programos versiją.</p> <p>Turėdamos omenyje tam tikro amžiaus grupėms skirtą turinį ar paslaugas, pramonės suinteresuotosios šalys turėtų imtis veiksmų vartotojų amžiaus patikrinimui. Jei įmanoma, naudoti amžiaus patikrinimą, taip apribojant prieigą prie turinio ar medžiagos, kuri pagal įstatymus ar politiką yra skirta tik vyresniems nei tam tikro amžiaus asmenims. Įmonės taip pat turėtų atkreipti dėmesį į galimybę piktnaudžiauti tokiais technologijomis, siekiant apriboti vaikų ir jaunimo teisę į žodžio laisvę ir prieigą prie informacijos arba pakenkti jų privatumui.</p>
<p>Saugesnės ir amžių atitinkančios aplinkos internete kūrimas (tęsinys)</p>	<p>Užtikrinti, kad ne visoms amžiaus grupėms skirtas turinys (ir paslaugos):</p> <ul style="list-style-type: none"> • klasifikuojamas pagal nacionalinius standartus ir kultūros normas; • atitinka esamų lygiaverčių terpių standartus; • turi aiškius prieigos valdymo pasirinkimus; • turi tinkamą amžiaus patikrinimo procesą, jei tai yra įmanoma, su aiškiais terminais, susijusiais su bet kokių asmens tapatybę identifikuojančių duomenų, gautų tikrinimo proceso metu, ištrynimu. <p>Pavyzdžiui, kalbant apie socialinių tinklų standartus, visos socialinių tinklų reguliavimo institucijos pateikia su amžiumi susijusio turinio reikalavimus, o interneto paslaugų teikėjai privalo pritaikyti saugyklas ir savo siūlomam turiniui taikyti numatytas gaires. Pavyzdžiai: CSA Prancūzijoje ir AGCOM</p>

	<p>Italijoje.</p>
	<p>Pateikti aiškias pranešimų pateikimo priemones ir sukurti tolesnį procesą pranešimams apie netinkamą turinį nagrinėjimui, ir pateikti kontaktus kur kreiptis, kai pranešimas netinkamai išnagrinėjamas bei teikti išsamias pranešimų nagrinėjimo proceso ataskaitas vartotojams.</p>
	<p>Užtikrinti, kad vaikams ir jaunimui skirtos interaktyvios erdvės būtų iš anksto moderuojamos taip, kad tai atitiktų vaikų teisę į privatumą ir besikeičiančius jų gebėjimus. Aktyvus moderavimas gali sukurti atmosferą be patyčių ir priekabiavimo. Nepriimtinas elgesys yra:</p> <ul style="list-style-type: none"> • nemalonių ar grėsmingų komentarų skelbimas kieno nors paskyroje; • suklastotų paskyrų ar neapykantos svetainių sukūrimas aukai pažeminti; • žalingų pranešimų su priedais siuntimas; • įsilaužimas į kieno nors paskyrą, siekiant siųsti įžeidžiančius pranešimus kitiems.
	<p>Imtis atsargumo priemonių dėl darbuotojų, kurie dirba su vaikais ir jaunimu, nes gali tekti patikrinti jų teistumą policijos įstaigose.</p>
	<p>Dėl įtariamo viliojimo kreiptis į interneto ar interaktyvių vykdomojo valdymo grupę, atsakingą už pranešimą atitinkamoms institucijoms:</p> <ul style="list-style-type: none"> • kur įmanoma, pranešti apie viliojimą vykdomojo valdymo grupei ir paskirtam vaikų apsaugos politikos vadovui; • leisti vartotojams tiesiogiai pranešti valdžios institucijoms apie įtariamus viliojimo atvejus; • sudaryti galimybę tiesiogiai susisiekti el. pašto adresais.

	<p>Visada teikti pirmenybę vaiko saugumui ir gerovei. Niekada neperžengti profesinių ribų ir užtikrinti, kad ryšys su vaikais yra būtinas suteikiant paslaugą, vykdant programą, renginį, veiklą ar projektą. Niekada neprisiimkite visos atsakomybės už vaiką. Jei vaikui reikalinga priežiūra, įspėkite tėvą, globėją ar auklę. Visada išklauskite vaikus ir juos gerbkite. Jei kas nors prie vaikų elgiasi netinkamai, praneškite apie tai vietiniam vaikų apsaugos atstovui.</p>
<p>Saugesnės ir amžių atitinkančios aplinkos internete kūrimas (tęsinys)</p>	<p>Sukurti aiškias taisykles, kurios primintų esminius paslaugų teikimo sąlygose nurodytus aspektus. Taisyklės turėtų būtų lengvai suprantamos vartotojui:</p> <ul style="list-style-type: none"> • paslaugos pobūdis ir ko tikimasi iš jos vartotojų; • koks turinys ar elgesys yra priimtinas ir kas yra neteisėta; • pažeidimui proporcingi padariniai, pavyzdžiui, pranešimas teisėsaugai arba vartotojo paskyros sustabdymas. <p>Padėti klientams lengvai informuoti klientų aptarnavimo skyrių apie įtarimus dėl netinkamo naudojimo, taikant standartinius ir prieinamus procesus, kad būtų galima išspręsti įvairias problemas, pvz., nepageidaujamų pranešimų (pvz., šlamšto žinučių) gavimą.</p> <p>Būti skaidriems ir pateikti klientams aiškią informaciją, pavyzdžiui, apie siūlomų paslaugų pobūdį:</p> <ul style="list-style-type: none"> • turinį / paslaugas ir kainas; • minimalų reikalaujamą amžių; • tėvų kontrolės priemonių prieinamumą, įskaitant tai, ką kontrolė apima (pvz., tinklą) ar neapima (pvz., „Wi-Fi“), ir mokymus, kaip jomis naudotis; • renkama informaciją apie vartotoją ir jos naudojimą. <p>Skatinti nacionalines paramos paslaugas, kurios leistų vaikams ir jaunimui prašyti pagalbos ir kreiptis dėl patiriamos prievartos ar išnaudojimo (žr., pavyzdžiui, „Child Helpline International“).</p>
<p>Vaikų, tėvų ir pedagogų švietimas apie vaikų saugumą ir jų atsakingą naudojimąsi IRT</p>	<p>Pramonė gali ne tik teikti technines priemones, bet ir prisidėti prie švietimo bei priemonių taikymo, atlikdama šiuos veiksmus:</p> <p>Aiškiai apibūdinant turinį ir atitinkamą tėvų kontrolės įrankius ar šeimos saugumo nustatymus. Supaprastinti vartojamą kalbą bei terminologiją, padaryti ją aiškia ir tinkama visiems vartotojams, įskaitant vaikus, tėvus ir globėjus, ypač atsižvelgiant į sąlygas bei išlaidas, susijusias su turiniu ar paslaugomis, privatumo politika, saugos informacija ir pranešimo mechanizmais.</p>

	<p>Mokyti klientus atpažinti su internetu susijusias problemas, įskaitant šlamštą (angl. „spam“), duomenų vagystes ir netinkamus kontaktus, įskaitant patyčias ar viliojimą, ir apibūdinti, kokių veiksmų klientai gali imtis ir kaip jie gali pranešti apie netinkamą turinį.</p>
	<p>Sukurti mechanizmus ir mokyti tėvus įsitraukti į savo vaikų, ypač jaunesnių, veiklą internete, pavyzdžiui, suteikiant tėvams galimybę peržiūrėti vaikų privatumo nustatymus.</p>
	<p>Bendradarbiauti su vyriausybe ir pedagogais, siekiant sustiprinti tėvų pagalbą jų vaikams, skatinant tėvus kalbėti su vaikais apie atsakingumą internete ir tinkamą jo naudojimą.</p>
<p>Vaikų, tėvų ir pedagogų švietimas apie vaikų saugumą ir jų atsakingą naudojimąsi IRT (tęsinys)</p>	<p>Pagal vietines aplinkybes, pateikti mokyklai ir namams skirtą mokomąją medžiagą, padėsiančią vaikams ir jaunimui geriau naudotis IRT ir ugdyti kritinį mąstymą, kad jie galėtų saugiai ir atsakingai naudotis interneto paslaugomis.</p>
	<p>Padėti klientams platinant šeimos saugumui internete skirtas gaires, kurios skatina tėvus ir globėjus:</p> <ul style="list-style-type: none"> • susipažinti su vaikų ir jaunimo naudojamais produktais ir paslaugomis; • užtikrinti, kad vaikų ir jaunimo naudojami elektroniniai prietaisai prisidėtų prie sveiko ir subalansuoto gyvenimo būdo; • kreipti ypatingą dėmesį į vaikų ir jaunimo elgesį, kad būtų galima nustatyti elgesio pokyčius, kurie galėtų reikšti internete patiriamas patyčias ar priekabiavimą.
	<p>Suteikti tėvams reikiamos informacijos, kad jie suprastų, kaip jų vaikai ir jaunimas naudojami IRT paslaugomis, kad galėtų spręsti su žalingu turiniu ir elgesiu susijusius klausimus ir būtų pasirengę padėti vaikams ir jaunimui atsakingai naudotis internetu. Tai galima skatinti bendraujant su mokyklomis ir teikiant tėvams vaikų saugumo internete programas ir mokomąją medžiagą.</p>
<p>Technologijų pažanga vaikų apsaugai ir ugdymui</p>	<p>Privatumą saugantis dirbtinis intelektas, suprantantis tekstus, vaizdus, pokalbius ir kontekstą, gali aptikti įvairias grėsmes internete bei naudoti šią informaciją, kad išmokytų ir paskatintų vaikus apie jas pranešti. Šios technologijos naudojimas išmaniuosiuose įrenginiuose gali apsaugoti jaunų žmonių duomenis ir privatumą.</p>
	<p>Viešųjų paslaugų sektorius ir nacionalinė žiniasklaida savo programomis (internetu ir ne tik) gali svariai prisidėti prie tėvų ir vaikų švietimo ir supažindinti juos su rizika internete ir interneto galimybėmis.</p>
<p>Skaitmeninių technologijų</p>	<p>Pramonė gali skatinti vaikus ir jaunimą veikti ir suteikti jiems daugiau galimybių palaikydama jų teisę į dalyvavimą, atlikdama šiuos veiksmus:</p>

<p>naudojimas skatinant pilietinį įsitraukimą</p>	<p>Pateikti informaciją apie paslaugą, pabrėžiant vaikų gaunamą naudą, jei paslauga naudojama tikslingai ir atsakingai, pavyzdžiui, kūrybiniais tikslams.</p>
<p>Skaitmeninių technologijų naudojimas skatinant pilietinį įsitraukimą (tęsinys.)</p>	<p>Nustatyti rašytines procedūras, saugančias vartotojų, įskaitant vaikų ir jaunimo žodžio laisvę, o taip pat pateikti tai apibrėžiančius dokumentus.</p> <p>Vengti blokuoti teisėtą ir vystymuisi tinkamą turinį. Siekiant užtikrinti, kad filtravimo įrankiai nebūtų panaudoti klaidingai – apribojant vaikų ir jaunimo prieigą prie informacijos, reikia patikrinti užblokuoto turinio skaidrumą ir nustatyti procesą, kuriuo vartotojai gali pranešti apie netyčinį užblokavimą. Šis procesas turėtų būti prieinamas visiems vartotojams, įskaitant žiniatinklio valdytojus. Bet koks pranešimų procesas turėtų sudaryti aiškias, įpareigojančias ir teisine atsakomybe pagrįstas paslaugų teikimo sąlygas.</p> <p>Sukurti interneto platformas, skatinančias vaikų ir jaunimo išraiškos teisę; palengvinti jų dalyvavimą viešajame gyvenime; skatinti jų bendradarbiavimą, verslumą ir pilietinį dalyvavimą.</p> <p>Kurti mokomąjį turinį vaikams ir jaunimui, taip skatinant mokymąsi, kūrybišką mąstymą ir problemų sprendimą.</p> <p>Skatinti skaitmeninį raštingumą, gebėjimų ir IRT įgūdžių stiprinimą, kad vaikai ir jaunimas, ypač kaimo ir nepakankamai aprūpintose vietovėse, galėtų naudotis IRT ištekliais ir visapusiškai saugiai dalyvauti skaitmeniniame pasaulyje.</p> <p>Bendradarbiauti su vietos pilietine visuomene ir vyriausybe dėl nacionalinių ir vietinių prioritetų, siekiant išplėsti visuotinę ir nešališką prieigą prie IRT, įvairių platformų bei įrenginių, o taip pat prie pagrindinės infrastruktūros.</p> <p>Informuoti klientus, tame tarpe tėvus, globėjus, vaikus ir jaunimą, apie siūlomas paslaugas:</p> <ul style="list-style-type: none"> • turinio tipą ir atitinkamą tėvų kontrolę; • kaip pranešti apie piktnaudžiavimo, netinkamo naudojimo ir netinkamo ar neteisėto turinio atvejus; • tolimesnius veiksmus po pranešimų pateikimo; • amžiaus cenzą turinčias paslaugas; • saugų ir atsakingą interaktyvių paslaugų naudojimą. <p>Susipažinti su platesnėmis problemomis, susijusiomis su saugiu ir atsakingu skaitmeniniu pilietiškumu, pvz., reputacija internete ir skaitmeniniai pėdsakai, žalingas turinys ir viliojimas. Apsvarstykite galimybę bendradarbiauti su vietos ekspertais, pvz., vaikų nevyriausybinėmis organizacijomis, labdaros organizacijomis ir tėvų grupėmis, taip skleidžiant įmonės politiką ir pasiekiant numatytą auditoriją.</p>

