Smjernice za IKT kompanije u pogledu bezbjednosti djece na internetu 2020.

Smjernice za IKT kompanije u pogledu bezbjednosti djece na internetu

Priznanja

Ove smjernice su razvile Međunarodna unija za telekomunikacije (ITU) i radna grupa autora koji su dali doprinos, a dolaze iz vodećih institucija aktivnih u sektoru informacionih i komunikacionih tehnologija (IKT), kao i na pitanjima zaštite djece, a uključuju EBU, Globalno partnerstvo za zaustavljanje nasilja nad djecom, GSMA, Međunarodna alijansa za osobe sa invaliditetom, The Internet Watch Foundation (IWF), Privately SA i UNICEF. Radnom grupom predsjedao je Anjan Bose (UNICEF), a koordinisala je Fanny Rotino (ITU).

Ove smjernice ITU-a ne bi bile moguće bez vremena, entuzijazma i predanosti autora koji su dali svoj doprinos. Neprocjenjive doprinose takođe su dali e-Worldwide Group (e-WWG), Facebook, Tencent Games, Twitter, kompanija Walt Disney, kao i druge interesne strane u IKT industriji, kojima je zajednički cilj učiniti internet boljim i bezbjednijim mjestom za djecu i mlade. ITU je zahvalan sljedećim partnerima koji su izdvojili svoje dragocjeno vrijeme i uvide (navedeni po abecednom redu organizacija):

- Giacomo Mazzone (EBU)
- Salma Abbasi (e-WWG)
- David Miles i Caroline Hurst (Facebook)
- Amy Crocker i Serena Tommasino (Globalno partnerstvo za zaustavljanje nasilja nad djecom)
- Jenny Jones (GSMA)
- Lucy Richardson (Međunarodna alijansa za osobe sa invaliditetom - IDA)
- 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 i Steven Edwin Vosloo (UNICEF)
- Amy E. Cunningham (Kompanija Walt Disney)

ISBN

978-92-61-30081-4 (Štampana verzija)

978-92-61-30411-9 (Elektronska verzija)

978-92-61-30071-5 (EPUB verzija)

978-92-61-30421-8 (Mobi verzija)

Molimo vas da uzmete u obzir prirodnu okolinu prije nego što odštampate ovaj izvještaj.

Predgovor

Eksplozija digitalnih tehnologija stvorila je bez presedana mogućnosti za djecu i mlade da komuniciraju, povezuju se, dijele, uče, pristupaju informacijama i izražavaju svoje mišljenje o pitanjima koja utiču na njihov život i njihove zajednice.

Ali širi i dostupniji pristup uslugama na internetu takođe predstavljaju značajne izazove za dječju bezbjednost i dobrobit - kako na internetu tako i izvan njega. Od pitanja privatnosti, vršnjačkog nasilja i nasilnog i/ili neprimjerenog sadržaja za određeni uzrast, do prevaranata na internetu i zločina nad djecom kao što su vrbovanje, seksualno zlostavljanje i iskorištavanje na internetu, današnja djeca suočena su sa mnogim rizicima. Prijetnje se umnožavaju, a počinitelji sve više istovremeno djeluju preko granica, što njihovo praćenje čini teškim, a još teže ih je procesuirati.

Uz to, globalna pandemija virusa COVID-19 zabilježila je porast broja djece koja su se prvi put pridružila svijetu na internetu, kako bi podržala svoje studije i održala socijalnu interakciju. Zbog ograničenja koja je nametnuo virus ne samo da su mnoga mlađa djeca započela interakciju na internetu mnogo ranije nego što su njihovi roditelji mogli planirati, već je potreba za usklađivanjem radnih obaveza mnogim roditeljima onemogućila nadzor nad njihovom djecom, stavljajući mlade ljude u rizik da pristupe neprimjerenom sadržaju ili da budu na meti kriminalaca u proizvodnji materijala seksualnog zlostavljanja djece (CSAM).

Kriminalci profitiraju od tehnološkog napretka, kao što su međusobno povezivanje aplikacija i igara, brzo dijeljenje datoteka, prenos uživo, kripto valute, Dark Web i snažni softveri za šifrovanje. Međutim, oni takođe profitiraju od često nekoordinisanog i neodlučnog djelovanja tehnološkog sektora u cilju efikasne borbe protiv problema.

Tehnologije u nastajanju mogu biti dio rješenja, na primjer Interpolova baza podataka o seksualnom zlostavljanju djece zasnovana na vještačkoj inteligenciji koja koristi softver za poređenje slika i video zapisa za brzo uspostavljanje veza između žrtava, nasilnika i mjesta. Ali sama tehnologija neće riješiti problem.

Kako bi se smanjili rizici digitalne revolucije i dala mogućnost sve većem broju mladih da iskoriste njene prednosti, zajednički i koordinisani odgovor više interesnih strana nikada nije bio bitniji. Vlade, civilno društvo, lokalne zajednice, međunarodne organizacije i interesne strane u IKT industriji moraju se okupiti radi zajedničkog cilja.

Prepoznavši to, 2018. godine države članice ITU zatražile su sveobuhvatno ažuriranje naših smjernica u pogledu bezbjednosti djece na internetu. Ove nove ITU smjernice su preispitane, ponovo napisane i preoblikovane kako bi odražavale vrlo značajne pomake u digitalnom krajoliku u kojem se djeca ove generacije nalaze. Pored toga što se bavi novim dostignućima u digitalnim tehnologijama i platformama, ovo novo izdanje bavi se i važnom prazninom: situacijom sa kojom se suočavaju djeca s invaliditetom, za koju svijet na internetu nudi posebno presudan spas za puno i ispunjeno društveno učestvovanje.

Tehnološka industrija ima presudnu i proaktivnu ulogu u uspostavljanju temelja za bezbjedniju i sigurniju upotrebu internetskih usluga i drugih tehnologija za današnju djecu i buduće generacije.

Preduzeće mora sve više stavljati dječje interese u središte svog rada, obraćajući posebnu pažnju na zaštitu privatnosti ličnih podataka mladih korisnika, čuvajući njihovo pravo na slobodu izražavanja, boreći se protiv rastuće pošasti materijala seksualnog zlostavljanja djece i osiguravajući da postoje sistemi koji efikasno rješavaju povrede dječjih prava kada se dogode.

Tamo gdje domaći zakoni još uvijek nisu sustigli međunarodno pravo, svako preduzeće ima priliku - i odgovornost - da svoje operativne okvire uskladi sa najvišim standardima i najboljom praksom.

Nadamo se da će ove smjernice IKT kompanijama poslužiti kao čvrsta osnova na kojoj će se razvijati poslovne politike i inovativna rješenja. U pravom duhu uloge ITU-a kao globalnog sazivača, ponosna sam na činjenicu da su ove smjernice proizvod zajedničkih globalnih napora i da su u njihovom pravljenju učestvovali stručnjaci iz široke međunarodne zajednice kao koautori.

Takođe mi je drago predstaviti našu novu maskotu zaštite djece na internetu Sango-a: prijateljski nastrojenog i neustrašivog lika kojeg je u potpunosti dizajnirala grupa djece kao dio ITU-ovog novog međunarodnog programa informisanja mladih.

U doba kada sve više mladih ljudi koristi internet, ITU smjernice za zaštitu djece su važnije nego ikad. IKT kompanije, vlade, roditelji i edukatori, kao i sama djeca, svi imaju vitalnu ulogu. Zahvalna sam, kao i uvijek, na vašoj podršci i radujem se nastavku naše bliske saradnje po ovom kritičnom pitanju.

Doreen Bogdan-Martin
Direktor
Biro za razvoj telekomunikacija, ITU

Sadržaj

Tabela

1. Pregled

Svrha ovog dokumenta je da pruži smjernice interesnim stranama IKT kompanija da izgrade vlastite resurse za zaštitu djece na internetu (COP). Cilj ovih smjernica za IKT kompanije u pogledu bezbjednosti djece na internetu je pružiti koristan, fleksibilan i jednostavan za korištenje okvir za vizije preduzeća i njihovu odgovornost da zaštite korisnike. One su takođe usmjerene na stvaranje temelja za bezbjedniju i sigurniju upotrebu internetskih usluga i srodnih tehnologija za današnju djecu i buduće generacije.

Kao alat, ove smjernice takođe imaju za cilj jačanje poslovnog uspjeha pomažući velikim i malim preduzećima i interesnim stranama da razviju i održavaju atraktivan i održiv poslovni model, uz razumijevanje pravne i moralne odgovornosti prema djeci i društvu.

Kao odgovor na značajan napredak u tehnologiji i spajanju, ITU, UNICEF i partneri za zaštitu djece na internetu razvili su i ažurirali smjernice za širok spektar kompanija koje razvijaju, pružaju ili koriste telekomunikacije ili srodne aktivnosti u isporuci svojih proizvoda i usluga.

Nove smjernice za IKT kompanije u pogledu bezbjednosti djece na internetu rezultat su konsultacija sa članovima Inicijative za zaštitu djece na internetu, kao i širih konsultacija sa članovima civilnog društva, privrede, akademske zajednice, vlada, medija, međunarodnih organizacija i mladih.

Svrha ovog dokumenta je da:

- uspostavi zajedničku referentnu tačku i smjernice za IK tehnologije i internetsku industriju i relevantne interesne strane;
- pruži smjernice kompanijama o identifikaciji, sprječavanju i ublažavanju bilo kakvih negativnih uticaja njihovih proizvoda i usluga na dječja prava;
- pruži smjernice kompanijama o utvrđivanju načina na koje mogu promovisati dječja prava i odgovorno digitalno građanstvo među djecom;
- predloži zajedničke principe koji čine osnovu nacionalnih ili regionalnih obaveza u svim srodnim industrijama, imajući na umu da će se različite vrste preduzeća koristiti različitim modelima implementacije.

Obim

Zaštita djece na internetu je složen izazov koji uključuje više različitih upravljačkih, političkih, operativnih, tehničkih i pravnih aspekata. Ove smjernice pokušavaju riješiti, organizovati i odrediti prioritete za mnoga od ovih područja, na osnovu postojećih i dobro poznatih modela, okvira i drugih referenci.

Smjernice se fokusiraju na zaštitu djece u svim područjima i od svih rizika digitalnog svijeta i, kao takve, ističu dobru praksu interesnih strana u IKT industriji koju kompanije mogu uzeti u obzir u procesu izrade, razvoja i upravljanja politikama zaštite djece na internetu. One navode aktere u IKT industriji ne samo o tome kako upravljati i obuzdati nezakonite aktivnosti na internetu protiv kojih su oni dužni djelovati (poput materijala seksualnog zlostavljanja djece na internetu) putem svojih usluga, već se takođe fokusiraju i na druga pitanja koja se ne mogu definisati kao krivična djela u svim nadležnostima. To uključuje nasilje među vršnjacima, sajber maltretiranje i uznemiravanje na internetu, kao i pitanja koja se odnose na privatnost ili opštu dobrobit, prevaru ili druge prijetnje, koje u određenom kontekstu mogu biti štetne za djecu.