	<p>Jei verslas jau įtraukia vaikus ar mokyklas, pavyzdžiui, per įmonių socialinės atsakomybės programas, galima pabandyti išplėsti šią veiklą įtraukiant vaikus ir jaunimo bei pedagogų švietimą ir bendradarbiavimą dėl vaikų apsaugos internete (COP) pranešimų.</p>
Investavimas į mokslinius tyrimus	<p>Investuoti į įrodymais pagrįstus tyrimus ir išsamią skaitmeninių technologijų analizę, technologijų poveikį vaikams, vaikų apsaugą ir vaiko teisių aspektus, susijusius su skaitmenine aplinka ir taip integruoti interneto apsaugos sistemas į vaikų ir jaunimo naudojamą paslaugas ir pamatyti, kokios intervencijos yra efektyviausios užtikrinant gerą vaikų patirtį internete.</p>

IRT įmonių tipai

Nors šios ITU gairės yra skirtos visai IRT pramonei, svarbu nepamiršti, kad IRT įmonių siūlomos paslaugos, jų veiklos būdas, taikomos reguliavimo sistemos ir jų pasiūlymų apimtys yra labai skirtingi. Bet kuri technologijų įmonė, kurios produktai ir paslaugos yra tiesiogiai ar netiesiogiai skirtos vaikams, gali pasinaudoti anksčiau išdėstytais bendraisiais principais, atsižvelgdama į savo veiklos sritį. Pagrindinė idėja yra remti IRT pramonę ir padėti jai imtis tinkamų priemonių, siekiant geriau apsaugoti vaikus internete nuo jiems kylančios rizikos, suteikiant jiems galimybę saugiai naršyti internete. Toliau pateikiama tipologija padės aiškiau suprasti kai kurias tikslines auditorijas ir kaip jos atitinka kitame skyriuje pateikiamą kontrolinį sąrašą. Reikėtų pažymėti, kad tai tik keletas konkrečių kategorijų pavyzdžių ir sąrašas nėra baigtinis:

- (a) Interneto paslaugų teikėjai, įskaitant teikiančius laidinio plačiajuosčio interneto ryšio paslaugas arba mobiliojo ryšio tinklo operatorių duomenų paslaugas: nors tai paprastai atspindi ilgalaikes abonentams teikiamas paslaugas, prie to taip pat galima priskirti ir įmones, teikiančias nemokamo ar mokamo viešojo mobilaus interneto („Wi-Fi“) ryšio paslaugas.
- (b) Socialinių tinklų / pranešimų platformos ir internetinių žaidimų platformos.
- (c) Techninės ir programinės įrangos gamintojai, pvz., delninių prietaisų, įskaitant mobiliuosius telefonus, žaidimų konsoles, balso pagalba paremtus namų prietaisus, daiktų internetą ir išmaniuosius prie interneto prijungiamus žaislus vaikams.
- (d) Skaitmeninės žiniasklaidos įmonės (kuriančios turinį, suteikiančios prieigą prie turinio arba jį talpinančios).
- (e) Įmonės, teikiančios tiesioginės transliacijos paslaugas.
- (f) Įmonės, siūlančios skaitmeninių rinkmenų saugojimo paslaugas, debesijos pagrindu veikiančių paslaugų teikėjai.

5. Konkrečioms funkcijoms taikomi veiksmai

Šis skyrius papildoma ankstesnį pramonės kontrolinį sąrašą, pateikdamas rekomendacijas įmonėms, kurių atliekamoms funkcijoms gali būti taikomi konkretūs veiksmai dėl vaikų teisių apsaugos internete. Šie konkretūs veiksmai yra rekomendacijos, kaip būtų galima papildyti 1 lentelėje pateiktus bendruosius principus ir metodus, o kadangi jie taikomi skirtingų paslaugų teikėjams, juos reikėtų taikyti kartu su 1 lentelėje nurodytais veiksmais.

Čia minimus veiksmus gali taikyti visos įmonės, o ta pati įmonė gali taikyti daugiau nei vieną veiksmą.

Šie veiksmai yra suskirstyti į tas pačias pagrindines sritis, kaip ir 1 lentelėje nurodytos bendrosios gairės. Kiekvienas veiksmas buvo sukurtas bendradarbiaujant su pagrindiniais bendraautoriais, todėl lentelėse yra neįžymių skirtumų.

5.1 Funkcija A: interneto prieigos, duomenų saugojimo ir talpinimo paslaugos

Interneto prieiga yra labai svarbi įgyvendinant vaikų teises, o interneto ryšys vaikams gali atverti visą pasaulį. Ryšio, duomenų saugojimo ir talpinimo paslaugų teikėjai turi geras galimybes į savo siūlomas paslaugas įtraukti vaikų ir jaunimų saugumą bei privatumą. Ši

paslaugos funkcija, be kitų, skirta mobiliojo ryšio operatoriams, interneto paslaugų, duomenų saugojimo sistemų ir talpinimo paslaugų teikėjams.

Mobiliojo ryšio operatoriai suteikia interneto prieigą ir siūlo daugybę duomenų paslaugų. Daugelis operatorių jau pasirašė vaikų saugumo internete praktikos kodeksus ir siūlo įvairius įrankius bei informacijos išteklius savo įsipareigojimams įgyvendinti.

Dauguma interneto paslaugų teikėjų veikia ir kaip kanalas, teikiantis prieigą prie interneto ir iš jo, ir duomenų saugykla teikianti talpinimo ir saugojimo paslaugas. Todėl visų pirmiausia jiems tenka atsakomybė už vaikų saugumą internete.

Interneto prieiga viešosiose erdvėse

Vis dažniau savivaldybės, mažmenininkai, transporto įmonės, viešbučių tinklai ir kitos įmonės bei organizacijos naudoja mobilaus interneto prieigą „Wi-Fi“. Tokia prieiga paprastai yra nemokama arba teikiama už minimalią kainą, be to, jei ši paslauga teikiama viešose vietose, kartais tenka atlikti minimalius prisijungimo formalumus, o, galiausiai, įmonė gali teikti šią paslaugą siekdama pritraukti klientus į savo patalpas arba įtikinti daugiau žmonių naudotis jos paslaugomis.

„Wi-Fi“ reklama yra veiksmingas būdas užtikrinti interneto prieinamumą įvairiose vietose. Tačiau reikia būti atsargiems, kai tokia prieiga suteikiama viešosiose erdvėse, kuriose dažnai lankosi vaikai. Vartotojai turi nepamiršti, kad „Wi-Fi“ gali būti pasiekiamas ir pro šalį einantiems žmonėms, todėl gali būti pažeisti vartotojų duomenys. „Wi-Fi“ paslaugų teikėjas ne visada galės prižiūrėti jo teikiamą interneto ryšį, todėl vartotojai turi imtis atsargumo priemonių, kad neskelbtų netinkamos informacijos per viešai prieinamą „Wi-Fi“ ryšį.

Viešosiose erdvėse „Wi-Fi“ ryšio paslaugų teikėjai gali apsvarstyti papildomas priemones, skirtas apsaugoti vaikus ir jaunimą, pvz.:

- Aktyviai blokuojant prieigą prie žiniatinklio adresų, kuriuose yra plačiąjai auditorijai netinkamo turinio, o taip pat blokuoti prieigą prie vaikų seksualinio išnaudojimo medžiagos (CSAM).
- Į bendras naudojimo sąlygas ir nuostatas įtraukti punktus, draudžiančius naudoti „Wi-Fi“ paslaugas norint pasiekti ar rodyti bet kokią medžiagą, kuri gali būti netinkama vaikams. Sąlygose taip pat turėtų būti aiškūs mechanizmai, susiję su tokių taisyklių pažeidimų pasekmėmis.
- Imtis visų priemonių apsaugoti nuo neteisėtos prieigos, dėl kurios gali būti manipuluojama ar prarandami asmens duomenys.
- Įdiegti filtrus į „Wi-Fi“ ryšio sistemą, kad būtų sustiprintas netinkamos medžiagos draudimas.
- Teikti procedūras ir programinę įrangą, siūlančią papildomą tėvų kontrolę, susijusią su vaikų ir jaunimo prieiga prie interneto turinio.

Geroji praktika: Pavyzdžiui, daugumos Europos Sąjungos valstybių narių telekomunikacijų nuostatose parašyta, kad prieigą prie tinklo reikia nustatyti naudojant tam tikras SIM korteles ar kitas identifikavimo priemones.

2 lentelėje pateikiamos veiksmų gairės – ryšio, duomenų saugojimo ir talpinimo paslaugų teikėjams, kurių jie gali imtis, kad sustiprintų vaikų apsaugą internete ir vaikų dalyvavimą.

2 lentelė: Funkcijos A veiksmai, skirti užtikrinti vaikų saugumą internete

<p>Vaiko teisių integravimas į tinkamą įmonės politiką ir valdymo procesus</p>	<p>Ryšio, duomenų saugojimo ir informacijos prieglobos paslaugų teikėjai gali nustatyti, užkirsti kelią ir sušvelninti neigiamą IRT poveikį vaikų ir jaunimo teisėms bei paieškoti galimybių ginti vaikų ir jaunimo teises.</p>
<p>Standartinių procesų kūrimas kovai su seksualinio vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu</p>	<p><i>Žr. 1 lentelėje pateiktas bendrąsias gaires.</i></p> <p>Bendradarbiaudami su vyriausybe, teisėsaugos institucijomis, pilietine visuomene ir interneto karštųjų linijų organizacijomis, ryšio, duomenų saugojimo ir informacijos prieglobos paslaugų teikėjai gali atlikti pagrindinį vaidmenį kovojant su vaikų seksualinio išnaudojimo medžiaga (CSAM), imdamiesi šių veiksmų:</p> <p>Bendradarbiauti su vyriausybe, teisėsaugos institucijomis, pilietine visuomene ir interneto karštųjų linijų organizacijomis kovojant su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu ir nustatant apie tokį turinį gautų pranešimų procesą. Jei santykiai su teisėsauga ir nacionaline interneto karštąja linija dar nėra užmegzti, bendradarbiaukite su jais ir procesus plėtokite kartu.</p> <p>Ryšio, duomenų saugojimo ar informacijos prieglobos paslaugų teikėjai taip pat gali organizuoti IKT mokymus teisėsaugai.</p> <p>Jei įmonė veikia mažiau teisinio reguliavimo ir teisėsaugos kontrolės klausimais išsivysčiusioje rinkoje, ji norinčius pranešti gali nukreipti į Tarptautinę interneto karštųjų linijų asociaciją (INHOPE), kur pranešimus galima pateikti bet kuriai tarptautinei interneto karštajai linijai.</p> <p>Apsvarstyti galimybę naudoti tarptautiniu mastu pripažintus URL adresų ar svetainių blokavimo sąrašus, kuriuos sukūrė atitinkamos valdžios institucijos (pvz., nacionalinės teisėsaugos ar interneto karštosios linijos, „Cybertip Canada“, Interpolas, IWF), kad vartotojams būtų sunkiau pasiekti jau žinomą vaikų seksualinio išnaudojimo medžiagą (CSAM).</p> <p>Parengti pranešimo apie draudžiamą turinį ir jo pašalinimo (angl. notice and takedown) procesus ir susieti pranešimus apie piktnaudžiavimą su šiais procesais viešųjų paslaugų sutartyje.</p> <p>Kaip pavyzdį galima naudoti UNICEF ir GSMA vadovą dėl pranešimo ir pašalinimo politikos bei praktikos.</p> <p>Sukurti nesudėtingą pranešimų (angl. notice and takedown) teikimo mechanizmą, pavyzdžiui, teikiant nurodymus dėl neteisėto turinio ir elgesio, apie kurį reikia pranešti, ir paaiškinant, kokios medžiagos negalima pridėti prie pranešimų, kad būtų išvengta tolesnio jos platinimo internete.</p>

<p>Standartinių procesų kūrimas kovai su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu (tęsinys)</p>	<p>Bendradarbiauti su teisėsauga kriminalinių tyrimų atveju padedant rinkti įrodymus.</p> <p>Paslaugų teikimo sąlygose paminėti, kad paslaugų naudojimas vaikų seksualinio išnaudojimo medžiagos (CSAM) saugojimui, dalijimuisi ar platinimui yra griežtai draudžiamas.</p> <p>Įsitikinti, kad sąlygos aiškiai nurodo, jog vaikų seksualinio išnaudojimo medžiaga (CSAM) nebus toleruojama.</p> <p>Įsitikinti, kad paslaugų teikimo sąlygose nurodoma, jog įmonė visapusiškai bendradarbiaus su teisėsauga, jei bus aptikta vaikų seksualinio išnaudojimo medžiaga (CSAM).</p>
	<p>Šiuo metu nacionaliniu lygiu apie vaikų seksualinio išnaudojimo medžiagą (CSAM) galima pranešti interneto karštosiomis linijomis ir internetu. Išsamų visų esamų interneto karštųjų linijų ir portalų sąrašą galite rasti INHOPE puslapyje.</p> <p>Interneto karštosios linijos: jei nacionalinės interneto karštosios linijos nėra, apsvarstykite jos įsteigimą (žr. „GSMA INHOPE“ interneto karštosios linijos vadovą, kuriame rasite daugybę galimybių, įskaitant bendradarbiavimą su INHOPE ir INHOPE fondu). Galima rasti interaktyvią „GSMA INHOPE“ vadovo versiją, kurioje pateikiamos rekomendacijos, kaip sukurti vidinius procesus, skirtus klientų aptarnavimo darbuotojams pateikti pranešimus dėl abejotino turinio teisėsaugai ir INHOPE.</p> <p>Portalai skirti pranešti: IWF pateikia pranešimų portalą, kuris leidžia interneto vartotojams šalyse be interneto karštųjų linijų pranešti apie įtariamą vaikų seksualinio išnaudojimo medžiagą (CSAM) tiesiogiai IWF.</p>
	<p>Ryšio, duomenų saugojimo ir informacijos prieglobos paslaugų teikėjai, kurių paslaugos apima tam tikrą turinio talpinimą (daugelis to netaiko), turėtų būti paruošę pranešimo apie draudžiamą turinį ir jo pašalinimo (angl. notice and takedown) procesus.</p>
<p>Saugesnės ir amžių atitinkančios interneto aplinkos kūrimas</p>	<p>Ryšio, duomenų saugojimo ir informacijos prieglobos paslaugų teikėjai gali padėti sukurti saugesnę, malonesnę skaitmeninę aplinką bet kokio amžiaus vaikams ir jaunimui atlikdami šiuos veiksmus:</p> <p>Duomenų saugojimo / informacijos prieglobos paslaugų teikėjai turėtų apsvarstyti galimybę sukurti pranešimų teikimo funkciją visose interneto svetainėse ir teikiant paslaugas bei nustatyti ir dokumentuoti aiškius procesus, kaip greitai valdyti pranešimus apie piktnaudžiavimą ar kitus sąlygų pažeidimus.</p>

	<p>Ryšio teikėjai turėtų pasiūlyti savo prekės ženklo techninius valdiklius arba nurodyti, ar yra specializuotų tiekėjų sukurtų įrankių, tinkamų jų siūlomoms paslaugoms ir kuriuos galutiniai vartotojai gali lengvai pritaikyti, o taip pat teikėjai turėtų pasiūlyti galimybę blokuoti ar filtruoti prieigą prie interneto. Be to, turėtų būti taikomi tinkami amžiaus patikrinimo mechanizmai, jei įmonė siūlo turinį ar paslaugas (įskaitant savo prekės ženklo ar trečiųjų šalių paslaugas, kurias reklamuoja įmonė), kurios yra teisėtos arba tinkamos tik suaugusiesiems (pvz., tam tikri žaidimai, loterijos).</p>
<p>Vaikų, tėvų ir pedagogų švietimas apie vaikų saugumą ir jų atsakingą naudojimąsi IRT</p>	<p>Ryšio, duomenų saugojimo ir informacijos prieglobos paslaugų teikėjai turėtų priminti vartotojams apie svarbiausias sąlygas, kurios taip pat turėtų būti aiškios ir lengvai suprantamos vaikams, jų tėvams ir globėjams. Teikiant turinio talpinimo paslaugą turi būti aiškiai priminta dėl netinkamo turinio.</p>
	<p>Teikti vaikams ir jaunimui informaciją apie saugesnį naudojimąsi internetu. Apsvarstyti kūrybinius būdus, kaip reklamuoti pagrindinius pranešimus, pavyzdžiui:</p> <p>“ Niekada nesidalykite jokia kontaktine informacija, įskaitant savo fizinę vietą ir telefono numerį, su niekuo, ko nepažįstate asmeniškai.”</p> <p>“ Niekada gyvai nesusitikite su internete sutiktais asmenimis, prieš tai nepasitarę su suaugusiuoju. Visada pasakykite patikimam draugui apie savo buvimo vietą.”</p> <p>“ Neatsakykite į patyčias, nešvankius ar įžeidžiančius pranešimus. Bet išsaugokite įrodymus - neištrinkite pranešimo.”</p> <p>“ Pasakykite patikimam suaugusiajam ar draugui, jei jums kažkas kelia nepatogumą ar nemaloniais emocijas.”</p> <p>“ Niekada neišduokite savo paskyros slaptažodžio ar vartotojo vardo! Turėkite omenyje, kad kiti žmonės internete gali pateikti melagingą informaciją, kad įtikintų jus dalytis jūsų asmenine informacija.”</p>
	<p>Paslaugų teikėjai gali bendradarbiauti su atitinkamomis organizacijomis, dėl vaikų švietimo ir pagalbos jiems saugaus interneto naudojimo ir susijusiais klausimais.</p> <p>Žr. pavyzdinį tarptautinį „Child Helpline International“ ir „GSMA“ praktinį vadovą, skirtą pagalbai vaikams ir mobiliojo ryšio operatoriams: dirbkime kartu gindami vaikų teises.</p>
<p>Skaitmeninių technologijų naudojimas skatinant pilietinį įsitraukimą</p>	<p>Žr. 1 lentelėje pateiktas bendrąsias gaires.</p>

5.2 Funkcija B: prižiūrimas skaitmeninis turinys

Internetu galima rasti įvairių turinį ir veiklas, kurių daugelis yra skirta vaikams ir jaunimui. Turinio priežiūros/redagavimo paslaugas teikiančios įmonės turi puikias galimybes pasirūpinti vaikų ir jaunimo saugumu ir privatumu internete.

Ši funkcija skirta tiek įmonėms, kurios kuria savo turinį, tiek toms, kurios suteikia prieigą prie skaitmeninio turinio. Ji, be kita ko, yra susijusi su naujienų ir daugialypės terpės transliavimo paslaugomis, nacionalinių ir viešųjų paslaugų transliavimu ir žaidimų pramone.

3 lentelėje pateikiamos rekomendacijos turinį kuriančių paslaugų teikėjams dėl politikos ir veiksmų, kurių jie gali imtis, kad sustiprintų vaikų saugumą internete.

3 lentelė: funkcijos B veiksmai, skirti užtikrinti vaikų saugumą internete:

<p>Vaiko teisių integravimas į tinkamą įmonės politiką ir valdymo procesus</p>	<p>Prižiūrimą skaitmeninį turinį teikiančios įmonės gali padėti nustatyti, užkirsti kelią ir sušvelninti neigiamą IRT poveikį vaikų ir jaunimo teisėms, o taip pat nustatyti galimybes paremti vaikų ir jaunimo teisių gynimą. Tam galima atlikti šiuos veiksmus:</p> <p>Parengti taisykles, kurios apsaugo vaikus ir jaunimą, atsižvelgiant į jaunesnių nei 18 metų žmonių, dalyvaujančių programose, filmuose, žaidimuose, naujienose ir kt., fizinę ir emocinę gerovę bei orumą, nepaisant gauto tėvų ar kitų suaugusių asmenų sutikimo.</p>
<p>Standartinių procesų kūrimas kovojant su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu</p>	<p>Bendradarbiaujant su vyriausybe, teisėsaugos institucijomis, pilietine visuomene ir interneto karštosiomis linijomis, įmonės, siūlančios skaitmeninio turinio talpinimo ir saugojimo paslaugas, gali atlikti pagrindinį vaidmenį kovojant su vaikų seksualinio išnaudojimo turiniu, atlikdamos šiuos veiksmus:</p> <p>Vaikų seksualinio išnaudojimo turinio atvejais, pavyzdžiui, naudojant „komentavimo“ ar „peržiūros“ funkcijas, kai vartotojai turi galimybę įkelti turinį, darbuotojai turėtų kreiptis į vykdomąją valdymo grupę, atsakingą už atitinkamų institucijų informaciją apie tokią medžiagą. Be to, jie turėtų:</p> <ul style="list-style-type: none"> • nedelsiant įspėti nacionalines teisėsaugos institucijas; • įspėti savo vadovą ir pranešti apie vaikų seksualinio išnaudojimo medžiagą vaikų apsaugos politikos vadovui; • susisiekti su vidaus tyrimo tarnyba telefonu arba elektroniniu paštu, nurodant išsamią informaciją apie įvykį ir paprašyti pagalbos; • neištrinti, neišsaugoti bendroje erdvėje ir nepersiųsti vaikų seksualinio išnaudojimo medžiagos nesulaukus atitinkamos tarnybos atsakymo.
<p>Standartinių procesų kūrimas kovojant su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu (tęsinys)</p>	<p>Jei toks turinys yra nustatytas, apie jį turėtų būti tiesiogiai pranešama saugumo internete organizacijai, turinčiai visuomenės nariams ir informacinių technologijų specialistams skirtą tiesioginių interneto karštųjų linijos pranešimų sistemą, skirtą informuoti apie konkrečias galimai neteisėto interneto turinio formas.</p> <p>Pavyzdžiui, remdamasis savo vaikų apsaugos ir apsaugos politika, BBC paskelbė redakcines gaires dėl bendravimo su vaikais ir jaunimu internete. Ji sukūrė papildomus reikalavimus ir elgesio taisykles darbui su vaikais ir jaunimu internete, kurie taip pat taikomi subrangovams ir išoriniams paslaugų teikėjams. „Ofcom“ vaikų apsaugos politika Jungtinėje Karalystėje atskiria interneto turinį, mobiliuosius įrenginius ir žaidimų konsoles.</p> <p>Reikia įgyvendinti greitą ir patikimą eskalavimo strategiją, jei patalpinama vaikų seksualinio išnaudojimo medžiaga (CSAM) arba įtariamas neteisėtas elgesys. Tam reikia:</p> <ul style="list-style-type: none"> • pasiūlyti vartotojams paprastą ir lengvai prieinamą būdą, kaip perspėti turinio teikėją apie bet kokių internetinės bendruomenės taisyklių pažeidimus;