U tu svrhu ove smjernice uključuju preporuke o dobroj praksi u otklanjanju rizika s kojima se djeca suočavaju u digitalnom svijetu i kako postupati u cilju uspostavljanja sigurnog okruženja za djecu na internetu. Ove smjernice daju savjete o tome kako IKT kompanije mogu raditi na osiguranju dječje bezbjednosti prilikom korištenja IK tehnologija, interneta ili bilo koje povezane tehnologije ili uređaja koji se na njega mogu povezati, uključujući mobilne telefone, konzole za igranje, igračke povezane s internetom, satove, internet stvari i sistemi vođeni vještačkom inteligencijom. Stoga pružaju pregled ključnih pitanja i izazova u vezi sa zaštitom djece na internetu i predlažu akcije za preduzeća i interesne strane za razvoj lokalnih i unutrašnjih politika zaštite djece na internetu. Ove smjernice ne pokrivaju aspekte kao što su stvarni proces razvoja ili tekst koji bi politike IKT kompanija u vezi sa zaštitom djece na internetu mogle obuhvatiti.

Struktura

Odjeljak 1 - Pregled: Ovaj odjeljak ističe svrhu, obim i ciljnu publiku ovih smjernica.

Odjeljak 2 - Uvod u zaštitu djece na internetu: Ovaj odjeljak daje pregled pitanja zaštite djece na internetu, navodeći neke osnovne informacije, uključujući posebnu situaciju djece sa invaliditetom. Štaviše, pruža primjere postojećih međunarodnih i nacionalnih modela za zaštitu djece na internetu kao moguće oblasti intervencije za interesne strane u IKT industriji.

Odjeljak 3 – Ključna područja zaštite i promocije dječjih prava: Ovaj odjeljak navodi pet ključnih područja u kojima kompanije mogu preduzeti mjere kako bi osigurale djeci bezbjednu i pozitivnu upotrebu IK tehnologija.

Odjeljak 4 – Opšte smjernice: Ovaj odjeljak daje preporuke svim interesnim stranama u IKT industriji u pogledu dječje bezbjednosti prilikom upotrebe IK tehnologija i promociji pozitivne upotrebe IK tehnologija, uključujući odgovorno digitalno građanstvo među djecom.

Odjeljak 5 - Kontrolna lista u vezi sa karakteristikama: Ovaj odjeljak ističe posebne preporuke za interesne strane o konkretnim akcijama za poštovanje i podršku dječjim pravima, sa sljedećim karakteristikama:

- Karakteristika A: Obezbijediti povezivanje, usluge skladištenja podataka i hostinga
- Karakteristika B: Ponuditi uređeni digitalni sadržaj
- Karakteristika C: Hostovati sadržaj koji generišu korisnici i povezani korisnici
- Karakteristika D: Sistemi vođeni vještačkom inteligencijom

Ciljana publika

Nadovezujući se na Vodeće principe Ujedinjenih nacija o poslovanju i ljudskim pravima,[1] Dečija prava i poslovni principi pozivaju preduzeća da ispune svoju odgovornost da poštuju dječija prava izbjegavanjem bilo kakvih negativnih uticaja povezanih sa njihovim poslovanjem, proizvodima ili uslugama. Ovi principi takođe artikulišu razliku između poštovanja (minimuma koji je potreban preduzeću da bi se izbjeglo nanošenje štete djeci) i podrške (na primjer, preduzimanjem dobrovoljnih akcija kojima se želi unaprijediti ostvarivanje dječjih prava). Preduzeća trebaju osigurati dječja prava kako na zaštitu na internetu, tako i na pristup informacijama i slobodu izražavanja, istovremeno promovišući pozitivnu upotrebu IK tehnologija od strane djece.

[1] Vodeći principi Ujedinjenih nacija o poslovanju i ljudskim pravima.

Tradicionalne razlike između različitih dijelova industrije telekomunikacija i mobilne telefonije, kao i internetskih kompanija i emitera, brzo se ruše i postaju nejasne. Spajanje uvlači ove prethodno različite digitalne tokove u jednu struju koja doseže milijarde ljudi u svim dijelovima svijeta. Saradnja i partnerstvo su osnove uspostavljanja temelja za sigurniju i bezbjedniju upotrebu interneta i povezanih tehnologija. Vlade, privatni sektor, kreatori politika, edukatori, civilno društvo, roditelji i staratelji imaju vitalnu ulogu u postizanju ovog cilja. IKT industrija može djelovati u pet ključnih područja, kako je opisano u odjeljku 3.

2. Šta je zaštita djece na internetu?

Tokom posljednjih 10 godina, upotreba i uloga interneta u životima ljudi znatno su se promijenili. Zahvaljujući rasprostranjenosti pametnih telefona i tableta, dostupnosti Wi-Fi i 4G tehnologije i razvoju platformi društvenih medija i aplikacija, sve više ljudi pristupa internetu iz sve većeg broja razloga.

U 2019. godini više od polovine svjetske populacije koristilo je internet. Najveći dio korisnika su ljudi mlađi od 44 godine, sa podjednakom upotrebom interneta između korisnika od 16 do 24 godine i od 35 do 44 godine. Na globalnom nivou, svaki treći korisnik interneta je dijete (0-18 godina), a UNICEF procjenjuje da je 71% mladih već na internetu.[2] Širenje pristupnih tačaka internetu, mobilne tehnologije i sve većeg spektra uređaja sa mogućnošću pristupa internetu, u kombinaciji sa ogromnim resursima koji se mogu naći u sajber prostoru, pružaju neviđene mogućnosti za učenje, dijeljenje i komunikaciju.

Prednosti upotrebe IK tehnologija uključuju širi pristup informacijama o socijalnim uslugama, obrazovnim resursima i zdravstvenim savjetima. Dok djeca i mladi i porodice koriste internet i mobilne telefone da traže informacije i pomoć i prijavljuju slučajeve zlostavljanja, ove tehnologije mogu pomoći u zaštiti djece i mladih od nasilja i iskorištavanja. Provajderi usluga dječje zaštite takođe koriste IK tehnologije za prikupljanje i prenos podataka, što olakšava registraciju rođenja, vođenje slučajeva, traženje porodice, prikupljanje podataka i mapiranje nasilja, između ostalog.

Štaviše, internet je povećao pristup informacijama u svim krajevima svijeta, omogućavajući djeci i mladima da istražuju gotovo bilo koju temu od interesa, pristupe svjetskim medijima, istražuju poslovne mogućnosti i prikupljaju ideje za budućnost. Upotreba IK tehnologija omogućava djeci i mladima da ostvare svoja prava i izraze svoja mišljenja, a takođe im omogućava da se povežu i komuniciraju sa svojim porodicama i prijateljima. IK tehnologije takođe služe kao najvažniji način kulturne razmjene i izvor zabave.

Uprkos dubokim prednostima interneta, djeca i mladi se takođe mogu suočiti s nizom rizika kada koriste IK tehnologije. Mogu biti izloženi neprikladnom sadržaju ili neprikladnom kontaktu, uključujući potencijalne počinitelje seksualnog zlostavljanja. Oni mogu pretrpiti reputacijsku štetu zbog objavljivanja osjetljivih ličnih podataka ili na internetu ili putem "sekstinga", često ne uspijevajući shvatiti implikacije svojih postupaka na sebe i

[2] OECD, "Nove tehnologije i djeca 21. vijeka: Najnoviji trendovi i ishodi", Obrazovni radni dokument br. 179.

druge i njihove dugoročne „digitalne otiske“. Takođe se suočavaju sa rizicima povezanim s privatnošću na internetu koji proizlaze iz prikupljanja podataka, prikupljanja i korištenja informacija o lokaciji.

Konvencija o pravima djeteta, koja je najratifikovaniji međunarodni ugovor o ljudskim pravima,[3] utvrđuje građanska, politička, ekonomska, socijalna i kulturna prava djece. Njime se utvrđuje da sva djeca i mladi imaju pravo na obrazovanje; razonodu, igru i kulturu; odgovarajuće informacije; slobodu misli i izražavanja; i privatnost, kao i da izraze svoje stavove o pitanjima koja utiču na njih u skladu sa njihovim razvojnim kapacitetima. Konvencija takođe štiti djecu i mlade od svih oblika nasilja, iskorištavanja, zlostavljanja i diskriminacije bilo koje vrste, i utvrđuje da bi najbolji interes djeteta trebao biti primarna briga u svim pitanjima koja utiču na njih. Roditelji, staratelji, edukatori i članovi zajednice, uključujući vođe zajednice i aktere civilnog društva, imaju odgovornost da njeguju i podržavaju djecu i mlade u njihovom prelasku u odraslo doba. Vlade imaju važnu ulogu u osiguravanju da sve takve interesne strane ispune tu ulogu.

Što se tiče zaštite dječijih prava na internetu, IKT kompanije moraju zajedno raditi na postizanju pažljive ravnoteže između prava djece na zaštitu i prava na pristup informacijama i slobode izražavanja. Kompanije bi zato trebale dati prioritet mjerama za zaštitu djece i mladih na internetu koje su ciljane i koje nisu pretjerano restriktivne, ni za dijete ni za druge korisnike. Štaviše, sve je veći konsenzus da bi promocija digitalnog građanstva među djecom i mladima, i razvoj proizvoda i platformi koji olakšavaju djeci pozitivnu upotrebu IK tehnologija, trebalo da bude prioritet privatnog sektora.

Iako internetske tehnologije djeci i mladima nude brojne mogućnosti za komunikaciju, učenje novih vještina, kreativnost i doprinos za poboljšanje društva za sve, one takođe mogu predstavljati nove rizike za bezbjednost djece i mladih. Mogu izložiti djecu i mlade potencijalnim rizicima i štetama u vezi sa pitanjima privatnosti, nezakonitog sadržaja, uznemiravanja, sajber maltretiranja, zloupotrebe ličnih podataka ili vrbovanja u seksualne svrhe, pa čak i seksualnog zlostavljanja i iskorištavanja djece. Mogu biti izloženi i reputacijskoj šteti, uključujući „osvetničku pornografiju“ povezanu s objavljivanjem osjetljivih ličnih podataka ili na internetu ili putem „sekstinga“, što je način na koji korisnici šalju seksualno eksplicitne poruke, fotografije ili slike između mobilnih telefona. Oni se takođe suočavaju sa rizicima vezanim za privatnost na internetu kada koriste internet. Djeca, po prirodi svojih godina i zrelosti, često nisu u stanju u potpunosti shvatiti rizike povezane sa internetskim svijetom i moguće negativne posljedice za druge i sebe zbog svog neprimjerenog ponašanja.

Uprkos prednostima, postoje i nedostaci u upotrebi novih i naprednijih tehnologija. Razvoj vještačke inteligencije i mašinskog učenja, virtuelne i proširene stvarnosti, velikih podataka, robotike i interneta stvari ima za cilj da još više transformiše medijsku praksu djece i mladih. Iako se ove tehnologije pretežno razvijaju kako bi proširile obim pružanja usluga i poboljšale pogodnost (putem, na primjer, glasovne pomoći, pristupačnosti i novih oblika digitalnog uranjanja), neke takve tehnologije mogu imati nenamjerne posljedice, pa čak i da ih zlostavljači djece koriste da služe njihovim potrebama. Stvaranje sigurnog i bezbjednog internetskog okruženja za djecu i omladinu zahtijeva djelotvorno učestvovanje vlada, privatnog sektora i svih interesnih strana. Fokusiranje na digitalne vještine i pismenost roditelja i edukatora takođe mora biti jedan od prvih ciljeva, u čijem postizanju IKT kompanije mogu da imaju vitalnu i održivu ulogu.

[3] Konvencija o pravima djeteta UN-a. Sve zemlje osim tri (Somalija, Južni Sudan i Sjedinjene Američke Države) ratifikovale su Konvenciju o pravima djeteta.