	<ul style="list-style-type: none"> pašalinti taisykles pažeidžiantį turinį; <p>Prieš į socialinius tinklus patalpinant prižiūrimą amžiaus cenzą turintį turinį, atkreipti dėmesį į svetainės naudojimo sąlygas. Tinkamai reaguoti į amžiaus cenzą skirtingose socialinių tinklų svetainėse.</p> <p>Kiekvienos interneto erdvės sąlygose taip pat turėtų būti aiškūs mechanizmai pranešti apie taisyklių pažeidimus.</p>
<p>Saugesnės ir amžių atitinkančios aplinkos internete kūrimas</p>	<p>Prižiūrimą skaitmeninį turinį siūlančios įmonės gali padėti sukurti saugesnę ir malonesnę skaitmeninę aplinką bet kokio amžiaus vaikams ir jaunimui, atlikdamos šiuos veiksmus:</p> <p>Bendradarbiauti su kitais pramonės atstovais kuriant turinio klasifikavimo / amžiaus cenzo sistemas, kurios būtų pagrįstos priimtais nacionaliniais ar tarptautiniais standartais ir atitiktų atitinkamą terpę.</p> <p>Kur įmanoma, turinio klasifikacija turėtų būti vienoda, pavyzdžiui, kino filmo anonsas kino teatre ir išmaniajame telefone klientams būtų pateiktas pagal tą pačią klasifikaciją.</p> <p>Kurti vaikams ir jaunimui tinkamus produktus, kurie yra saugūs ir turi patikimą amžiaus patikrinimo sistemą.</p> <p>Norint padėti tėvams ir kitiems žmonėms nuspręsti, ar turinys tinka vaikams ir jaunimui, galima sukurti visuose įrenginiuose taikomas priemones, turinčias turinio vertinimo sistemas.</p> <p>Priimti tinkamus amžiaus patikrinimo metodus, kad vaikai ir jaunimas negalėtų naudotis vyresnio amžiaus žmonėms skirtu turiniu, svetainėmis, produktais ar interaktyviomis paslaugomis.</p> <p>Pateikti patarimus ir priminimus apie naudojamo turinio pobūdį ir amžiaus cenzą.</p> <p>Garso ir vaizdo bei daugialypės terpės paslaugas siūlanti įmonė, gali norėti suteikti asmens identifikavimo numerį vartotojams, norintiems pasiekti vaikams ir jaunimui žalingą turinį.</p> <p>Užtikrinti produktų ir paslaugų kainų bei apie vartotojus surinktos informacijos skaidrumą. Užtikrinti, kad duomenų rinkimo politika laikytųsi atitinkamų įstatymų, susijusių su vaikų ir jaunimo privatumu, įskaitant tėvų sutikimą dėl leidimo komercinėms įmonėms rinkti asmeninę informaciją iš vaiko ar apie jį.</p> <p>Užtikrinti, kad reklama ar komercinė komunikacija būtų aiškiai atpažįstama.</p> <p>Prižiūrėti internete talpinamą turinį ir pritaikyti jį vartotojų grupėms, kurios gali jį pasiekti, pavyzdžiui, nustatydami tinkamos vaikams ir jaunimui skirtos reklamos internete politiką. Jei turinyje siūlomas interaktyvus elementas, pvz., komentavimas, internetiniai forumai, socialiniai tinklai, žaidimų platformos, pokalbių kambariai ar pranešimų lentos, reikia pateikti klientams aiškias „pagrindines naudojimo taisykles“, laikantis paslaugų teikimo sąlygų ir vartotojo gairių.</p> <p>Prieš pradėdant teikti interneto paslaugą, reikia įvertinti ją naudosiančią auditoriją. Į vaikus orientuotos paslaugos turėtų pateikti tik jaunai auditorijai tinkamą turinį. Jei kyla abejonių,</p>

	<p>galima pasikonsultuoti su nacionalinėmis už vaikų apsaugą atsakingomis valdžios institucijomis.</p> <p>Pateikti aiškų ir faktinį turinio ženklimą. Atminkite, kad vartotojai gali rasti netinkamą turinį sekdami trečiųjų šalių svetainių nuorodas, apeinančias kontekstinius puslapius.</p>
<p>Vaikų, tėvų ir pedagogų švietimas apie vaikų saugumą ir jų atsakingą naudojimąsi IRT</p>	<p>Prižiūrimą skaitmeninį turinį siūlančios įmonės be techninių priemonių taip pat gali prisidėti prie vaikų švietimo, atlikdamos šiuos veiksmus:</p>
	<p>Teikti klientams konkrečią ir aiškią informaciją apie turinį, pvz., turinio tipą, amžiaus cenzą / apribojimus ir pan. bei informuoti apie atitinkamą galimą tėvų kontrolę; ir apie tai, kaip pranešti apie netinkamą ar neteisėtą turinį ir kaip bus į tokius pranešimus bus reaguojama.</p> <p>Interaktyviame pasaulyje ši informacija turėtų būti pateikiama kiekvienos programos turinio reklamoje.</p>
	<p>Paraginti suaugusiuosius, ypač tėvus, globėjus ir pedagogus, įsitraukti į vaikams ir jaunimui skirto turinio internete stebėjimą, kad jie galėtų padėti vaikams ir jaunimui rinktis perkamą turinį ir nustatyti elgesio taisykles.</p> <p>Padėti vaikams (ir tėvams bei globėjams) išmokti valdyti savo laiką internete ir suprasti, kaip naudotis technologijomis, kad jos leistų vaikams mėgautis internetu, o taip pat, kada reiktų pereiti prie kitos veiklos.</p>
	<p>Pateikti naudojimo taisykles aiškia ir prieinama kalba, kurios skatinantį vaikus ir jaunimą išlikti budriems ir atsakingiems naršant internete.</p>
	<p>Sukurti amžiui tinkamus įrankius, pvz., mokymo programas ir pagalbos centrus. Prireikus, dirbti su internetinėmis ar asmeninėmis prevencijos programomis ir konsultavimo klinikomis. Pavyzdžiui, jei yra pavojus, kad vaikai ir jaunimas pernelyg įsitraukia į technologijas, dėl ko jiems pasidaro sunku užmegzti asmeninius santykius ar dalyvauti sveikoje fizinėje veikloje, puslapis gali suteikti kontaktinę nuorodą pagalbos linijai ar konsultavimo tarnybai.</p> <p>Padaryti saugumo informaciją, pvz., pagalbos nuorodas, lengvai prieinamą ir aiškią, jei interneto turinys gali pritraukti daug vaikų ir jaunimo.</p>
	<p>Siūlyti tėvų priežiūros įrankį, pvz., „užraktą“, skirtą valdyti turinį, kurį galima pasiekti per tam tikrą naršyklę.</p>
	<p>Bendradarbiauti su tėvais siekiant užtikrinti, kad internete atskleista informacija apie vaikus nekeltų jiems pavojaus. Tai, kaip vaikai identifikuojami prižiūrimame turinyje, turi būti atidžiai apsvastyta ir priklauso nuo konteksto. Jei įmanoma, gaukite informuotą vaikų sutikimą, kai jie bus rodomi programose, filmuose, vaizdo įrašuose ir pan., ir gerbkite jų sprendimą, jei jie atsisako dalyvauti.</p>
	<p>Skaitmeninių technologijų naudojimas skatinant</p> <p>Prižiūrimą skaitmeninį turinį siūlančios įmonės gali padrąsinti vaikus, atlikdamos šiuos veiksmus:</p>

pilietinį įsitraukimą	Sukurti ir (arba) pasiūlyti kokybišką, sudėtingą, edukacinį, malonų ir įdomų turinį, kuris atitiktų vartotojo amžių ir padėtų vaikams ir jaunimui suvokti pasaulį, kuriame jie gyvena. Be to, kad toks turinys yra patrauklus, tinkamas naudoti, patikimas bei saugus, jis gali prisidėti prie vaikų ir jaunimo fizinio, protinio ir socialinio vystymosi, suteikdamas naujų galimybių pramogoms ir švietimui. Reiktų kurti turinį, kuris įgalintų vaikus priimti įvairovę ir būti pozityviais pavyzdžiais.
------------------------------	---

5.3 Funkcija C: vartotojų sukurtą turinį talpinimas ir vartotojų sujungimas

Buvo laikas, kai interneto pasaulyje dominavo suaugusieji, tačiau akivaizdu, kad vaikai ir jaunimas dabar yra sudaro didelę turinio kūrėjų dalį. Ši paslaugos funkcija, be kitų, skirta socialinių tinklų paslaugoms, programoms ir svetainėms, susijusioms su kūrybine realizacija. Vartotojus sujungiančias paslaugas galima suskirstyti į tris kategorijas:

- Pagrindines susirašinėjimo programėles (Facebook Messenger, Groupme, Line, Tinder, Telegram, Viber, WhatsApp).
- Socialinių tinklų paslaugas, kurios ieško ir talpina vartotojų sukurtą turinį ir leidžia vartotojams juo dalytis ir prisijungti prie savo ir kitų tinklų (Instagram, Facebook, SnapChat, TikTok).
- Tiesioginės transliacijos programėles (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

Paslaugų teikėjai reikalauja minimalaus amžiaus norint prisijungti prie platformų, tačiau tai sunku įgyvendinti, nes amžiaus patikrinimas priklauso nuo nurodyto amžiaus. Dauguma paslaugų, sujungiančių naujus vartotojus, taip pat leidžia naudotis vietos sekimo funkcijomis, dėl kurių šiomis paslaugomis besinaudojantys vaikai ir jaunuoliai tampa dar jautresni pavojui už interneto ribų.

4 lentelėje, kuri buvo pritaikyta pagal vieno iš didžiausių socialinių tinklų taisykles, vartotojų sukurtą turinį talpinantiems ir naujus vartotojus sujungiantiems paslaugų teikėjams pateikia gaires apie taisykles ir veiksmus, kurių jie gali imtis, kad sustiprintų vaikų saugumą internete.

4 lentelė: funkcijos C veiksmai užtikrinti vaikų saugumą internete:

Vaiko teisių integravimas į tinkamą įmonės politiką ir valdymo procesus	Vartotojų sukurtą turinį talpinančių ir vartotojus sujungiančių paslaugų teikėjai gali nustatyti, užkirsti kelią ir sušvelninti neigiamą IRT poveikį vaikų ir jaunimo teisėms bei paieškoti galimybių ginti vaikų ir jaunimo teises. <i>Žr. 1 lentelėje pateiktas bendrąsias gaires.</i>
--	---

Standartinių procesų kūrimas kovojant su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu	<p>Bendradarbiaujant su vyriausybe, teisėsaugos institucijomis, pilietine visuomene ir interneto karštųjų linijų organizacijomis, vartotojų sukurtą turinį talpinančių ir vartotojus sujungiančių paslaugų teikėjai gali atlikti pagrindinį vaidmenį kovojant su vaikų seksualinio išnaudojimo medžiaga (CSAM), atlikdamos šiuos veiksmus:</p>
	<p>Nustatyti bendrą tvarką, kaip skubiai suteikti pagalbą teisėsaugai ekstremalių situacijų bei paprastų patikrinimų metu.</p>
	<p>Nurodyti, kad įmonė visapusiškai bendradarbiaus su teisėsaugos tyrimais, jei bus pranešta apie neteisėtą turinį arba jis bus aptiktas, ir pateikti išsamią informaciją apie atitinkamas nuobaudas, tokias kaip baudos ar aptarnavimo paslaugų nutraukimas.</p>
	<p>Dirbti su vidinėmis funkcijomis, tokiomis kaip klientų aptarnavimas, sukčiavimo prevencija ir saugumas, kad įmonė tiesiogiai galėtų pranešti apie įtariamą neteisėtą turinį teisėsaugai ir interneto karštosioms linijoms. Geriausia, kad tai būtų daroma taip, jog interneto karštųjų linijų darbuotojai nesusidurtų su žalingu turiniu, o vaikai dėl to nenukentėtų dar kartą. Sukurkite politiką ar programą, skirtą skatinti darbuotojų atsparumą, saugumą ir gerovę, jei jiems tektų susidurti su žalinga medžiaga.</p>
	<p>Paslaugų teikimo sąlygose paminėti, kad neteisėtas turinys ir elgesys yra draudžiami, pabrėžiant tai, kad:</p> <ul style="list-style-type: none"> • žalingas turinys, įskaitant įtariamą vaikų viliojimą, siekiant juos išnaudoti, nebus toleruojamas; • neteisėtas turinys ir elgesys, įskaitant vaikų seksualinio išnaudojimo medžiagos (CSAM) įkėlimą ar tolesnį platinimą, nebus toleruojamas; • jei bus pranešta apie neteisėtą turinį ar bet kokį vaiko saugumo pažeidimą, įmonė apie tai informuos teisėsaugą ir visapusiškai su ja bendradarbiaus.
	<p>Dokumentuoti įmonės praktiką dėl vaikų seksualinio išnaudojimo medžiagos (CSAM), pradedant stebėjimu ir baigiant galutiniu turinio perdavimu bei sunaikinimu. Į dokumentaciją įtraukite visų darbuotojų, atsakingų už medžiagos tvarkymą, sąrašą.</p>
	<p>Taikykite vartotojų sukurtą turinio nuosavybės politiką, įskaitant galimybę pašalinti vartotojo sukurtą turinį vartotojo prašymu. Pašalinkite turinį, kuris pažeidžia teikėjo politiką, ir įspėkite jį paskelbusį naudotoją apie pažeidimą.</p>

<p>Standartinių procesų kūrimas kovai su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu (tęsinys)</p>	<p>Nurodykite, kad priimtinių naudojimo taisyklių nesilaikymas turės pasekmes, įskaitant:</p> <ul style="list-style-type: none"> • turinio pašalinimą, jų paskyros sustabdymą ar panaikinimą; • jų galimybės dalytis tam tikro tipo turiniu ar naudoti tam tikras funkcijas panaikinimą; • draudimą susisiekti su vaikais; • teisėsaugos informavimą.
<p>Standartinių procesų kūrimas kovai su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu (tęsinys)</p>	<p>Skatinti pranešimus apie seksualinio vaikų išnaudojimo ar bet kokio kito neteisėto turinį ir užtikrinti, kad klientai, pastebėję tokį turinį, žino, kaip apie jį pranešti.</p> <p>Kurti sistemas ir apmokyti personalą, kuris galėtų įvertinti problemas ir imtis atitinkamų veiksmų. Sukurti visapusiškas ir pakankamai išteklių turinčias komandas vartotojų pagalbai. Geriausia, jei šios komandos būtų mokomos spręsti įvairaus pobūdžio problemas, kad būtų užtikrinta tinkama reakcija ir atliekami atitinkami veiksmai. Kai vartotojas pateikia pranešimą, atsižvelgiant į incidento tipą, jis turėtų būti perduotas atitinkamam personalui.</p> <p>Įmonė taip pat gali sudaryti specialias grupes, kurios nagrinės vartotojų apeliacijas tais atvejais, jei pranešimai būtų pateikti per klaidą.</p> <p>Turėti procesus, skirtus nedelsiant pašalinti arba blokuoti prieigą prie vaikų seksualinio išnaudojimo medžiagos (CSAM), įskaitant pranešimo apie draudžiamą turinį ir jo pašalinimo (angl. notice and takedown) procesus neteisėto turinio pašalinimui. Užtikrinti, kad trečiosios šalys, su kuriomis įmonė palaiko sutartinius santykius, turėtų panašiai patikimus pranešimo ir pašalinimo (angl. notice and takedown) procesus. Jei leidžia įstatymai, tyrimo metu medžiagą galima laikyti nusikaltimo įrodymams.</p> <p>Sukurti technines sistemas, kurios galėtų aptikti žinomą neteisėtą turinį ir užkirsti kelią jo platinimui, įskaitant ir įkėlimą į privačias grupes, arba pažymėti jį, kaip reikalaujantį bendrovės saugos komandos peržiūros. Imtis visų atitinkamų priemonių apsaugoti nuo vaikų seksualinio išnaudojimo medžiagos (CSAM) talpinimo, platinimo ar kūrimo.</p> <p>Kur įmanoma, sukurti aktyvias technines priemones, kad būtų galima išanalizuoti su paskyra susijusius objektus ir metaduomenis, siekiant nustatyti nusikalstamą elgesį ar jo modelius, ir imtis atitinkamų veiksmų.</p>

	<p>Jei programa ar paslauga leidžia klientams įkelti ir saugoti nuotraukas serveriuose, kurie priklauso įmonei ar yra jos valdomi, reikia parengti procesus ir įrankius galimų seksualinio vaikų išnaudojimo nuotraukų atpažinimui. Reikia apsvarstyti aktyvias identifikavimo technologijas, tokias kaip skenavimo technologija ar žmonių atvaizdų peržiūra.</p>
<p>Saugesnės ir amžių atitinkančios interneto aplinkos kūrimas</p>	<p>Paslaugų teikėjai, siūlantys vartotojo sukurtą turinį ir sujungiantys vartotojus, gali padėti sukurti saugesnę, malonesnę skaitmeninę aplinką bet kokio amžiaus vaikams, atlikdami šiuos veiksmus:</p> <p>Laikydami paslaugų teikimo sąlygų, naudojant paprastą ir aiškiai suprantamą kalbą, perteikti klientams pagrindines taisykles, nusakančias:</p> <ul style="list-style-type: none"> • paslaugos pobūdį ir ko tikimasi iš jos vartotojų; • koks turinys ir elgesys yra priimtinas ir koks ne, o taip pat informuoti, kad nelegalus turinys yra draudžiamas; • taisyklių pažeidimo pasekmes, pavyzdžiui, tai gali būti pranešimas teisėsaugai ar vartotojo paskyros sustabdymas. <p>Pagrindiniai saugos ir teisiniai pranešimai turėtų būti pateikiami amžiui tinkamu formatu (t. y. naudojant intuityvias piktogramas ir simbolius) tiek registracijos metu, tiek kaskart atliekant skirtingus veiksmus svetainėje.</p> <p>Palengvinti pranešimų dėl netinkamo naudojimo teikimą, taikant standartinius ir prieinamus procesus, kad būtų galima išspręsti įvairias problemas, pvz., gaunamus nepageidaujamus pranešimus (šlamšto (angl. „spam“) el. laiškus, patyčias) ar netinkamą turinį.</p> <p>Pateikti amžiui tinkamo turinio bendrinimo ir prieinamumo nustatymus. Pavyzdžiui, galima padaryti, kad vaikų ir jaunimo privatumo ir matomumo nustatymai būtų griežtesni nei pagal numatytuosius nustatymus suaugusiems.</p> <p>Pritaikyti minimalaus amžiaus reikalavimus ir remti naujų amžiaus patikrinimo sistemų, tokių kaip biometrija, tyrimus ir plėtrą, naudojant žinomus tarptautinius tokių priemonių kūrimo standartus. Imtis veiksmų siekiant nustatyti ir pašalinti nepilnamečius vartotojus, kurie neteisingai nurodė savo amžių, norėdami gauti prieigą. Reikia atsižvelgti į tam galima reikalingą papildomų asmens duomenų rinkimą ir poreikį apriboti tokios informacijos rinkimą ir saugojimą bei jos tvarkymą.</p> <p>Parengti atitinkamus prisijungimo procesus, siekiant nustatyti, ar vartotojai yra pakankamo amžiaus pasiekti tam tikrą turinį ar paslaugą, neatskleidžiant jų tapatybės, vietos ir kitos asmeninės informacijos. Atitinkamai naudoti nacionaliniu mastu nustatytas funkcines amžiaus tikrinimo sistemas ten, kur yra tinkamos priemonės užtikrinti vaiko privatumą. Pranešimo funkcija arba</p>

	<p>pagalbos tarnyba / centras gali paskatinti vartotojus pranešti apie savo amžių suklastojusius žmones.</p>
<p>Saugesnės ir amžių atitinkančios interneto aplinkos kūrimas (tęsinys)</p>	<p>Apsaugoti jaunesnius vartotojus nuo nepageidaujamo bendravimo ir užtikrinti, kad būtų taikomos privatumo ir informacijos rinkimo gairės.</p> <p>Rasti būdus, kaip būtų galima peržiūrėti ir patikrinti įkeltas nuotraukas ir vaizdo įrašus. Tam gali būti naudojami tokie įrankiai kaip žinomų vaizdų maiša (angl. hashing) ir vaizdų atpažinimo programinė įranga. Vaikams skirtose paslaugose nuotraukas ir vaizdo įrašus galima patikrinti iš anksto, siekiant nustatyti, ar vaikai nesidalina neskelbtina asmenine informacija apie save ar kitus.</p> <p>Siekiant kontroliuoti prieigą prie vartotojų sukurto turinio ir apsaugoti vaikus ir jaunuolius internete nuo netinkamo ar neteisėto turinio, gali būti naudojamos kelios priemonės. Reikia įsitinkinti, kad, naudojami saugūs slaptažodžiai, taip siekiant apsaugoti vaikus ir jaunimą žaidimų ir kitose socialinės žiniasklaidos vietose. Kiti būdai apsaugos būdai:</p> <ul style="list-style-type: none"> • peržiūrėti diskusijų grupes, siekiant nustatyti žalingą temą, neapykantos kurstymą ir neteisėtą elgesį ir ištrinti tokį turinį, kai nustatoma, kad tai pažeidžia naudojimo sąlygas; • sukurti įrankius, skirtus aktyviai ieškoti ir pašalinti turinį, kuris yra neteisėtas arba pažeidžia įmonės sąlygas, taip pat įrankius, skirtus užkirsti kelią žinomo neteisėto turinio įkėlimui į svetainę; • iš anksto moderuoti pranešimų lentas su specializuota vaikų ir jaunimo moderatorių komanda, tikrinančia taisyklėms prieštaraujantį turinį. Galima tikrinti kiekvieną pranešimą dar prieš jį paskelbiant, o moderatoriai taip pat gali pastebėti ir pažymėti įtartinus ar pažeidžiamus vartotojus; • įsteigti už bendruomenę atsakingų žmonių komandą, kuri pirmoji sužinotų apie moderatoriams klausimų keliančius vartotojus.

	<p>Atsakyti už komercinio turinio peržiūrą, įskaitant forumus, socialinius tinklus ir žaidimų svetaines. Įgyvendinti tinkamus standartus ir taisykles, siekiant apsaugoti vaikus nuo jų amžiui netinkamos reklamos ir nustatyti aiškias s vaikams ir jaunimui skirtos reklamos ribas internete.</p>
<p>Vaikų, tėvų ir pedagogų švietimas apie vaikų saugumą ir jų atsakingą naudojimąsi IRT</p>	<p>Vartotojų sukurtą turinį siūlantys paslaugų teikėjai, be techninių priemonių, taip pat gali prisidėti prie švietimo ir įgalinimo veiklos, atlikdami šiuos veiksmus:</p>
	<p>Sukurti saugos politiką, skirtą patarimams, straipsniams, funkcijoms ir dialogui apie skaitmeninį pilietiškumą, taip pat nuorodas į naudingą trečiųjų šalių ekspertų turinį. Saugos patarimai turėtų būti lengvai pastebimi ir pateikiami lengvai suprantama kalba. Platformos teikėjai taip pat raginami turėti vienodą naršymo sąsają įvairiuose įrenginiuose (pavyzdžiui, įprastuose bei planšetiniuose kompiuteriuose ar mobiliuosiuose telefonuose).</p>
	<p>Siūlyti tėvams aiškią informaciją apie turinio ir paslaugų tipus, įskaitant, pavyzdžiui, paaiškinimus apie socialinių tinklų svetaines ir vietos nustatymu pagrįstas paslaugas, kai interneto prieiga pasiekama per mobiliuosius įrenginius, ir tėvų turimas galimybes tai valdyti.</p>
	<p>Informuoti tėvus apie tai, kaip pranešti apie piktnaudžiavimą, netinkamą naudojimą ir netinkamą ar neteisėtą turinį ir kaip bus vykdomas šis procesas. Pranešti jiems, kokios paslaugos yra ribojamos pagal amžių, ir kitus būdus saugiai ir atsakingai naudotis interaktyviomis paslaugomis.</p>
	<p>Sukurti pasitikėjimu ir reputacija paremtą sistemą, kad būtų skatinamas geras elgesys ir bendraamžiai galėtų vieni iš kitų semtis gerosios praktikos pavyzdžių. Akcentuoti socialinius pranešimus, kurie leidžia žmonėms susisiekti su kitais vartotojais ar patikimais draugais, kurie jiems padėtų išspręsti konfliktą ar pradėti pokalbį apie netinkamą turinį.</p>
	<p>Teikti patarimus ir priminimus apie tam tikros paslaugos ar turinio pobūdį ir kaip ja naudotis saugiai. Įtraukti bendruomenės taisykles į interaktyvias paslaugas, pavyzdžiui, naudojant iššokančius langus, kurie vartotojams primena apie tinkamą ir saugų elgesį, pavyzdžiui, nenurodyti savo kontaktinės informacijos.</p>
	<p>Bendradarbiauti su tėvais ir padėti jiems užtikrinti, kad internete apie vaikus atskleista informacija nekeltų jiems pavojaus. Jei įmanoma, gauti patvirtintą vaikų sutikimą, jei jie rodomi jų pačių sukurtame turinyje, ir gerbti jų sprendimą, jei jie atsisako.</p>

Skaitmeninių technologijų naudojimas skatinant pilietinį įsitraukimą	Vartotojų sukurto turinio talpinimo paslaugų tiekėjai gali paskatinti vaikus ir jaunimą ir suteikti jiems daugiau galimybių, remdami jų teisę į dalyvavimą.
	<i>Žr. 1 lentelėje pateiktas bendrąsias gaires.</i>

5.4 Funkcija D: dirbtinio intelekto valdomos sistemos

Padidėjus dėmesiui giliojo mokymosi technologijoms, žmonės pradėjo vartoti sąvokas „dirbtinis intelektas“, „mašininis mokymasis“ ir „gilus mokymasis“, turėdami galvoje „intelektualaus“ elgesio atkartojimo mašinose koncepciją. Šiame skyriuje daugiausia dėmesio skiriama būdams, kaip mašininis mokymasis ir giliojo mokymosi procesai daro įtaką vaikų gyvenimui ir galiausiai jų žmogaus teisėms.