Neka djeca možda dobro razumiju rizike na internetu i kako na njih odgovoriti. Međutim, to se ne može reći za svu djecu svuda, posebno među ranjivim grupama. Prema cilju 16.2 Ciljeva održivog razvoja Ujedinjenih nacija, čiji je cilj zaustaviti zlostavljanje, eksploataciju, trgovinu ljudima i sve oblike nasilja i mučenja nad djecom, zaštita djece na internetu je od vitalnog značaja.

Od 2009. godine, Inicijativa zaštite djece na internetu, međunarodna akcija sa više interesnih strana koju je pokrenuo ITU, ima je za cilj podizanje svesti o riziku za decu na internetu i da odgovori na te rizike. Inicijativa okuplja partnere iz svih sektora globalne zajednice kako bi djeci svuda osigurali sigurno i bezbjedno internetsko iskustvo. Kao dio Inicijative, ITU je 2009. godine objavio set smjernica za zaštitu djece na internetu za četiri grupe: djecu, roditelje, staratelje i edukatore, IKT kompanije i kreatore politika. Zaštita djece na internetu podrazumjeva se u ovim smjernicama kao sveobuhvatan pristup da se odgovori na sve potencijalne prijetnje i štete sa kojima se djeca i mladi mogu suočiti bilo na internetu ili na nekoj od internetskih tehnologija. U ovom dokumentu zaštita djece na internetu takođe uključuje štetu nanijetu djeci koja se dogodi izvan interneta, ali je povezana sa dokazima o nasilju i zlostavljanju na internetu. Pored razmatranja dječjeg ponašanja i aktivnosti djece na internetu, zaštita djece na internetu takođe se odnosi na zloupotrebu tehnologije od strane osoba koje nisu djeca radi iskorištavanja djece.

Sve relevantne interesne strane imaju ulogu u pomaganju djeci i mladima da imaju koristi od mogućnosti koje internet pruža, dok stiču digitalnu pismenost i otpornost u pogledu njihove dobrobiti i zaštite na internetu.

Zaštita djece i mladih zajednička je odgovornost svih interesnih strana. Da bi se to dogodilo, kreatori politika, IKT kompanije, roditelji, staratelji, edukatori i druge interesne strane, moraju osigurati da djeca i mladi mogu ostvariti svoj potencijal - na internetu i izvan njega.

Iako ne postoji univerzalna definicija, zaštita djece na internetu ima za cilj cjelovit pristup izgradnji bezbjednih, prikladnih za sve uzraste, inkluzivnih i participativnih digitalnih prostora za djecu i mlade, koje karakterišu:

- reagovanje, podrška i samopomoć u slučaju suočavanja sa prijetnjama;
- sprječavanje šteta;
- dinamičan balans između osiguranja zaštite i pružanja mogućnosti djeci da budu digitalni građani;
- podržavanje prava i odgovornosti i djece i društva.

Štaviše, zbog brzog napretka u tehnologiji i društvu i bezgranične prirode interneta, zaštita djece na internetu mora biti agilna i prilagodljiva da bi bila efikasna. Razvojem tehnoloških inovacija pojaviće se novi izazovi koji će se razlikovati od regije do regije. Najbolje će se izaći na kraj sa njima zajedničkim radom u vidu globalne zajednice, jer treba pronaći nova rješenja za te izazove.

2.1 Osnovne informacije

Pošto je internet u potpunosti integrisan u živote djece i mladih, nemoguće je posmatrati odvojeno digitalni i fizički svijet.

Takva povezanost izuzetno osnažuje. Svijet interneta omogućava djeci i mladima da prebrode nedostatke i invaliditet, a pružio je nova mjesta za

zabavu, obrazovanje, učestvovanje i izgradnju odnosa. Današnje digitalne platforme se koriste za razne aktivnosti i često su multimedijalna iskustva.

Pristup i učenje korištenja i navigacije ovom tehnologijom smatra se presudnim za razvoj mladih ljudi i IK tehnologije se prvi put koriste u ranom uzrastu. Zato je presudno da svi akteri budu svjesni da djeca i mladi ljudi često počinju koristiti platforme i usluge prije nego što dostignu definisanu minimalnu starosnu granicu koje se tehnološka industrija mora pridržavati, pa bi zato obrazovanje uz mjere zaštite trebalo integrisati u sve internetske usluge koje koriste djeca.

2.1.1 Djeca u digitalnom svijetu

Pristup internetu

U 2019. godini više od polovine svjetske populacije koristilo je internet (53.6 posto), sa procijenjenih 4.1 milijardu korisnika. Na globalnom nivou, svaki treći korisnik interneta je dijete mlađe od 18 godina[1]. Prema UNICEF-u, širom svijeta 71% mladih već je na internetu[2]. Uprkos zahtjevima minimalne starosne granice, Ofcom (Regulator za komunikacije Velike Britanije) procjenjuje da gotovo 50% djece između 10 i 12 godina već ima profil na društvenim mrežama.[3] Djeca i mladi ljudi sada su značajno, trajno i dosljedno prisutni na internetu. Internet služi u druge društvene, ekonomske ili političke svrhe i postao je porodični ili potrošački proizvod ili usluga koja je sastavni dio načina na koji porodice, djeca i mladi žive svoj život.

U 2017. godini, na regionalnom nivou, pristup internetu za djecu i mlade bio je čvrsto povezan sa nivoom nacionalnog dohotka. Zemlje sa niskim prihodima imaju tendenciju da imaju manje djece korisnika interneta od zemalja sa visokim prihodima. Djeca i mladi u većini zemalja vikendom provode više vremena na internetu nego radnim danom, a adolescenti od 15 do 17 godina provode najviše vremena na internetu, u prosjeku između 2.5 i 5.3 sati, u zavisnosti od zemlje.

---

1 Livingstone, S., Carr, J., i Byrne, J. (2015) Svako treće: *Zadatak za globalno upravljanje internetom u rješavanju dječjih prava.* Globalna komisija za upravljanje internetom: Paper Series. London: CIGI i Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

2 Komisija za širokopojasni pristup, „Bezbjednost djece na internetu: Smanjenje rizika od nasilja, zlostavljanja i iskorištavanja na internetu (2019)," *Komisija za širokopojasni pristup za održivi razvoj,* oktobar 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

3 BBC, "Upotreba socijalnih medija od strane maloljetnika 'raste', kaže Ofcom".

Upotreba interneta

Među djecom i mladima najpopularniji uređaj za pristup internetu je mobilni telefon, a slijede ga stoni računari i laptopi. Djeca i mladi provode u prosjeku dva sata dnevno na internetu u toku sedmice i četiri sata svakog dana vikenda. Dok se neki osjećaju trajno povezanima, mnogi drugi još uvijek nemaju pristup internetu kod kuće. U praksi većina djece i mladih koji koriste internet imaju pristup preko više uređaja, a oni koji se barem jednom nedeljno povezuju ponekad koriste i do tri različita uređaja. Starija djeca i djeca u bogatijim zemljama uglavnom koriste više uređaja, a dječaci koriste nešto više uređaja nego djevojčice u svim anketiranim zemljama.

Najpopularnija aktivnost - i za djevojčice i za dječake je gledanje video isječaka. Više od tri četvrtine djece i mladih koji koriste internet kažu da video isječke gledaju na internetu barem jednom sedmično, bilo sami ili s drugim članovima svoje porodice. Mnoga djeca i mladi ljudi mogu se smatrati "aktivnim socijalizatorima" koristeći nekoliko platformi društvenih medija kao što su Facebook, Twitter, TikTok ili Instagram. Djeca i mladi se takođe bave politikom putem interneta i njihov glas se čuje putem blogova.

Ukupni nivo učešća u igranju na internetu razlikuje se od zemlje do zemlje i približno je u skladu sa lakoćom pristupa internetu za djecu i mlade. Međutim, dostupnost i pristupačnost igara na internetu brzo se mijenjaju, a starosna granica djece i mladih koji prvi put pristupaju igrama na internetu se smanjuje.

Nedeljno se 10%-30% djece i mladih koji se koriste internetom - koja su konsultovana u odabranom nizu zemalja - bavi kreativnim aktivnostima na internetu.[1] U obrazovne svrhe, mnoga djeca i mladi svih uzrasta koriste internet za izradu domaćih zadataka, ili čak da nadoknade gradivo nakon propuštenih predavanja ili potraže zdravstvene informacije na internetu svake sedmice. Čini se da starija djeca imaju veći apetit za informacijama od mlađe djece.

[1] Livingstone, S., Kardefelt Winther, D., i Hussein, M. (2019.). Global Kids Online uporedni izvještaj, izvještaj o istraživanju Innocenti. UNICEF-ova kancelarija za istraživanje - Innocenti, Firenca, https://www .unicef-irc.org/publications/1059-global-kids-online-comparative-report.html.

Seksualno iskorištavanje i zlostavljanje djece na internetu

Seksualno iskorištavanje i zlostavljanje djece (CSEA) na internetu raste zapanjujućom brzinom. Prije deset godina bilo je manje od milion dosijea materijala o zlostavljanju djece. U 2019. taj broj se popeo na 70 miliona, što je skoro 50% više u odnosu na brojke iz 2018. godine. Pored toga, po prvi put su video zapisi zlostavljanja premašili broj fotografija u prijavama nadležnim organima, što pokazuje potrebu za novim alatima za suočavanje sa ovim trendom. Žrtve seksualnog iskorištavanja i zlostavljanja djece na internetu pripadaju svim starosnim grupama, ali postaju sve mlađe. 2018. godine mreža linija za podršku INHOPE zabilježila je promjenu profila žrtava sa pubertetskih na predpubertetske. Pored toga, istraživanje ECPAT International-a i INTERPOL-a u 2018. godini pokazalo je da su mlađa djeca bila podložnija da budu podvrgnuta teškom zlostavljanju, uključujući mučenje, nasilno silovanje ili sadizam. To uključuje novorođenčad koja su stara samo nekoliko dana, sedmica ili mjeseci. Iako su djevojčice pogođenije, zlostavljanje dječaka može biti teže. Isti izvještaj pokazuje da su 80% žrtava o kojima se govori u izvještajima bile djevojčice, a 17% dječaci. Djeca oba pola navedena su u 3% procijenjenih izvještaja.[1]

Snimak podataka[2]

- Svaki treći korisnik interneta širom svijeta je dijete.
- Svake pola sekunde jedno dijete prvi put ide na internet.
- 800 miliona djece koristi društvene medije.
- Procjenjuje se da u jednom trenutku 750.000 pojedinaca na internetu želi da se poveže sa djecom u seksualne svrhe.
- U spremištu EUROPOL-a nalazi se više od 46 miliona jedinstvenih slika ili videozapisa materijala seksualnog zlostavljanja djece.
- Preko 89% žrtava je uzrasta između 3 i 13 godina.

Za više informacija o obimu i reakcijama na seksualno iskorištavanje i zlostavljanje djece na internetu pogledajte Globalni savez WeProtect.

1 ECPAT i Interpol, “U susret globalnom pokazatelju o neidentifikovanim žrtvama u materijalu seksualnog iskorištavanja djece: sažeti izvještaj”, 2018.
2 Zaustavljanje nasilja nad djecom, “Bezbjedni na internetu”.

2.1.2 Uticaj različitih platformi na dječje digitalno iskustvo

Internet i digitalna tehnologija djeci i mladima predstavljaju i mogućnosti i rizike. Neki od njih navedeni su u nastavku.

Kada djeca koriste **društvene medije**, imaju koristi od mnogih prilika za istraživanje, učenje, komunikaciju i razvijanje ključnih vještina. Djeca društvene mreže vide kao platforme koje im omogućavaju da istražuju svoje lične identitete u bezbjednom okruženju. Imati odgovarajuće vještine i znati kako riješiti pitanja vezana za privatnost i reputaciju važno je za mlade ljude.

"Znam da sve što objavite na internetu ostaje tu zauvijek i da to može uticati na vaš život u budućnosti", dječak koji ima 14 godina, Čile.

Međutim, s obzirom na to da istraživanja pokazuju da većina djece koristi društvene medije prije navršenih trinaest godina, a usluge provjere godišta su uglavnom slabe ili ih nema, rizici sa kojima se djeca mogu susresti mogu biti veoma veliki. Dalje, dok djeca žele naučiti digitalne vještine, da postanu digitalni građani i da kontrolišu postavke privatnosti, oni obično razmišljaju o privatnosti u odnosu na svoje prijatelje i poznanike - „Šta mogu vidjeti moji prijatelji?“ - a manje u odnosu na strance i treće strane. Ovo, u kombinaciji sa dječijom prirodnom znatiželjom i uopšteno sa nižim pragom straha od rizika, može ih učiniti ranjivima na vrbovanje, iskorištavanje, maltretiranje ili druge vrste štetnog sadržaja ili kontakata.

Raširena popularnost razmjene slika i video zapisa putem mobilnih aplikacija, a posebno korištenje platformi za strimovanje uživo od strane djece predstavlja daljnju zabrinutost u vezi sa privatnošću i rizikom. Neka djeca stvaraju seksualne slike sebe, prijatelja, braće i sestara i dijele ih na internetu. U 2019. godini gotovo trećina (29%) svih internet stranica s natpisom IWF sadržavale su samostalno generisane slike. Od toga je 76% pokazivalo djevojke uzrasta od 11 do 13 godina, većinom u svojim spavaćim sobama ili drugim sobama u kućnom okruženju. Za neku, posebno stariju djecu, to se može smatrati prirodnim istraživanjem seksualnosti i seksualnog identiteta, dok za drugu, posebno mlađu djecu, često postoji prisila odrasle osobe ili drugog djeteta. Bez obzira na slučaj, rezultujući sadržaj je u mnogim zemljama nezakonit i može izložiti djecu riziku od krivičnog gonjenja ili se može koristiti za daljnje iskorištavanje djeteta, vrbovanje ili iznuđivanje.

Slično tome, **igre na internetu** omogućavaju djeci da ispune svoje osnovno pravo na igru, kao i da grade mreže, provode vrijeme sa prijateljima i upoznaju nove prijatelje i razvijaju važne vještine. Iako ovo može biti veoma pozitivno, u nekim slučajevima, i ako nema nadzora i podrške odgovorne odrasle osobe, platforme za igre takođe mogu predstavljati rizik za djecu. To uključuje pretjerano igranje, finansijske rizike povezane sa prekomjernim kupovinama u igri, prikupljanje i unovčavanje ličnih podataka djece od strane aktera iz IKT industrije, sajber zlostavljanje, govor mržnje, nasilje i izlaganje neprimjerenom ponašanju ili sadržaju, vrbovanje korištenjem stvarnih, kompjuterski generisanih ili čak slika iz virtuelne realnosti i video zapisa koji prikazuju i normalizuju seksualno iskorištavanje i zlostavljanje djece. Ovi rizici nisu jedinstveni za okruženje za igranje, već se primjenjuju na druga digitalna okruženja u kojima djeca provode vrijeme.

Nadalje, tehnološki razvoj doveo je do pojave "interneta stvari", gdje je sve veći broj i obim uređaja sa mogućnosti da se povežu, komuniciraju i umrežavaju putem interneta. To uključuje igračke, monitore za bebe i uređaje koje pokreće vještačka inteligencija koji mogu predstavljati rizike u pogledu privatnosti i neželjenog kontakta.

Dobre prakse: Istraživanje

U kontekstu internetskog ili sajber maltretiranja, Microsoft je sproveo istraživanje digitalne bezbjednosti i sajber maltretiranja. 2012. godine anketirao je djecu od 8 do 17 godina u 25 zemalja o negativnom ponašanju na internetu. Rezultati su pokazali da je u prosjeku 54% učesnika navelo da se brinu da će biti maltretirani na internetu, 37% je izjavilo da su doživjeli sajber maltretiranje, a 24% je otkrilo da su nekoga maltretirali. Isto istraživanje je pokazalo da je manje od troje od deset roditelja razgovaralo sa djecom o nasilju na internetu. Od 2016. Microsoft sprovodi **redovno istraživanje** rizika na internetu dajući godišnje Izvještaje o indeksu digitalne učtivosti.

FACES je multimedijalni program koji su proizveli NHK Japan i konzorcijum različitih javnih servisa sa pričama o žrtvama nasilja na internetu i izvan njega širom svijeta. Serija se sastoji od portreta adolescenata u kojima protagonisti pred kamerama objašnjavaju kako su reagovali na napade putem interneta. Seriju, koja je takođe proizvedena u dvominutnim klipovima, prihvatili su Facebook, UNESCO, i Savjet Evrope, i dostupna je na mnogim jezicima.

U 2019. godini, UNICEF je objavio diskusioni dokument o Pravima djeteta i igranje na internetu: Prilike i izazovi za djecu i IKT industriju kako bi se pozabavili mogućnostima i izazovima za djecu u jednoj od najbrže rastućih industrija zabave. Rad istražuje sljedeće teme:

- Pravo djece na igru i slobodu izražavanja (vrijeme igranja i zdravstveni ishodi),
- Nediskriminacija, učešće i zaštita od zlostavljanja (socijalna interakcija i inkluzija, toksična okruženja, starosne granice i verifikacija, zaštita od vrbovanja i seksualnog zlostavljanja),
- Pravo na privatnost i slobodu od ekonomskog iskorištavanja (poslovni modeli za pristup podacima, besplatne igre i unovčavanje, nedostatak transparentnosti u komercijalnom sadržaju).

Dobre prakse: Tehnologija

Googleova laboratorija za virtuelnu realnost ispituje kako virtuelna realnost može pomoći u ohrabrivanju mladih da se bore protiv nasilja izvan interneta i na internetu.[1]

U septembru 2019. BBC je pokrenuo mobilnu aplikaciju koja se zove **Own IT**, aplikaciju za bezbjednost namijenjenu djeci od 8 do 13 godina koja dobijaju prvi pametni telefon. Aplikacija je dio BBC-jeve posvećenosti u pružanju podrške mladim ljudima u današnjem promjenjivom medijskom okruženju i prati uspješno pokretanje internet stranice Own IT u 2018. godini. Aplikacija kombinuje najsavremeniju tehnologiju mašinskog učenja za praćenje dječjih aktivnosti na njihovim pametnim telefonima s opcijom da djeca samostalno prijave svoje emocionalno stanje. Ona koristi ove informacije za isporuku prilagođenog sadržaja i intervencija koje pomažu djeci da ostanu sretna i bezbjedna na internetu, nudeći prijateljske i podržavajuće podsticaje kada njihovo ponašanje počne da odudara od normalnog. Korisnici mogu pristupiti aplikaciji kada traže pomoć, ali im je na raspolaganju i pružanje trenutnih savjeta i podrške na ekranu kada im je potrebna putem posebno razvijene tastature. Karakteristike uključuju:

- Podsjećanje korisnika da dobro razmisle prije nego što podijele lične podatke poput brojeva mobilnih telefona na društvenim medijima.
- Pomoć da razumiju kako bi drugi mogli da shvate poruke prije nego što pritisnu slanje.
- Praćenje njihovog raspoloženja tokom vremena i pružanje smjernica kako poboljšati situaciju ako je to potrebno.
- Pružanje informacija o temama poput korištenja telefona kasno naveče i uticaja na dobrobit korisnika.

Aplikacija sadrži posebno dopušten sadržaj sa BBC-a. Pruža korisne materijale i resurse koji pomažu mladim ljudima da iskoriste vrijeme na internetu na najbolji način i izgrade zdravo ponašanje i navike na internetu. Pomaže mladim ljudima i roditeljima da konstruktivnije razgovaraju o svojim iskustvima na internetu, ali roditeljima neće davati izvještaje ili povratne informacije, a niti jedan podatak neće napustiti uređaje korisnika. Aplikacija ne prikuplja nikakve lične podatke ili sadržaj generisan od korisnika dok se cijelo mašinsko učenje odvija u aplikaciji i na uređaju korisnika. Mašine se posebno podešavaju sa podacima koji se koriste za testiranje kako bi se osiguralo da nema kršenja privatnosti.

[1] Za više informacija pogledajte Alexa Hasse i dr., "Mladi i sajber zlostavljanje: Još jedan pogled", Berkman Klein centar za internet i društvo, 2019.

2.1.3 Posebna situacija kod djece sa smetnjama u razvoju[4]

Djeca i mladi sa invaliditetom suočavaju se sa rizicima na internetu na sličan način kao i ona bez invaliditeta, ali, pored toga, mogu se suočiti sa specifičnim rizicima koji se odnose na njihove invalidnosti. Djeca i mladi sa invaliditetom često se suočavaju sa isključenošću, stigmatizacijom i preprekama (fizičkim, ekonomskim, društvenim i u stavovima) u učešću u svojim zajednicama. Ova iskustva mogu imati negativan uticaj na dijete s invaliditetom i navesti ga da traži socijalne

[4] Pogledati Savjet Evrope, "Dva klika naprijed i jedan klik nazad: Izvještaj o djeci sa invaliditetom u digitalnom okruženju", 2019.

interakcije i prijateljstva na prostorima na internetu. Iako takve interakcije mogu biti pozitivne i pomoći u izgradnji samopoštovanja i stvaranju mreža podrške, one takođe mogu takvu djecu izložiti većem riziku slučajevima vrbovanja, podsticanja na internetu i/ili seksualnog uznemiravanja. Istraživanja pokazuju da su djeca i mladi koji imaju poteškoće izvan interneta i oni pogođeni psihosocijalnim poteškoćama pod povećanim rizikom od takvih incidenata.[5]

Djeca koja su žrtve izvan interneta, vjerovatno će biti žrtve i na internetu. To djecu sa invaliditetom stavlja u veći rizik na internetu, ali imaju i veću potrebu da budu na internetu. Istraživanja pokazuju da će djeca s invaliditetom vjerovatnije doživjeti zlostavljanje bilo koje vrste,[6] a posebno je vjerovatno da će doživjeti seksualnu viktimizaciju.[7] Viktimizacija može uključivati maltretiranje, uznemiravanje, isključenje i diskriminaciju na osnovu stvarne ili zamišljene invalidnosti djeteta ili zbog aspekata povezanih s njegovom invalidnošću, poput načina na koji se ponaša ili govori ili opreme ili usluga koje koristi.

Počinoci vrbovanja, podsticanja putem interneta i / ili seksualnog uznemiravanja djece i mladih sa invaliditetom mogu uključivati ne samo prestupnike sa preferencijama koji ciljaju djecu i mlade, već i one koji ciljaju djecu i mlade sa invaliditetom. Takvi počinioci mogu biti „privrženici“ - osobe koje nemaju invaliditet a koje seksualno privlače osobe s invaliditetom (najčešće osobe sa amputacijama i osobe koje koriste pomagala u kretanju), a od kojih se neki i sami pretvaraju da imaju invaliditet.[8] Radnje takvih ljudi mogu uključivati preuzimanje fotografija i video zapisa djece i mladih sa invaliditetom (koje su neškodljive prirode) i / ili njihovo dijeljenje putem namjenskih foruma ili profila na društvenim medijima. Alati za prijavljivanje na forumima i društvenim medijima često nemaju odgovarajući put za rješavanje takvih radnji.