„Dėl eksponentinės, per pastaruosius kelerius metus įvykusios, dirbtiniu intelektu pagrįstų technologijų pažangos, dabartinė vaikų teises ginanti tarptautinė sistema aiškiai neišsprendžia daugelio dirbtinio intelekto kūrimo ir naudojimo klausimų. Tačiau joje minimos kelios teisės, kurias šios technologijos gali paveikti, o tai yra svarbus pradinis taškas, analizuojant, kaip naujos technologijos gali paveikti vaikų teises, pvz., teises į privatumą, švietimą, žaidimus ir į nediskriminavimą“.²⁶

Dirbtinio intelekto taikymas gali paveikti įvairių socialiniuose tinkluose naudojamų paslaugų, tokių kaip vaizdo transliacijos platformos, vaikams daromą poveikį. Mašininio mokymosi algoritmai, rekomendacijų optimizavimas, kuriuos pirmiausia naudoja populiarios vaizdo įrašų bendrinimo platformos, yra sukurti taip, kad būtų užtikrinta maksimali konkrečių vaizdo įrašų peržiūra per tam tikrą laiką.²⁷ Jutiklinio ekrano technologija ir šių platformų dizainas leidžia labai mažiems vaikams naršyti šį turinį. Ypatingą susirūpinimą kelia tai, kad algoritmai, kurie naudoja rekomenduojamus vaizdo įrašus, gali įtraukti vaikus į netinkamo turinio „rekomendavimo burbulus“. Kadangi vaikai yra ypač linkę į turinio rekomendacijas, šokiruojantys „susiję vaizdo įrašai“ gali patraukti jų dėmesį ir nukreipti juos nuo labiau vaikams pritaikyto turinio.²⁸

Dirbtinis intelektas taip pat turi įtakos vaikų saugumui internete, susijusiam su išmaniaisiais žaislais. Įvairūs, su išmaniųjų žaislų veikimu susiję, procesai, susiduria su atitinkamais iššūkiais, t. y. žaislas (kurį naudoja vaikas), mobilioji programa, veikianti kaip „Wi-Fi“ ryšio prieigos taškas, ir suasmeninta žaislo (vartotojo) interneto paskyra, kurioje saugomi duomenys. Tokie žaislai sujungti su debesų serveriais, kuriuose saugomi ir apdorojami žaislų naudojančių vaikų pateikti duomenys. Šis modelis kelia susirūpinimą dėl privatumo, jei saugumas nėra akcentuojamas kiekviename žingsnyje. Tai įrodo daugybė įsilaužimų atvejų, kai nutekinama asmeninė informacija. Be to, kai kuriuos įrenginius, į kuriuos buvo įsilaužta (įskaitant išmaniuosius įrenginius, tokius kaip kūdikių stebėjimo prietaisai, balsu valdomi įrenginiai ir kt.), gali būti naudojami vartotojų stebėjimui be jų žinios ar sutikimo.

Integruojant vaikams kylančią grėsmę nustatyti skirtus mechanizmus, pritaikomus būtent vaikų naudojamiems įrenginiams, pavyzdžiui, teikiant patarimus ir rekomendacijas, pagrįstas pastebėtomis elgesio tendencijomis (kaip minėta anksčiau su „BBC Own It“ programa), labai

²⁶ UNICEF ir UC Berkeley, „Executive Summary: Artificial Intelligence and Children’s Rights“, 2018.

²⁷ Ten pat.

²⁸ Ten pat.

svarbu, kad išmaniuosius įrenginius kuriančios įmonės pagrįstų šias rekomendacijas turimais įrodymais ir parengtų jas konsultuodamiesi su vaikų apsaugos ekspertais.

Nors kai kurios kompanijos propaguoja etiško intelekto naudojimo principus,²⁹ neaišku, ar yra kokia nors DI ir vaikams skirta viešoji politika.³⁰ Kelios technologijų ir prekybos asociacijos bei informatikos grupės parengė etikos principus, susijusius su dirbtiniu intelektu.³¹ Tačiau juose nėra aiškiai kalbama apie vaiko teises ar būdus, kuriais šios dirbtinio intelekto technologijos gali kelti riziką vaikams, arba tokių problemų sprendimą.

²⁹ Žr. Microsoft, "Salient Human Rights Issues", pranešimą - FY17; ir Google, "Responsible Development of AI" (2018).

³⁰ Microsoft Official Blog, "The Future Computed: Artificial Intelligence and its role in society", 2018.

³¹ The Guardian, "'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft", 2016.

„Kaip ir korporacijos, vyriausybės visame pasaulyje priėmė strategijas, kaip rodyti pavyzdį kuriant ir naudojant dirbtinį intelektą, puoselėjant naujovėms ir korporacijoms palankią aplinką.“³² Tačiau neaišku, kaip tokiose nacionalinėse strategijose tiesiogiai atsižvelgiama į vaikų teises.

„Facebook“ kova su savižudybėmis ir savęs žalojimu susijusiu turiniu

2019 m. „Facebook“ pradėjo reguliariai [konsultuotis](#) su ekspertais iš viso pasaulio, kad aptartų didesnę susirūpinimą keliančias temas, susijusias su savižudybe ir savęs žalojimu. Tai apima, kaip elgtis radus savižudybės raštelius ar riziką, susijusia su slegiančiu turiniu internete ir žiniose rodomais savižudybių vaizdais. Daugiau informacijos apie šiuos susitikimus galima rasti naujajame „Facebook“ [savižudybių prevencijos puslapyje](#), esančiame „Facebook“ [saugos centre](#). Šios konsultacijos padėjo sukurti keletą patobulinimų, kaip „Facebook“ galėtų tvarkyti tokio tipo turinį. Pavyzdžiui, buvo sustiprinta prieš savęs žalojimą nukreipta politika, uždraudžiant grafiškus pjaustymo vaizdus, taip siekiant išvengti savęs žalojimo skatinimo. Net kai kas nors ieško pagalbos arba parodo save, kad pasveiko, „Facebook“ dabar uždengia net ir sugijusių įsipjovimų vaizdus. Šio tipo turinys dabar atrandamas taikant dirbtinį intelektą, pagal kurį galima automatiškai atlikti veiksmus su potencialiai žalingu turiniu, įskaitant jo pašalinimą ar vaizdų uždengimą. Nuo 2019 m. balandžio iki birželio „Facebook“ savo svetainėje sutvarkė daugiau nei 1,5 milijono su savižudybe ir savęs žalojimu susijusio turinio vienetų ir nustatė daugiau nei 95 procentus jo, kol apie tai dar nepranešė vartotojai. Tuo pačiu laikotarpiu „Instagram“ sutvarkė daugiau nei 800 tūkstančių panašaus turinio vienetų, iš kurių daugiau nei 77 proc. aptikta prieš pranešimus iš vartotojų.

Galimų patyčių ar tarpusavio smurto nustatymas realiuoju laiku ir pranešimas vartotojams „Instagram“ diegia dirbtinį intelektą, kad pašalintų tokį elgesį kaip įžeidimai, gėdos skatinimas ir nepagarba. Naudojamiesi sudėtingais pranešimų teikimo įrankiais, moderatoriai gali greitai uždaryti patyčių vykdytojų priklausančią paskyrą internete.

Geroji praktika: dirbtinio intelekto naudojimas aptinkant vaikų seksualinio išnaudojimo medžiagą internete

Remdamasis dideliu „Microsoft“ „PhotoDNA“ indėliu kovojant su vaikų seksualiniu išnaudojimu ir neseniai paskelbta „Google Content Safety API“, „Facebook“ taip pat sukūrė technologijas, skirtas aptikti vaikų seksualinio išnaudojimo medžiagą.

Šios technologijos, žinomos kaip PDQ ir TMK + PDQF, yra dalis įrankių, kuriuos „Facebook“ naudoja žalingam turiniui aptikti. Kiti pramonėje prieinami algoritmai ir priemonės yra pHash, aHash ir dHash. „Facebook“ nuotraukų derinimo algoritmas PDQ sukurtas pagal pHash, nors nuo pat pradžių jis buvo kuriamas kaip atskiras algoritmas su nepriklausomu programinės įrangos pritaikymu. Vaizdo įrašų atpažinimo technologiją „TMK + PDQF“ kartu sukūrė „Facebook“ [DI tyrimų komanda](#) ir Italijos Modenos bei Reggio Emilia universitetų mokslininkai.

Šios technologijos sukuria efektyvų būdą saugoti failus kaip trumpas skaitmenines maišas (angl. hashes), pagal kurių reikšmes galima nustatyti, ar du failai yra vienodi ar panašūs, net ir be originalaus vaizdo ar vaizdo įrašo. Maišų reikšmėmis (angl. hashes) taip pat gali būti lengviau dalijamasi su kitomis įmonėmis ir ne pelno organizacijomis.

³² Ten pat.

PDQ ir TMK + PDQF buvo suprojektuoti veikti dideliu mastu, palaikant vaizdo kadry maišos (angl. hashing) ir realaus laiko programas.

Kai kurios rekomendacijos, skirtos įmonėms suderinti savo principus kuriant ir įgyvendinant vaikams skirtus DI pagrįstus sprendimus, pateiktos 5 lentelėje.

Rekomendacijos yra pagrįstos UNICEF darbu kuriant pasaulines intelektinės nuosavybės ir vaikų politikos gaires, kurios bus skirtos vyriausybėms ir pramonei. Norėdami gauti daugiau informacijos apie projektą, apsilankykite <https://www.unicef.org/globalinsight/featured-projects/ai-children>. Rekomendacijos taip pat remiasi UNICEF ir UC Berkeley straipsniu apie dirbtinį intelektą ir vaiko teises.³³

5 lentelė: COP kontrolinis sąrašas, skirtas savybei D: dirbtinio intelekto valdomoms sistemoms

Vaiko teisių integravimas į tinkamą įmonės politiką ir valdymo procesus	Dirbtiniu intelektu pagrįstų sistemų teikėjai gali nustatyti, sustabdyti ar sušvelninti neigiamą IRT poveikį vaikų ir jaunimo teisėms, ir prisidėti prie vaikų ir jaunimo teisių gynimo.
	Dirbtinio intelekto sistemos turėtų būti kuriamos, pritaikomos ir tiriamos siekiant gerbti, skatinti ir saugoti vaiko teises, kaip nustatyta vaiko teisių konvencijoje. Vaikystė, kuri vis labiau įtraukia skaitmeninę aplinką, yra laikas, skirtas ypatingai priežiūrai ir pagalbai. Dirbtinio intelekto sistemos turėtų būti vienas iš pagalbos įrankių.
	Kuriant vaikams skirtus produktus, reikia pritaikyti įtraukiančio dizaino metodus, kurie maksimaliai padidina lyčių, geografinę ir kultūrinę įvairovę ir įtraukia platų suinteresuotųjų šalių ratą, pvz., tėvus, mokytojus, vaikų psichologus ir, kai tai yra tinkama, pačius vaikus.
	Turėtų būti sukurtos valdymo sistemos, įskaitant elgesio gaires, įstatymus, standartus ir reguliavimo institucijas, kad būtų galima prižiūrėti procesus, užtikrinančius, kad dirbtinio intelekto sistemų taikymas nepažeistų vaiko teisių.
Standartinių procesų kūrimas kovai su vaikų seksualinio išnaudojimo medžiagos (CSAM) platinimu	Dirbtinio intelekto valdomų sistemų teikėjai, bendradarbiaudami su vyriausybe, teisėsauga, pilietine visuomene ir interneto karštųjų linijų organizacijomis, vaidina pagrindinį vaidmenį kovojant su vaikų seksualinio išnaudojimo medžiaga (CSAM), imdamiesi šių veiksmų:
	<i>Žr. 1 lentelėje pateiktas bendrąsias gaires.</i>

³³ UNICEF ir UC Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.