Postoji briga da „roditeljsko dijeljenje“ (roditelji koji dijele informacije i fotografije svoje djece i mladih na internetu) može narušiti djetetovu privatnost, dovesti do maltretiranja, izazvati sramotu ili imati negativne posljedice kasnije u životu. [9] Neki roditelji djece sa smetnjama u razvoju mogu dijeliti informacije ili medijski materijal svog djeteta u potrazi za podrškom ili savjetom, što može kao rezultat imati da njihovo dijete stavlja u rizik kršenja privatnosti u tom trenutku i u budućnosti. Takvi roditelji takođe rizikuju da budu na meti neupućenih ili nesavjesnih ljudi koji nude tretmane, terapije ili "lijekove" za djetetov invaliditet. Jednako tako, neki roditelji djece i mladih sa invaliditetom mogu biti previše zaštitnički nastrojeni zbog nedostatka znanja o tome kako najbolje usmjeravati svoje dijete da koristi internet ili kako ga zaštititi od nasilja ili uznemiravanja.[10]

Pojedina djeca i mladi sa invaliditetom mogu se suočiti sa poteškoćama u korištenju ili čak isključenjem iz okruženja na internetu zbog nepristupačnog dizajna (npr. aplikacije koje ne dopuštaju povećanje veličine teksta), uskraćivanja traženih pogodnosti (npr. softvera za čitanje teksta sa ekrana ili prilagodljivih računarskih kontrola), ili potreba za odgovarajućom podrškom (npr. podučavanje kako se koristi oprema, podrška jedan na jedan za navigaciju u društvenim interakcijama).[11]

5 Andrew Schrock i dr., “Podsticanje, uznemiravanje i problematičan sadržaj”, Berkmanov centar za internet i društvo, 2008.
6 UNICEF, „Izvještaj o stanju djece u svijetu: Djeca sa invaliditetom,” 2013.
7 Katrin Mueller-Johnson i dr., “Seksualna viktimizacija mladih sa tjelesnim invaliditetom: Ispitivanje nivoa rasprostranjenosti, rizika, i zaštitnih faktora”, Časopis o međuljudskom nasilju, 2014.
8 Richard L Bruno, „Privrženici, glumci i ljudi koji to žele biti: Dva slučaja faktičkog poremećaja invalidnosti”, Seksualnost i invaliditet, 1997.
9 UNICEF, “Privatnost djece u doba Web 2.0 i 3.0: Izazovi i mogućnosti za politiku”, Innocenti diskusioni rad 2017-03 .
10 UNICEF, “Postoji li ljestvica dječjeg učešća na internetu?”, Innocenti istraživački sažetak, 2019.
11 Za smjernice o ovim pravima, vidi Konvenciju UN-a o pravima osoba s invaliditetom i Fakultativni protokol, posebno član 9. o pristupačnosti i član 21. o slobodi izražavanja i mišljenja i pristupu informacijama.

2.2 Postojeći nacionalni i transnacionalni modeli za zaštitu djece na internetu

Na globalnom nivou usvaja se nekoliko modela kako bi se djeca i mladi zaštitili na internetu. Interesne strane u IKT industriji trebale bi ih smatrati smjernicama za međunarodne inicijative i okvirom koji će osigurati da se ne štede napori u zaštiti djece i mladih na internetu. Internet industrija je raznolika i zamršena oblast, sastavljena od kompanija različitih veličina i funkcija. Važno je da se zaštitom djece ne bave samo platforme i usluge zasnovane na sadržaju već i oni koji podržavaju infrastrukturu interneta.

Mora se napomenuti da je kapacitet IKT kompanija da uvedu sveobuhvatnu politiku zaštite djece ograničen njihovim dostupnim resursima. Stoga ove smjernice preporučuju da IKT kompanije rade zajedno na uvođenju usluga za zaštitu korisnika. Dijeleći resurse i inženjersku stručnost, IKT kompanije bi mogle efikasnije da stvore "bezbjedne prostore" kako bi se spriječilo zlostavljanje.

Saradnja IKT kompanija

Tehnološka koalicija je primjer uspješne saradnje između interesnih strana u IKT industriji u borbi protiv seksualnog iskorištavanja i zlostavljanja djece.

Transnacionalni modeli

IKT kompanije bi trebale uključiti relevantne međunarodne smjernice u svoj strukturni program, i trebale bi se pridržavati svih relevantnih nacionalnih ili transnacionalnih zakona koji se primjenjuju u zemljama u kojima posluju. IKT kompanije ne bi trebalo da razmatraju samo radnje koje moraju preduzeti na pravnom nivou, već i koje aktivnosti mogu da obavljaju i, gde je to moguće, da nastoje da sprovode inicijative na globalnom nivou. Neki od modela koji pružaju principe za takve inicijative uključuju:

- Ministarski dobrovoljni principi pet država za borbu protiv seksualnog iskorištavanja i zlostavljanja djece (2020);
- Komisija za širokopojasni pristup za održivi razvoj, Bezbjednost djece na internetu: Smanjenje rizika od nasilja, zlostavljanja i iskorištavanja na internetu (2019);
- Globalni savez WePROTECT, Globalni strateški odgovor na seksualno iskorištavanje i zlostavljanje djece na internetu (2019);
- Globalno partnerstvo za zaustavljanje nasilja nad djecom, Bezbjedno za učenje: Poziv na akciju;
- Dječje dostojanstvo u digitalnom svijetu, Savez za dostojanstvo djeteta: Izvještaj radnje grupe za Tehnologiju (2018);
- Direktiva (EU) 2018/1808 Evropskog parlamenta i Savjeta: Direktiva o audio vizuelnim medijskim uslugama;
- Opšta uredba Evropske komisije o zaštiti podataka (2018);
- Preporuka OECD-a u pogledu bezbjednosti djece na internetu (2012).

Nacionalni modeli

Postoji niz nacionalnih i međunarodnih modela koji utvrđuju jasne uloge i odgovornosti tehnoloških kompanija u rješavanju zaštite djece na internetu. Neke od njih nisu specifične za djecu same po sebi, ali se mogu na njih odnositi kao na korisnike interneta. Oni pružaju sveobuhvatne smjernice IKT kompanijama u vezi sa regulatornim politikama, standardima i saradnjom sa drugim sektorima. U svrhu ovog dokumenta istaknuti su ključni principi takvih modela, koji se primjenjuju na IKT kompanije.

Kodeks dizajna prilagođenog uzrastu, Velika Britanija

Početkom 2019. godine Kancelarija povjerenika za informacije objavila je prijedloge za svoj kodeks za dizajniranje prilagođeno uzrastu radi unaprjeđenja zaštite dječjih podataka. Predloženi kodeks zasnovan je na najboljem interesu za djecu, kako je utvrđeno u Konvenciji o pravima djeteta UN-a, i u njemu je iznijeto nekoliko očekivanja od IKT kompanija. Kodeks se sastoji od petnaest standarda koji uključuju usluge određivanja lokacije za djecu isključene u početnim podešavanjima, IKT kompanije da prikupljaju i zadržavaju samo minimalnu količinu ličnih podataka djece, da proizvodi budu privatni po samom dizajnu i da objašnjenja odgovaraju uzrastu i da su dostupna.

Zakon o štetnim digitalnim komunikacijama, Novi Zeland

Zakonom iz 2015. godine sajber zlostavljanje je okarakterisano kao specifično krivično djelo i fokusira se na širok raspon šteta, od sajber maltretiranja do pornografije iz osvete. Cilj mu je obeshrabriti, spriječiti i umanjiti štetnu digitalnu komunikaciju, čineći nezakonitim postavljanje digitalne komunikacije sa namjerom da se izazove ozbiljna emocionalna uznemirenost kod druge osobe, i postavlja niz od 10 principa komunikacije. Omogućava korisnicima da se žale nezavisnoj organizaciji ako su ovi principi prekršeni ili se primjenjuju na sudske naloge protiv autora ili domaćina komunikacije ako problem nije riješen.

Povjerenik eSafety, Australija

Osnovana 2015. godine, australijski Povjerenik eSafety prva je svjetska vladina agencija posvećena borbi protiv zloupotrebe na internetu i održavanju bezbjednosti svojih građana na internetu. Kao nacionalni nezavisni regulator za bezbjednost na internetu, eSafety ima snažnu kombinaciju funkcija. One se kreću od prevencije preko podizanja svijesti, obrazovanja, istraživanja i davanja smjernica za najbolju praksu, do rane intervencije i sanacije štete kroz više zakonskih regulatornih planova koje daju eSafety-u ovlaštenja da brzo ukloni sajber maltretiranje, zlostavljanje zasnovano na slikama i nezakonit sadržaj na internetu. Ova široka nadležnost omogućava eSafeti-u da se brine o bezbjednosti na internetu na višestran, cjelovit i proaktivan način.

U 2018. godini eSafety je razvio Safety by Design (SbD), inicijativu koja stavlja bezbjednost i prava korisnika u središte dizajna, razvoja i uvođenja internetskih proizvoda i usluga. Skup principa bezbjednosti po dizajnu nalazi se u središtu inicijative koja utvrđuje realne, djelotvorne i ostvarive mjere koje IKT kompanije trebaju preduzeti kako bi bolje zaštitile i odbranile građane na internetu. Tri sveobuhvatna principa su:

1) **Odgovornosti pružaoca usluga**: teret bezbjednosti nikada ne bi trebao pasti na krajnjeg korisnika. Mogu se preduzeti preventivni koraci kako bi se osiguralo da se poznate i predviđene štete procijene u dizajnu i pružanju usluga na internetu, zajedno sa koracima kako bi se smanjila vjerovatnoća da će usluge olakšati, započeti ili podstaknuti nezakonito i neprikladno ponašanje.
2) **Davanje mogućnosti i autonomije korisnicima**: dostojanstvo korisnika i njihovi najbolji interesi su od centralne važnosti. Ljudske djelatnosti i autonomiju treba podržati, pojačati i ojačati u dizajnu usluga omogućavajući korisnicima veću kontrolu, upravljanje i regulaciju sopstvenih iskustava.
3) **Transparentnost i odgovornost**: ovo su obilježja snažnog pristupa bezbjednosti, koje pružaju garancije da službe djeluju u skladu sa objavljenim bezbjedonosnim ciljevima, kao i edukacija i davanje mogućnosti javnosti da preduzmu mjere radi rješavanja sigurnosnih problema.

Globalni savez WeProtect

U središtu strategije WePROTECT Globalnog saveza je podrška zemljama da razviju koordinisane odgovore više interesnih strana za borbu protiv seksualnog iskorištavanja djece na internetu, vođene svojim Modelima nacionalnog odgovora, koji djeluju kao nacrt za djelovanje na nacionalnom nivou. Pruža okvir za zemlje na koji bi se trebale osloniti u borbi protiv seksualnog iskorištavanja djece na internetu. Unutar WePROTECT Modela nacionalnog odgovora, postoji jasan skup obaveza za IKT kompanije koje se odnose na:

- postupke obavještavanja i uklanjanja;
- prijavljivanje seksualnog iskorištavanja i zlostavljanja djece (CSEA);
- razvoj tehnoloških rješenja; i
- investiranje u efikasne preventivne programe i usluge reagovanja za zaštitu djece na internetu.

Globalno partnerstvo i fond za zaustavljanje nasilja nad djecom

Globalno partnerstvo i fond za zaustavljanje nasilja nad djecom pokrenuo je generalni sekretar Ujedinjenih nacija 2016. godine sa jednim ciljem: katalizovati i podržati akciju za zaustavljanje svih oblika nasilja nad djecom do 2030. godine, kroz jedinstvenu saradnju preko 400 partnera iz svih sektora.

Fokus rada je na spašavanju i pružanju podrške žrtvama, tehnološkim rješenjima za otkrivanje i sprječavanje prekršaja, pružanju podrške organima za sprovođenje zakona, zakonodavnim i političkim reformama, i generisanju podataka i dokaza o razmjerama i prirodi seksualnog iskorištavanja i zlostavljanja djece na internetu, kao i razumijevanju dječjih perspektiva.[12]

3. Ključna područja zaštite i promocije dječjih prava

Ovaj odjeljak navodi **pet ključnih područja** u kojima IKT kompanije mogu preduzeti mjere za zaštitu djece i mladih kada koriste IK tehnologije i da promovišu njihovu pozitivnu upotrebu IK tehnologija.

3.1 Razmatranja o integraciji prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja

Razmatranje integracije prava djeteta zahtijeva da kompanije preduzmu odgovarajuće mjere za identifikovanje, sprečavanje, ublažavanje i, po potrebi, saniranje potencijalnih i stvarnih negativnih uticaja na dječja prava. Vodeći principi UN-a o poslovanju i ljudskim pravima pozivaju sva preduzeća i industrije da uspostave odgovarajuće politike i procese kako bi ispunili svoju odgovornost prema poštovanju ljudskih prava.

[12] Za više informacija pogledajte Zaustavljanje nasilja nad djecom, "Korisnici fonda za zaustavljanje nasilja".

IKT kompanije bi trebale posvetiti posebnu pažnju djeci i mladima kao ranjivoj grupi s obzirom na njihovu zaštitu podataka i slobodu izražavanja. Rezolucija Generalne skupštine Ujedinjenih nacija 68/167 o pravu na privatnost u digitalno doba potvrđuje pravo na privatnost i slobodu izražavanja bez izlaganja nezakonitom uplitanju. Pored toga, Rezolucija 32/13 Savjeta UN-a za ljudska prava o promociji, zaštiti i uživanju ljudskih prava na internetu prepoznaje globalnu i otvorenu prirodu interneta kao pokretačke snage u ubrzavanju napretka prema razvoju i potvrđuje da ista prava koja ljudi imaju izvan interneta takođe moraju biti zaštićena na internetu. U državama u kojima nedostaje odgovarajući pravni okvir za zaštitu prava djece i mladih na privatnost i slobodu izražavanja, IKT kompanije bi trebale da prate pojačanu dubinsku analizu kako bi osigurale da su politike i prakse u skladu sa međunarodnim pravom. Kako se građanski angažman mladih nastavlja povećavati putem komunikacija na internetu, IKT kompanije imaju veću odgovornost za poštovanje prava djece i mladih, čak i tamo gdje domaći zakoni još uvijek nisu sustigli međunarodne standarde.

> Kompanije bi trebale imati uspostavljen mehanizam za žalbe na operativnom nivou koji će osigurati format za pogođene pojedince da izraze zabrinutost zbog potencijalnih prekršaja. Mehanizmi na operativnom nivou trebaju biti dostupni djeci, njihovim porodicama i onima koji zastupaju njihove interese. Princip 31 Vodećih principa o poslovanju i ljudskim pravima pojašnjava da takvi mehanizmi trebaju biti legitimni, dostupni, predvidljivi, nepristrasni, transparentni, kompatibilni sa pravima, izvor kontinuiranog učenja i zasnovani na angažovanju i dijalogu. Zajedno sa internim procesima za rješavanje negativnih uticaja, mehanizmi za žalbe trebali bi osigurati da kompanije imaju uspostavljene okvire koji osiguravaju djeci i mladima odgovarajući način da traže pomoć kada su njihova prava ugrožena.

Kompanije treba da zauzmu pristup prema IKT bezbjednosti zasnovan na usklađenosti koji se fokusira na ispunjavanje nacionalnog zakonodavstva, slijeđenje međunarodnih smjernica kada nema nacionalnog zakonodavstva i izbjegavanje negativnih uticaja na prava djece i mladih, i da kompanije proaktivno promovišu razvoj i dobrobit djece i mladih volonterskim akcijama koje unaprjeđuju prava djece i mladih na pristup informacijama, slobodu izražavanja, učešće, obrazovanje i kulturu.

Dobre prakse: Dizajn koji odgovara politici i uzrastu

Kompanija za razvoj aplikacija Toca Boca proizvodi digitalne igračke iz perspektive djeteta. Politika privatnosti kompanije osmišljena je tako da navodi koje podatke kompanija prikuplja i kako se koriste. Toca Boca, Inc je član PRIVO bezbjedne dječje privatnosti CORPA programa za certifikaciju bezbjednih utočišta.

LEGO® Life je primjer bezbjedne platforme društvenih medija za djecu mlađu od 13 godina za dijeljenje svojih LEGO kreacija, za dobijanje inspiracije i bezbjednu interakciju. Ovdje se od djece ne traže nikakvi lični podaci za stvaranje profila, za šta je samo potrebna adresa e-pošte roditelja ili staratelja. Aplikacija stvara priliku djeci i porodicama da razgovaraju o bezbjednosti na internetu i privatnosti u pozitivnom okruženju.

Primjeri dizajna primjerenog uzrastu uključuju specifične ponude nekih od velikih javnih servisa za određene starosne grupe: na primjer, njemački ARD (Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland - Das Erste) i ZDF (Zweites Deutsches Fernsehen) cilja svoju publiku počevši od uzrasta od 14 godina, nudeći prilagođeni sadržaj putem internetskog kanala funk.net. BBC (Britanska radiodifuzna korporacija) pokrenula je CBeebies koji je usmjeren na djecu mlađu od 6 godina. Sadržaj internet stranice je posebno prilagođen odgovarajućim starosnim grupama.

Dobre prakse: Politika i tehnologija

Twitter konstantno ulaže u vlasničku tehnologiju, što je doprinijelo stabilnom smanjenju opterećenja za ljude kod slanja prijava.[1] Konkretno, više od 50% tweetova, u poređenju sa 20% u 2018. godini, koje je Twitter ispratio da odgovori na njihovu nasilnu prirodu, trenutno se proaktivno pojavljuju korištenjem tehnologije, umjesto da se oslanjaju na prijavljivanje Twitteru. Nova tehnologija se koristi za bavljenje političkim sadržajima polja privatnog informisanja, osjetljivim medijima, ponašanjem iz mržnje, zlostavljanjem i lažnim predstavljanjem.

[1] Twitterov,"15. izvještaj o transparentnosti: Povećanje proaktivnog izvršenja na profilima".

3.2 Razvoj standardnih postupaka za rukovanje materijalima seksualnog zlostavljanja djece

U 2019. godini IWF je djelovala na 132.676 internet stranica za koje je potvrđeno da sadrže seksualno zlostavljanje djece.[13] Bilo koja internet adresa bi mogla sadržavati stotine, ako ne i hiljade slika i video zapisa. Od slika nad kojima je IWF preduzela mjere, 45% je prikazivalo djecu uzrasta 10 ili manje godina i 1.609 internet stranica prikazivalo je djecu uzrasta 0–2 godine, od kojih je 71% sadržavalo najteže seksualno zlostavljanje, poput silovanja i seksualnog mučenja. Ove uznemirujuće činjenice ističu važnost zajedničkog djelovanja IKT kompanija, vlada, organa za sprovođenje zakona i civilnog društva u borbi za prevenciju materijala seksualnog zlostavljanja djece.

[13] IWF, "Zašto. Kako. Ko. I rezultati. Godišnji izvještaj 2019".

Iako se mnoge vlade bore protiv širenja i distribucije materijala seksualnog zlostavljanja djece donošenjem zakona, progonom i procesuiranjem nasilnika, podizanjem svijesti i pružanjem podrške djeci i mladima u oporavku od zlostavljanja ili iskorištavanja, postoje mnoge zemlje koje još uvijek nemaju uspostavljene odgovarajuće sisteme. U svakoj zemlji su potrebni mehanizmi koji će omogućiti široj javnosti da prijavi nasilni i eksploatacioni sadržaj ove prirode. IKT kompanije, organi za sprovođenje zakona, vlade i civilno društvo moraju sarađivati kako bi osigurali uspostavljanje odgovarajućeg pravnog okvira u skladu sa međunarodnim standardima. Takvi okviri bi trebalo da inkriminišu sve oblike seksualnog iskorištavanja i zlostavljanja djece, uključujući i materijal seksualnog zlostavljanja djece, i da zaštite decu koja su žrtve takvog zlostavljanja ili iskorištavanja. Ti okviri moraju osigurati da procesi prijavljivanja, istrage i uklanjanja sadržaja rade što efikasnije.

IKT kompanije bi trebale obezbijediti veze do nacionalnih linija za podršku ili drugih lokalno dostupnih linija za podršku, poput IWF portala u nekim zemljama, a u nedostatku lokalnih mogućnosti prijavljivanja, da obezbijede veze do drugih međunarodnih linija za podršku po potrebi, kao što je Američki nacionalni centar za nestalu i zlostavljanu djecu (NCMEC) ili Međunarodno udruženje internetskih linija za podršku (INHOPE), gdje se bilo koja međunarodna linija za podršku može koristiti za podnošenje prijave.

Odgovorne kompanije poduzimaju niz koraka kako bi spriječile da se njihove mreže i usluge koriste za širenje materijala seksualnog zlostavljanja djece. To uključuje uvođenje jezika u uslove i odredbe ili kodekse ponašanja koji izričito zabranjuju takav sadržaj ili ponašanje;[14] razvijanje snažnih procesa obavještavanja i uklanjanja; te rad i podrška nacionalnim linijama za podršku.

Pored toga, neke kompanije primenjuju tehničke mjere kako bi spriječile zloupotrebu svojih usluga ili mreža za deljenje poznatog materijala seksualnog zlostavljanja djece. Na primjer, neki provajderi internetskih usluga blokiraju pristup internet adresama za koje je odgovarajuće tijelo potvrdilo da sadrže materijal seksualnog zlostavljanja djece ako je internet stranica hostirana u zemlji u kojoj nisu uspostavljeni procesi kako bi se osiguralo da će se on brzo ukloniti. Drugi koriste tehnologije heširanja za automatsko otkrivanje i uklanjanje slika seksualnog zlostavljanja djece koje su već poznate policiji ili linijama za podršku. Članovi IKT industrije trebali bi razmotriti i uključiti sve relevantne službe u svoje operacije kako bi se spriječilo širenje seksualnog zlostavljanja djece.

Akteri u IKT industriji trebali bi se obavezati na dodjelu proporcionalnih resursa i nastaviti razvijati i dijeliti, po mogućnosti, tehnološka rješenja otvorenog koda za otkrivanje i uklanjanje materijala seksualnog zlostavljanja djece.

Dobre prakse: Tehnologija

Microsoft koristi četvorostruki pristup za podsticanje odgovorne i bezbjedne upotrebe tehnologije, sa fokusom na samu tehnologiju, samoupravljanje, partnerstva i obrazovanje i dopiranje do potrošača. Microsoft je takođe ugradio funkcije koje daju mogućnost pojedincima da efikasnije upravljaju sa bezbijednosti na internetu. "Porodična bezbjednost" je jedna od takvih karakteristika koja omogućava roditeljima i starateljima da nadgledaju upotrebu interneta svoje djece.

Microsoft sprovodi politike protiv uznemiravanja na svojim platformama, a korisnici koji zloupotrebljavaju ove propise podliježu ukidanju profila ili, u slučaju ozbiljnijih kršenja, mjerama za sprovođenje zakona.