Saugesnės ir amžių atitinkančios interneto aplinkos kūrimas	Dirbtiniu intelektu pagrįstų sistemų teikėjai gali padėti sukurti saugesnę ir malonesnę skaitmeninę aplinką bet kokio amžiaus vaikams, atlikdami šiuos veiksmus:
	Kuriant vaikams įtaką darančias technologijas, reikia laikytis daugiadisciplininio požiūrio ir konsultuotis su pilietine visuomene, įskaitant akademinę bendruomenę, siekiant nustatyti galimą šių technologijų poveikį įvairių galutinių vartotojų teisėms.
	Kurti į vaikų saugumą ir privatumą orientuotus dažniausiai naudojamus produktus ir paslaugas.
	Kadangi dirbtinio intelekto sistemos reikalauja duomenų, įmonės, naudojančios dirbtinį intelektą savo paslaugoms, turėtų būti ypač budrios renkant, tvarkant, saugant, parduodant ir skelbiant vaikų asmens duomenis. Dirbtinio intelekto sistemos turėtų būti skaidrios ir turėtų būti įmanoma sužinoti, kaip ir kodėl sistema priėmė tam tikrą sprendimą arba, robotų atveju, elgėsi taip, kaip elgėsi. Šis skaidrumas yra labai svarbus ugdant pasitikėjimą ir palengvinant auditą, tyrimus ir skundus įtarus žalą vaikams. Reikia užtikrinti, kad būtų taikomi funkciniai ir teisiniai pagalbos mechanizmai, jei vaikai yra sužeisti arba teigia, kad jiems dirbtinio intelekto sistemos padarė žalą. Turėtų būti nustatyti procesai, kaip laiku ištaisyti bet kokį diskriminacinį poveikį, ir įsteigtos priežiūros įstaigos, teikiančios apeliacijas ir nuolat besirūpinančios vaikų saugumu. Atskaitomybė ir žalos atlyginimo mechanizmai veikia išvien.
	Reikia parengti ypatingai svarbių duomenų tvarkymo metodus, įskaitant skundus dėl užgauliojimo ar kitų neigiamą poveikį turinčių veiksmų, kurie gali skliti per įmonės produktus. Skaitmeninės platformos ir dirbtinio intelekto sistemos turėtų kuo labiau sumažinti duomenų apie vaikus rinkimą ir maksimaliai padidinti vaikų turimą kontrolę jų sukurtų duomenų atžvilgiu. Naudojimo sąlygos turėtų būti suprantamos vaikams, kad jie būtų tinkamai informuoti.
Vaikų, tėvų ir pedagogų švietimas apie vaikų saugumą ir jų atsakingą naudojimąsi IRT	Dirbtiniu intelektu pagrįstų sistemų teikėjai, be techninių priemonių, taip pat gali prisidėti prie švietimo ir įgalinimo veiklos, atlikdami šiuos veiksmus.
	Turėtų būti įmanoma paaiškinti dirbtinio intelekto sistemų paskirtį vaikams, jų tėvams ar globėjams, kad jie turėtų galimybę nuspręsti dėl tokių platformų naudojimo.
Skaitmeninių technologijų naudojimas skatinant pilietinį įsitraukimą	Dirbtiniu intelektu pagrįstų sistemų teikėjai gali paskatinti vaikus ir jaunimą ir suteikti jiems daugiau galimybių, remdami jų teisę į dalyvavimą.
	<i>Žr. 1 lentelėje pateiktas bendrąsias gaires.</i>

<p>Technologijų pažangos naudojimas vaikų apsaugai ir mokymui</p>	<p>Dirbtiniu intelektu pagrįstos sistemos turėtų būti sukurtos taip, kad būtų skatinama vaikų raida ir gerovė, kaip sistemos kūrimo, pritaikymo ir įgyvendinimo rezultatas. Geriausia turima ir plačiai pripažinta raidos ir gerovės metrika turėtų būti jų atskaitos taškas.</p> <p>Įmonės, bendradarbiaudamos su pagrindiniais vaikų teisių ekspertais ir pačiais vaikais, turėtų investuoti į etinių dirbtiniu intelektu pagrįstų įrankių, skirtų nustatyti vaikų seksualinio išnaudojimo atvejus internete, priekabiavimą ir patyčias internete, tyrimus ir plėtrą.</p> <p>Dirbtinio intelekto technologijos pažanga turėtų būti taikoma siekiant užtikrinti, kad vaikai gauna tik jų amžių atitinkančias žinutes, nepakenkiant jų tapatybei, vietai ir asmens duomenims.</p>
--	---

Nuorodos

[GDPR tekstas](#) (2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir panaikinantis Direktyvą 95/46 / EB (Bendrasis duomenų apsaugos reglamentas)) ir tekstas, paskelbtas [oficialiajame ES leidinyje](#).

[Patikslinta AVMS \(garso ir vaizdo žiniasklaidos paslaugos\)](#), iš dalies keičianti Direktyvą 2010/13 / ES dėl tam tikrų valstybių narių įstatymuose ir kituose teisės aktuose esančių nuostatų, susijusių su garso ir vaizdo žiniasklaidos paslaugų teikimu, derinimo (Garso ir vaizdo žiniasklaidos paslaugų direktyva), siekiant pakeisti rinkos realijos ir tekstas, paskelbtas [oficialiajame ES leidinyje](#).

BBC taisyklės:

- [Vaikų apsaugos ir apsaugos politikos 2017 m. versija](#), pataisyta 2018 m. ir [atnaujinta 2019 m. versija](#).
- [BBC darbas su jaunimu ir vaikais](#);
- Nepriklausomų prodiuserių kompanijų, dirbančių „BBC Productions“, išorės teikėjų sistemoje, [taisyklės dėl vaikų apsaugos](#);
- Vadovavimas: bendravimas su vaikais ir jaunimu internete [dėl internetinės veiklos redakcinių gairių](#).

Tyrimas, įrodantis, kad Jungtinės Karalystės socialinėje žiniasklaidoje nebuvo laikomasi amžiaus patikrinimo: [2016](#), [2017](#); [2020](#).

Terminai

Toliau pateikiami apibrėžimai daugiausia remiasi egzistuojančia terminologija, išdėstyta 1989 m. Vaiko teisių konvencijoje, taip pat 2016 m. jungtinės kovos su vaikų seksualiniu išnaudojimu darbo grupės [Vaikų apsaugos nuo seksualinio išnaudojimo ir seksualinės prievartos terminų gairėse](#) (Liuksemburgo gairės), 2007 m. Europos Tarybos konvencija dėl vaikų apsaugos nuo seksualinio išnaudojimo ir seksualinės prievartos, o taip pat 2019 m. UNICEF „Global Kids Online“ ataskaita.

Paaugliai

Paaugliai yra 10–19 metų žmonės. Svarbu pažymėti, kad, pagal tarptautinę teisę, „paaugliai“ nėra griežtas terminas, nes jaunesni nei 18 metų asmenys laikomi vaikais, o 18–19 metų asmenys laikomi pilnamečiais, nebent nacionalinė teisė nurodo kitaip.³⁴

Dirbtinis intelektas

Plačiąja prasme, dirbtinis intelektas (DI) reiškia sistemas, kurios yra grynoji mokslinė fantastika (vadinamasis „stiprus“ DI su savimonės forma) ir sistemas, kurios jau veikia ir gali atlikti labai sudėtingas užduotis (sistemos, įvardinamos kaip „silpnas“ ar „vidutinis“ DI, tokios kaip veido ar balso atpažinimas ir transporto priemonių vairavimas).³⁵

Dirbtinio intelekto sistemos

Dirbtinio intelekto sistema yra mašininė sistema, kuri tam tikram žmogaus nustatytų tikslų rinkiniui gali pateikti prognozes, rekomendacijas ar sprendimus, turinčius įtakos realiai ar virtualiajai aplinkai. DI sistemos yra skirtos įvairiems autonomijos lygiams.³⁶

Alexa

„Amazon Alexa“, žinomas tiesiog kaip „Alexa“, yra „Amazon“ sukurtas virtualus dirbtinio intelekto padėjėjas. Jis gali bendrauti balsu, atkurti muziką, sudaryti darbų sąrašus, nustatyti žadintuvus, transliuoti tinklalaidės, leisti garso knygas ir teikti orų, eismo, sporto ir kitą realaus laiko informaciją, pvz., naujienas. „Alexa“ taip pat gali valdyti keletą išmaniųjų įrenginių, naudodama save kaip namų automatikos sistemą. Vartotojai gali išplėsti „Alexa“ galimybes įdiegdami „įgūdžius“ (papildomas funkcijas, kurias kuria trečiųjų šalių tiekėjai, dar žinomas kaip programėlės, tokias kaip orų ir garso programėlės).³⁷

³⁴ UNICEF ir ITU, „Guidelines for Industry on Child Online Protection“, 2014.

³⁵ Europos Taryba, „What’s AI?“.

³⁶ OECD, „Recommendation of the Council on Artificial Intelligence“, 2019.

³⁷ UNICEF ir ITU, „Guidelines for Industry on Child Online Protection“, 2014.

Geriausias vaiko interesas

Nurodo visus elementus, būtinus norint priimti sprendimą tam tikroje situacijoje dėl konkretaus vaiko ar vaikų grupės.³⁸

Vaikas

Pagal Vaiko teisių konvencijos 1 straipsnį, vaikas yra bet kuris jaunesnis nei 18 metų asmuo, išskyrus atvejus, kai pagal nacionalinę teisę pilnametystės sulaukiama anksčiau.³⁹

Vaikų seksualinis išnaudojimas ir prievarta

Apibūdina visas seksualinio išnaudojimo ir seksualinės prievartos formas, pvz. „A) vaiko skatinimas ar prievarta verstis bet kokia neteisėta seksualine veikla; b) vaikų išnaudojimas prostitucijoje ar kitoje neteisėtoje seksualinėje veikloje; c) vaikų išnaudojimas pornografijoje ar kitame turinyje“,⁴⁰ taip pat „seksualinis kontaktas, kuris paprastai apima jėgą prieš asmenį be sutikimo“.⁴¹ Vaikų seksualinis išnaudojimas ir prievarta vis dažniau vyksta internetu arba kitu internetu pagrįstu ryšiu.

Vaikų seksualinio išnaudojimo ir prievartos turinys

Sparti IRT raida sukūrė naujas vaikų seksualinio išnaudojimo ir prievartos formas internete, kurioms nereikia fizinio susitikimo su vaiku.⁴² Nors daugelyje jurisdikcijų seksualinės prievartos prieš vaikus vaizdai ir vaizdo įrašai vis dar žymimi kaip „vaikų pornografija“ arba „nepadorios vaikų nuotraukos“, šiose gairėse šie terminai bendrai vadinami „vaikų seksualinio išnaudojimo medžiaga“ (CSAM). Šis terminas atitinka plačiajuosčio ryšio komisijos gaires ir „WePROTECT Global Alliances“ pavyzdinį nacionalinį atsaką⁴³ ir turinį apibūdina tiksliau. Pornografija reiškia teisėtą, komercinę pramonę ir, kaip teigiama Liuksemburgo gairėse, šio termino vartojimas:

„gali (tyčia ar ne) sumenkinti tikrąją seksualinės prievartos ir (arba) seksualinio vaikų išnaudojimo reikšmę. Sąvoka „vaikų pornografija“ gali reikšti, kad veiksmai atliekami su vaiko sutikimu ir yra teisėta seksualinė medžiaga“. Naudojant vaikų seksualinio išnaudojimo medžiagos (CSAM) terminą, mes kalbame apie medžiagą, vaizduojančią seksualinę prievartą prieš vaikus ir (arba) jų išnaudojimą. Tai apima, tačiau neapsiriboja, medžiagą, kurioje užfiksuota seksualinė prievarta prieš vaikus, vaikų, priverstinai atliekančių seksualinius veiksmus, nuotraukas ar vaizdo įrašus ir vaikų lytinių organų nuotraukas, kuriamas ar naudojamas pirmiausia seksualiniams tikslams.