[14] Treba imati na umu da neprimjereno ponašanje korisnika nije ograničeno na materijal seksualnog zlostavljanja djece i da kompanija treba na odgovarajući način postupati s bilo kojom vrstom neprimjerenog ponašanja ili sadržaja.

Microsoft PhotoDNA je alat koji kreira heševe slika i upoređuje ih sa bazom podataka hešova koji su već identifikovani i za koje je potvrđeno da su materijal seksualnog zlostavljanja djece. Ako pronađe podudaranje, slika se blokira. Ovaj je alat omogućio provajderima sadržaja uklanjanje miliona nezakonitih fotografija sa interneta; pomogao je osuditi dječje seksualne predatore; a u nekim slučajevima pomogao je policiji da spasi potencijalne žrtve prije nego što su bile fizički povrijeđene. Microsoft se već dugo zalaže za zaštitu svojih kupaca od nezakonitih sadržaja na svojim proizvodima i uslugama, a primjena tehnologije koju je kompanija već napravila u borbi protiv rasta ovakvih nezakonitih video zapisa bio je logičan sljedeći korak. Međutim, ovaj alat ne koristi tehnologiju prepoznavanja lica niti može identifikovati osobu ili predmet na slici. Ali sa pojavom PhotoDNA for Video stvari su poprimile novi zaokret. PhotoDNA for Video rastavlja video zapis u ključne kadrove i u osnovi stvara hešove za te snimke ekrana. Na isti način na koji PhotoDNA može pronaći podudaranje sa slikom koja je izmijenjena kako bi se izbjeglo otkrivanje, PhotoDNA for Video može pronaći sadržaj seksualnog iskorištavanja djece koji je uređen ili spojen u video zapis koji bi u protivnom mogao izgledati bezazlen.

Štaviše, Microsoft je u skorije vrijeme objavio novi alat za prepoznavanje dječjih predatora koji u chatovima na internetu vrbuju djecu zbog zlostavljanja. Projekat Artemis, razvijen u saradnji sa kompanijama The Meet Group, Roblox, Kik i Thorn, nadovezuje se na Microsoftovu patentiranu tehnologiju i putem Thorna će biti dostupan besplatno kvalifikovanim uslužnim kompanijama na internetu koje nude funkciju chata. Projekat Artemis je tehnički alat koji daje upozorenja administratorima kada je potrebna moderacija u chat sobama. Ovom tehnikom otkrivanja vrbovanja moći će otkriti, reagovati i prijaviti predatore koji pokušavaju namamiti djecu u seksualne svrhe.

IWF pruža niz usluga članovima IKT industrije kako bi zaštitio svoje korisnike od toga da slučajno naiđu na materijal seksualnog zlostavljanja djece. One uključuju:

- Dinamičku blok listu internet adresa materijala uživo, osiguranog kvaliteta;
- Heš listu poznatog kriminalnog sadržaja koji se odnosi na materijal seksualnog zlostavljanja djece;
- Jedinstvena lista ključnih riječi tajnih izraza za koje se zna da su povezane sa materijalima seksualnog zlostavljanja djece;
- Spisak detalja o nazivima domena koji su poznati po hostiranju sadržaja seksualnog zlostavljanja djece kako bi se omogućilo brzo uklanjanje domena u kojima se nalazi nezakoniti sadržaj.

3.3 Stvaranje bezbjednijeg okruženja na internetu prilagođenog uzrastu

Vrlo malo stvari u životu može se smatrati apsolutno bezbjednim i bez rizika cijelo vrijeme. Čak se i u gradovima u kojima je kretanje saobraćaja visoko regulisano i strogo kontrolisano, nesreće se i dalje dešavaju. Na isti način, sajber prostor nije bez rizika, posebno za djecu i mlade. O djeci i mladima se može razmišljati kao o primaocima, učesnicima i akterima u njihovom okruženju na internetu. Rizici sa kojima se suočavaju mogu se podijeliti u četiri područja:[15]

15 Sonia Livingstone i dr., “EU Kids Online: Završni izvještaj”, Londonska škola ekonomije, 2009.

- *Neprimjeren sadržaj* - Djeca i mladi mogu naići na neprimjeren i nezakonit sadržaj dok traže nešto drugo klikom na vjerovatno bezazlen link u instant poruci, na blogu ili prilikom dijeljenja datoteka. Oni takođe mogu tražiti i dijeliti neprikladan materijal ili materijal neprilagođen uzrastu. Ono što se smatra štetnim sadržajem razlikuje se od zemlje do zemlje; primjeri uključuju sadržaj koji promoviše zloupotrebu opojnih droga, rasnu mržnju, rizično ponašanje, samoubistvo, anoreksiju ili nasilje.
- *Neprimjereno ponašanje* - Djeca i odrasli mogu koristiti internet za uznemiravanje ili čak iskorištavanje drugih ljudi. Djeca mogu ponekad emitovati uvrjedljive komentare ili neugodne slike ili mogu ukrasti sadržaj ili povrijediti autorska prava.
- *Neprikladan kontakt* - I odrasli i mladi mogu putem interneta tražiti djecu ili druge mlade ljude koji su ranjivi. Često, njihov cilj je uvjeriti metu da su razvili smislen odnos, ali osnovna svrha je manipulativna. Oni mogu pokušati nagovoriti dijete da izvrši seksualna ili druga izopačena djela na internetu, koristeći veb kameru ili drugi uređaj za snimanje, ili će pokušati ugovoriti lični sastanak i fizički kontakt. Ovaj proces se često naziva „vrbovanje“.
- *Komercijalni rizici* - Ova kategorija odnosi se na rizike narušavanja privatnosti podataka koji se odnose na prikupljanje i upotrebu dječjih podataka, kao i digitalni marketing. Bezbjednost na internetu je izazov zajednice i prilika za IKT kompanije, vlade i civilno društvo da rade zajedno na uspostavljanju bezbjedonosnih principa i praksi. IKT kompanije mogu da ponude čitav niz tehničkih pristupa, alata i usluga za roditelje, djecu i mlade, i prije svega treba napraviti proizvode koji su jednostavni za upotrebu, bezbjedni po dizajnu i primjereni uzrastu za njihov širok spektar korisnika. Dodatni pristupi uključuju ponudu alata za razvoj odgovarajućih sistema za provjeru starosti koji poštuju dječja prava na privatnost i pristup ili ograničavaju pristup djeci i mladima sadržaju koji je neprimjeren njihovim godinama ili ograničavaju ljude sa kojima djeca mogu imati kontakt ili vrijeme u kojem mogu koristiti internet. Ono što je najvažnije, okviri „bezbjednost po dizajnu“[16], uključujući i privatnost, moraju biti uključeni u procese razvijanja inovacija i dizajna proizvoda. Dječja bezbjednost i odgovorno korištenje tehnologije moraju se pažljivo razmotriti i o njima se ne smije misliti naknadno.

Neki programi omogućavaju roditeljima nadgledanje tekstualnih poruka i drugih komunikacija koje njihova djeca i mladi šalju i primaju. Ako će se koristiti programi ove vrste, važno je da se o tome otvoreno razgovara s djetetom, inače se takvo ponašanje može doživjeti kao „špijuniranje“ i može potkopati povjerenje u porodici.

Politike prihvatljive upotrebe jedan su od načina na koji IKT kompanije mogu utvrditi kakvo se ponašanje podstiče i kod odraslih i kod djece, koje vrste aktivnosti nisu prihvatljive i posljedice bilo kakvog kršenja ovih politika. Jasni i transparentni mehanizmi prijavljivanja trebaju biti dostupni korisnicima koji se brinu o sadržaju i ponašanju. Pored toga, prijavljivanje treba ispratiti na odgovarajući način, uz pravovremeno pružanje informacija o statusu prijave. Iako kompanije mogu različito primjenjivati prateće mehanizme od slučaja do slučaja, bitno je postaviti jasan vremenski okvir za reagovanje, saopštiti odluku donesenu u vezi sa prijavom i ponuditi način rješavanja ako korisnik nije zadovoljan odgovorom.

16 Povjerenik eSafety, Pregled bezbjednosti po dizajnu, 2019.

Dobre prakse: Izvještavanje

Facebook je, u nastojanju da suzbije seksualno uznemiravanje na digitalnim platformama, sufinansirao projekat deSHAME sa Evropskom unijom, saradnju između Childnet, Save the Children, Kek Vonal i UCLan. Cilj ovog projekta je povećati prijavljivanje seksualnog uznemiravanja putem interneta među maloljetnicima i poboljšati multisektorsku saradnju u prevenciji i reagovanju na ovakvo ponašanje.

Kako je jedna od glavnih svrha projekta podsticanje korisnika da prijavljuju sadržaje koji su uznemiravajućeg karaktera ili su neprimjereni, Facebook-ovi standardi zajednice takođe su relevantni kao smjernice o tome šta je dopušteno, a šta nije dopušteno na Facebooku. Oni takođe navode tipove korisnika kojima ne dopušta postavljanje sadržaja. Facebook je takođe stvorio bezbjedonosne elemente poput elementa "Poznajete li ovu osobu?"; „drugi“ inboks koji prikuplja nove poruke od ljudi koje korisnik ne poznaje; i popup prozor koji se pojavljuje na obavještenjima ako to izgleda kao da je maloljetnika kontaktirala odrasla osoba koju on ili ona ne poznaje.

Provajderi sadržaja i usluga na internetu mogu takođe opisati prirodu sadržaja ili usluga koje pružaju i predviđeni ciljni starosni raspon. Ovi bi opisi trebali biti usklađeni sa postojećim nacionalnim i međunarodnim standardima, relevantnim propisima i savjetima o marketingu i oglašavanju za djecu koje odgovarajući organi za klasifikaciju stavljaju na raspolaganje. Ovaj proces postaje sve komplikovaniji s rastućim spektrom interaktivnih usluga koje omogućavaju objavljivanje korisničkog sadržaja, na primjer putem oglasnih ploča, chat soba i usluga društvenih mreža. Kada kompanije posebno ciljaju djecu i mlade i kada su usluge pretežno usmjerene na mlađu publiku, očekivanja u smislu lakoće za korištenje, lako razumljivom i pristupačnom sadržaju i bezbjednosti biće mnogo veća.

Kompanije se takođe podstiču da usvoje najviše standarde zaštite privatnosti kada je u pitanju prikupljanje, obrada i čuvanje podataka od ili o djeci i mladima, jer djeci i mladima može nedostajati zrelost da uvide šire društvene i lične posljedice otkrivanja ili pristanka na dijeljenje svojih ličnih podataka na internetu ili na upotrebu njihovih ličnih podataka u komercijalne svrhe. Usluge usmjerene na ili koje bi vjerovatno privukle kao glavnu publiku djecu i mlade moraju uzeti u obzir rizike u kojima se mogu naći zbog pristupa ili prikupljanja i upotrebe ličnih podataka (uključujući podatke o lokaciji) i osigurati da se ti rizici rješavaju na pravi način i da su korisnici informisani. Konkretno, kompanije bi trebale osigurati da jezik i stil bilo kojeg materijala ili komunikacije koji se koriste za promociju usluga, pružanje pristupa uslugama ili putem kojih se pristupa, prikuplja i koriste lični podaci, pomažu razumijevanju i pomažu korisnicima u upravljanju zaštitom njihove privatnosti na jasan i jednostavan način i da objašnjavaju na šta pristaju jasnim, razumljivim jezikom.