Žr. [Liuksemburgo gaires](#) dėl tokių terminų kaip „kompiuteriniu ar skaitmeniniu būdu sukurta vaikų seksualinio išnaudojimo medžiaga“.

³⁸ Žr. Jungtinių Tautų vaiko teisių konvenciją.

³⁹ UNICEF ir ITU, „Guidelines for Industry on Child Online Protection“, 2014.

⁴⁰ Jungtinių Tautų vaiko teisių konvencijos 34 straipsnis.

⁴¹ Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Liuksemburgo gairės), 2016.

⁴² Liuksemburgo gairės (kaip nurodyta pirmiau), 2016 m. Ir UNICEF Global Kids Online report, 2019.

⁴³ Broadband Commission for Sustainable Development, „Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online“, 2019; WePROTECT Global Alliance, „Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response“, 2016.

Vaikai ir jaunimas

Apibūdina visus asmenis, jaunesnius nei 18 metų, kuomet „vaikai“ (šiose ITU gairėse dar vadinami „jaunesniais vaikais“) apima visus asmenis, jaunesnius nei 15 metų, o „jaunimą“ sudaro 15–18 metų asmenys.

Išmanieji žaislai

Išmanieji žaislai prijungiami prie interneto naudojant tokias technologijas kaip „Wi-Fi“ ir „Bluetooth“ ryšys, ir paprastai veikia kartu su papildomomis programomis, kad vaikai galėtų žaisti interaktyviai. „Juniper Research“ duomenimis, 2015 m. išmaniųjų žaislų rinka pasiekė 2,8 mlrd. USD ir prognozuojama, kad iki 2020 m. ji padidės iki 11 mlrd. USD. Šie žaislai renka ir saugo asmeninę vaikų informaciją, įskaitant vardus, geografinę vietą, adresus, nuotraukas, garso ir vaizdo įrašus.⁴⁴

Elektroninės patyčios

Elektroninėmis patyčiomis apibūdinamas tyčinis agresyvus elgesys, kurį pakartotinai atlieka grupė arba individualūs asmenys, naudodamiesi skaitmeninėmis technologijomis, ir yra nukreiptas į auką, kuri negali apsiginti.⁴⁵ Paprastai tai apima „skaitmeninių technologijų ir interneto naudojimą skleisti aukoms žalingą informaciją, tyčia dalytis privačia informacija, nuotraukomis ar vaizdo įrašais, siųsti grėsmingus ar įžeidžiančius pranešimus (el. paštu, tiesioginiais pranešimais, pokalbiais ar žinutėmis), skleisti gandus ir melagingą informaciją apie auką arba pašalinti ją iš bendravimo internete“.⁴⁶

Kibernetinė neapykanta, diskriminacija ir smurtinis ekstremizmas

„Kibernetinė neapykanta, diskriminacija ir smurtinis ekstremizmas yra aiški kibernetinio smurto forma, nes jie nukreipti į kolektyvinę tapatybę, o ne į individualius asmenis, ir dažnai yra susiję su rase, seksualine orientacija, religija, tautybe ar imigracijos statusu, lytimi ir politika“.⁴⁷

Skaitmeninis pilietiškumas

Skaitmeninis pilietiškumas reiškia gebėjimą pozityviai, kritiškai ir kompetentingai įsitraukti į skaitmeninę aplinką, pasitelkiant efektyvius bendravimo ir kūrybos įgūdžius, praktikuoti dalyvavimo socialiniame gyvenime formas, gerbiančias žmogaus teises ir orumą.⁴⁸

⁴⁴ Jeremy Greenberg, „Dangerous Games: Connected Toys, COPPA, and Bad Security“, Džordžtauno teisės technologijų apžvalga, 2017.

⁴⁵ Anna Costanza Baldry ir kt. „Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities“, Vaikų ir jaunimo paslaugų apžvalga, 2019.

⁴⁶ 2016 m. Liuksemburgo gairės ir 2019 m. UNICEF „Global Kids Online“ ataskaita (kaip nurodyta aukščiau).

⁴⁷ 2019 m. UNICEF [Global Kids Online ataskaita](#) (kaip nurodyta aukščiau).

⁴⁸ Europos Taryba, „Digital Citizenship and Digital Citizenship Education“.

Skaitmeninis raštingumas

Skaitmeninis raštingumas reiškia įgūdžių, reikalingų žmogui gyventi, mokytis ir dirbti visuomenėje, kurioje vis dažniau bendraujama ir prieinama prie informacijos per skaitmenines technologijas, tokias kaip interneto platformos, socialiniai tinklai ir mobilieji įrenginiai, turėjimą.⁴⁹ Tai apima aiškų bendravimą, techninius įgūdžius ir kritinį mąstymą.

Skaitmeninis atsparumas

Šis terminas apibūdina vaiko gebėjimą emociškai susitvarkyti su internete patirta žala. Tai taip pat reiškia emocinį intelektą, kurio reikia norint suprasti, kada vaikui kyla pavojus internete, mokėjimą ieškoti pagalbos, mokymąsi iš patirties ir gebėjimą susitvarkyti su negandomis.⁵⁰

Vadovai

Apibūdina visus asmenis, užimančius pareigas mokyklos valdymo struktūroje.

Viliojimas / viliojimas internete

Viliojimas / viliojimas internete, kaip apibrėžta Liuksemburgo gairėse, nurodo „santykių su vaiku užmezgimo procesą naudojantis internetu ar kitomis skaitmeninėmis technologijomis, siekiant seksualinio ryšio internete ar gyvai“. Tai yra nusikalstama veikla, kuomet bandoma susidraugauti su vaiku ..., siekiant priversti jį atlikti seksualinius veiksmus.

Informacinės ir ryšių technologijos

Informacinės ir ryšių technologijos (IRT) apibūdina visas informacines technologijas, kurios pabrėžia komunikacijos aspektą. Tai apima visas prisijungimo prie interneto paslaugas ir įrenginius, tokius kaip kompiuteriai, nešiojamieji kompiuteriai, planšetiniai kompiuteriai, išmanieji telefonai, žaidimų konsolės ir išmanieji laikrodžiai.⁵¹ Tai taip pat apima tokias paslaugas kaip radijas ir televizija, taip pat plačiajuostį ryšį, tinklo technines ir palydovines sistemas.

Žaidimai internete

Internetiniai žaidimai apibrėžiami kaip bet kokio tipo vienam ar keliems žaidėjams skirti skaitmeniniai žaidimai per bet kokį prie interneto prijungtą įrenginį, įskaitant specialias konsoles, stalinius kompiuterius, nešiojamus kompiuterius, planšetinius kompiuterius ir mobiliuosius telefonus. Apibrėžta „internetinių žaidimų ekosistema“ apima žiūrėjimą, kaip kiti žaidžia vaizdo žaidimus per el. sporto, tiesioginės transliacijos ar vaizdo dalijimosi platformas, kurios paprastai suteikia žiūrovams galimybę komentuoti ir bendrauti su kitais auditorijos nariais.⁵²

⁴⁹ Vakarų Sidnėjaus universitetas, „What is digital literacy?“.

⁵⁰ Dr. Andrew K. Przybylski ir kt., „A Shared Responsibility: Building children’s online resilience“, Virgin Media and Parent Zone, 2014.

⁵¹ UNICEF ir ITU, „Guidelines for Industry on Child Online Protection“, 2014 (kaip nurodyta aukščiau).

⁵² UNICEF, „Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry“, 2019.

Tėvų kontrolės priemonės

Programinė įranga, leidžianti vartotojams, paprastai tėvams, valdyti kai kurias arba visas kompiuterio ar kito įrenginio, galinčio prisijungti prie interneto, funkcijas. Paprastai tokios programos gali apriboti prieigą prie tam tikro tipo svetainių ar internetinių paslaugų. Kai kurios priemonės taip pat leidžia valdyti įrenginių naudojimo trukmę, t.y. galima nustatyti, kad įrenginys turėtų prieigą prie interneto tik tam tikromis valandomis. Pažangesnėse versijose galima įrašyti visas išsiųstas ar gautas žinutes. Paprastai programos bus apsaugotos slaptažodžiu.⁵³

Asmeninė informacija

Šis terminas apibūdina internete renkama individualiai identifikuojamą informaciją apie asmenį. Tai apima vardą ir pavardę, kontaktinius duomenis, pvz., namų ir el. pašto adresus, telefonų numerius, pirštų atspaudus ar veido atpažinimo medžiagą, draudimo numerius ar bet kokią kitą informaciją, leidžiančią fiziškai ar internetu susisiekti su asmeniu arba jį surasti. Šiame kontekste ji taip pat nurodo bet kokią informaciją apie vaiką ir jo aplinką, kurią internete renka paslaugų teikėjai, įskaitant išmaniuosius žaislus ir daiktų internetą, ir bet kurią kitą susijusią technologiją.

Privatumas

Privatumas dažnai vertinamas pagal dalijimąsi asmenine informacija internete, viešas socialinių tinklų paskyras, dalijimąsi informacija su internete sutiktais žmonėmis, privatumo nustatymų naudojimą, slaptažodžių dalijimąsi su draugais ir susirūpinimą dėl privatumo.⁵⁴

Viešojo žiniasklaida

Tai nacionaliniai transliuotojai, gavę licenciją pagal sutartinius įsipareigojimus su valstybe ar parlamentu. Pastaraisiais metais daugelyje šalių šie įsipareigojimai buvo išplėsti siekiant kovoti su skaitmeninės pertvarkos padariniais naudojantis žiniasklaidos ir skaitmeninio raštingumo programomis ir įsipareigojimais spręsti skaitmeninę atskirtį.

Sekstingas (angl. Sexting)

Sekstingas paprastai apibrėžiamas kaip pačių sukurto seksualizuoto turinio, įskaitant vaizdus, pranešimus ar vaizdo įrašus, siuntimas, gavimas ar keitimasis jais per mobiliuosius telefonus ir (arba) internetą.⁵⁵ Daugelyje šalių vaikų seksualinių vaizdų kūrimas, platinimas ir laikymas yra neteisėtas. Jei dalijamasi pačių vaikų sukurtais seksualiniais vaizdais, suaugusieji neturėtų jų žiūrėti. Suaugusio asmens dalijimasis seksualiniais vaizdais su vaiku visada yra nusikalstama veika, kuri gali būti žalinga, todėl gali tekti pranešti apie tokius vaizdus ir juos pašalinti.

⁵³ UNICEF and ITU, "Guidelines for Industry on Child Online Protection", 2014 (kaip nurodyta aukščiau).

⁵⁴ JAV Federalinė prekybos komisija, "Children's Online Privacy Protection Act", 1998.

⁵⁵ 2016 m. Liuksemburgo gairės, (kaip nurodyta aukščiau).

Sekstortas (angl. sextortion) arba seksualinis turto iš vaikų prievartavimas

Sekstortas yra „asmens šantažavimas pasitelkiant jo paties sukurtus atvaizdus, siekiant seksualinių veiksmų, pinigų ar kitokios naudos, grasinant pasidalinti medžiaga be vaizduose esančio asmens sutikimo (pvz., vaizdų skelbimas socialiniuose tinkluose)“.⁵⁶

Daiktų internetas

„Daiktų internetas yra kitas žingsnis link mūsų visuomenės ir ekonomikos skaitmeninimo, kai objektai ir žmonės yra susieti tinklais ir praneša apie savo būklę ir (arba) supančią aplinką“.⁵⁷

URL

Ši santrumpa reiškia „universalus adresas“, t.y. interneto puslapio adresas.⁵⁸

Virtuali realybė

„Virtuali realybė yra kompiuterinių technologijų naudojimas siekiant sukurti interaktyvų erdvinį pasaulį, kuriame objektai daro erdvės poveikį“.⁵⁹

Wi-Fi

„Wi-Fi“ („Wireless Fidelity“) yra techninių standartų grupė, leidžianti perduoti duomenis belaidžiais tinklais.⁶⁰

⁵⁶ 2016 m. Liuksemburgo gairės, (kaip nurodyta aukščiau).

⁵⁷ Europos Komisija, „[Policy: The Internet of Things](#)“.

⁵⁸ UNICEF ir ITU, „[Guidelines for Industry on Child Online Protection](#)“, 2014 (kaip nurodyta aukščiau).

⁵⁹ NASA, „[Virtual Reality: Definition and Requirements](#)“.

⁶⁰ JAV Federalinė prekybos komisija, „[Children’s Online Privacy Protection Act](#)“, 1998.