Dobre prakse: Inovacija

U 2018. – 2019. UNICEF-ova Regionalna kancelarija za Istočnu Aziju i Pacifik organizovala je pet okruglih stolova sa više interesnih strana radi razmjene obećavajućih praksi IKT kompanija za borbu protiv seksualnog iskorištavanja i zlostavljanja djece na internetu. Učesnici okruglih stolova bile su vodeće kompanije iz privatnog sektora, kao što su Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Mongolija) Mobifone + (Vijetnam), Globe Telecom (Filipini), True (Tajland), GSMA i partneri iz civilnog društva, uključujući INHOPE, ECPAT International i Međunarodna linija za pomoć djeci.

U sklopu istog projekta, u februaru 2020. godine, UNICEF je pokrenuo Think Tank kako bi ubrzao liderstvo u IKT kompanijama u istočnoj Aziji i pacifičkom regionu da bi spriječio nasilje nad djecom u svijetu na internetu. Think Tank je inkubator ideja i inovacija, koji se oslanja na jedinstvene perspektive aktera u IKT industriji (stvaranje proizvoda, marketing, itd.) za razvoj uticajnih obrazovnih materijala i identifikaciju najefikasnijih platformi za isporuku, kao i za razvoj okvira za evaluaciju koji može izmjeriti uticaj ovih obrazovnih materijala i poruka usmjerenih na djecu. Think Tank čine Facebook, Telenor, akademski stručnjaci, agencije Ujedinjenih nacija, poput ITU-a, UNESCO-a i UNODC-a, i druge, poput australijskog povjerenika eSafety, ECPAT International, ICMEC-a, INTERPOL-a i Globalnog fonda za zaustavljanje nasilja. Inaugurativni sastanak Think Tank-a, održan paralelno s ASEAN-ovom regionalnom konferencijom o zaštiti djece na internetu, okupio je stručnjake, uključujući Microsoft, kako bi istražili tehnologije i istraživačke mogućnosti za bolje praćenje promjena u ponašanju na internetu, na osnovu preuzimanja bezbjedonosnih materijala i poruka na internetu.

3.4 Edukacija djece, roditelja i edukatora o bezbjednosti djece i njihovoj odgovornoj upotrebi IK tehnologija

Tehničke mjere mogu biti važan dio osiguranja zaštite djece i mladih od potencijalnih rizika na internetu, ali one su samo jedan elemenat jednačine. Alati za roditeljsku kontrolu, podizanje svijesti i obrazovanje takođe su ključne komponente koje će pomoći u osnaživanju i informisanju djece i mladih svih uzrasta, kao i roditelja, staratelja i edukatora. Iako kompanije imaju važnu ulogu u podsticanju djece i mladih da koriste IK tehnologije na odgovoran i bezbjedan način, tu odgovornost dijele sa roditeljima, školama, djecom i mladima.

Mnoge kompanije ulažu u obrazovne programe osmišljene kako bi korisnicima omogućile donošenje utemeljenih odluka o sadržaju i uslugama. Kompanije pomažu roditeljima, starateljima i edukatorima u usmjeravanju djece i mladih prema bezbjednijim, odgovornijim i primjerenijim iskustvima na internetu i mobilnim telefonima. To uključuje objavljivanje znakovnog sadržaja osjetljivog na starosnu granicu i osiguravanje da se informacije o stavkama kao što su cijene sadržaja, uslovi pretplate i način otkazivanja pretplate jasno saopštavaju. Promovisanje poštovanja uslova minimalne starosne granice od strane društvenih medija u svim zemljama u kojima je moguće provjeravanje starosti takođe bi pomoglo u zaštiti djece omogućavanjem pristupa uslugama odgovarajućem uzrastu. Važno razmatranje koje treba uskladiti sa ovom preporukom je dodatno prikupljanje ličnih podataka koje ovo može da podrazumijeva i potreba da se ograniči prikupljanje i čuvanje ovih podataka i njihova obrada.

Takođe je važno pružiti informacije djeci i mladima direktno o bezbjednijoj upotrebi IK tehnologija i pozitivnom i odgovornom ponašanju. Pored podizanja svijesti o bezbjednosti, kompanije mogu omogućiti pozitivna iskustva razvijanjem sadržaja za djecu i mlade o tome da poštuju jedni druge, budu ljubazni i otvorenog uma kada koriste IK tehnologije i brinu se o prijateljima. One mogu pružiti informacije o radnjama koje se trebaju preduzeti ako postoje negativna iskustva, poput maltretiranja na internetu ili vrbovanja, olakšavajući prijavu takvih incidenata i pružajući funkciju za odbijanje primanja anonimnih poruka.

Roditelji ponekad imaju manje razumijevanja i znanja o internetu i mobilnim uređajima od djece i mladih. Štaviše, spajanje mobilnih uređaja i internet usluga otežava roditeljski nadzor. IKT kompanije mogu raditi u saradnji sa vladom i edukatorima na jačanju sposobnosti roditelja da podrže svoju djecu u izgradnji njihove digitalne otpornosti i ponašanja kao odgovornih digitalnih građana. Cilj nije prenijeti odgovornost za upotrebu IK tehnologija od strane djece i mladih samo na roditelje, već prepoznati da su roditelji u boljoj poziciji da odluče šta je prikladno za njihovu djecu i da ih treba upoznati sa svim rizicima kako bi bolje zaštititi svoju djecu i osnažiti ih za preduzimanje akcije.

Informacije se mogu prenositi na internetu i izvan njega putem više medijskih kanala, uzimajući u obzir da neki roditelji ne koriste internet usluge. Važno je sarađivati sa školskim distriktima kako bi se pripremili nastavni planovi i programi o bezbjednosti na internetu i odgovornoj upotrebi IK tehnologija od strane djece i mladih, kao i obrazovni materijali za roditelje. Primjeri uključuju objašnjenje vrsta usluga i opcija dostupnih za praćenje aktivnosti, radnje koje se preduzimaju ako se dijete suočava sa maltretiranjem ili vrbovanjem na internetu, kako izbjeći neželjenu poštu i upravljati podešavanjima privatnosti i kako razgovarati sa dječacima i djevojčicama različitih starosnih grupa o osjetljivim problemima. Komunikacija je dvosmjeran proces i mnoge kompanije nude mogućnost kupcima da ih kontaktiraju kako bi prijavili probleme ili razgovarali o problemima.

Kako sadržaj i usluge postaju sve bogatiji, svi će korisnici i dalje imati koristi od savjeta i podsjetnika o prirodi određene usluge i načinu bezbjednog uživanja u njoj. Iako je važno djecu naučiti odgovornim korištenjem interneta, znamo da djeca vole eksperimentisati, rizikovati, da su znatiželjna i možda ne donose uvijek najbolje odluke. Davanje šanse da se bave svojim djelatnostima doprinosi njihovom razvoju i zdrav je način koji će im pomoći da razviju autonomiju i otpornost, sve dok povratni efekat nije preoštar. Iako se djeci mora dozvoliti da preuzimaju određene rizike u internetskom okruženju, presudno je da ih roditelji i kompanije mogu podržati kada stvari krenu po zlu, jer to može nadoknaditi negativan uticaj neugodnog iskustva i pretvoriti ga u korisnu lekciju za budućnost.

Dobre prakse: Obrazovanje

NHK Japan vodi kampanju prevencije samoubistava za mlade na Twitteru: U Japanu samoubistva među tinejdžerima dostižu vrhunac kada se vrate u školu nakon ljetnog raspusta. Povratak u stvarnost je razlog za vrhunac. Produkcijski tim NHK Heart Net TV (NHK Japan) proizvodi multimedijalni program # U noći 31. avgusta. Povezujući televiziju, prenos uživo i društvene medije, NKH je uspješno stvorio "mjesto" na kojem su tinejdžeri mogli bez straha podijeliti svoja osjećanja.

Dobre prakse: Obrazovanje

Twitter je takođe objavio vodič za edukatore o medijskoj pismenosti. Sastavljen sa UNESCO-om, priručnik prvenstveno ima za cilj da pomogne edukatorima da razviju kod mlađih generacija vještine medijske pismenosti. Drugi aspekt bezbjedonosnog rada Twittera odnosi se na njihovo otkrivanje operacija sa informacijama. Ovo je arhiva operacija sa informacijama koje podržava država i koju Twitter javno dijeli. Inicijativa je pokrenuta kako bi se osnažilo akademsko i javno razumijevanje kampanja povezanih sa ovom problematikom širom svijeta, i da bi se osnažila nezavisana kontrola trećih lica ovih taktika na Twitter platformi.

Projekat deSHAME, koji sufinansiraju Facebook i Evropska unija, takođe omogućava stvaranje resursa za širok raspon starosnih grupa, sa posebnim fokusom na djecu uzrasta od 9 do 13 godina. Kao dio projekta, razvijen je alat pod nazivom "Iskorači, govori!", koji pruža niz materijala za obrazovanje, obuku i podizanje svijesti, kao i praktične alate za multisektorske strategije prevencije i reagovanja. Projekat će ove materijale za učenje prenijeti drugim evropskim zemljama i partnerima širom svijeta u svrhu promocije digitalnih prava mladih.

Google je razvio niz obrazovnih inicijativa, resursa i alata koji pomažu u promociji bezbjednosti za mlade na internetu. Jedna od njih je kampanja Budi sjajan na internetu organizovana oko digitalnog građanstva, kreirana u saradnji sa organizacijama kao što su ConnectSafely, Porodični institut za bezbjednost na internetu i koalicija Internet Keep Safe. Ova kampanja je usmjerena na mlade ljude uzrasta od 8 do 11 godina. Sadrži internetsku igru za mlade (Interland) koja podučava osnovama digitalne bezbjednosti i resurse za edukatore, poput digitalnog građanstva i bezbjednosnog plana i programa. Bezbjednosni plan i program nudi planove lekcija za pet ključnih tematskih područja kampanje, od kojih se jedno fokusira na sajber maltretiranje. Kao dodatak ovome Google je napravio kurs digitalnog građanstva i bezbjednosti na internetu za edukatore učenika svih starosnih grupa, pružajući dalju podršku za integrisanje digitalnog građanstva i bezbjednosnih aktivnosti u učionici. Google takođe nudi nekoliko programa koji pomažu mladima da se direktno uključe u napore na polju bezbjednosti na internetu i na polju digitalnog građanstva. Globalna inicijativa Web Rangers jedan je od takvih programa koji mlade podučava o bezbjednosti na internetu i podstiče ih da kreiraju sopstvene kampanje oko pozitivne i bezbjedne upotrebe interneta. Postoje i posebni programi za mlade za određene države, poput programa Internet Citizens i Internet Legends u Velikoj Britaniji, koje je pokrenuo Google.

Na **Evrovizijskoj razmjeni vijesti za mlade**, Evropska radiodifuzna unija okuplja 15 evropskih televizijskih kuća kako bi razmjenjivale programe, formate i rješenja na internetu i izvan njega. Posljednjih godina, podučavanje digitalne pismenosti i upozoravanje djece na rizike na internetu postali su ključni za njihove programe. Među najuspješnijim inicijativama posljednjih godina su oglasi na društvenim mrežama i vijesti prilagođene za djecu koje su proizveli Super i Ultra nytt pod NRK, norveškim javnim emiterom.

Dobre prakse: Strateška partnerstva

Kao dio projekta podržanog od Fonda za zaustavljanje nasilja nad djecom, Capital Humano y Social Alternativo je 2018. godine sklopio partnerstvo s kompanijom Telefónica, najvećim provajderom internetskih, kablovskih i telefonskih usluga u Peruu, sa 14.4 miliona korisnika, uključujući više od 8 miliona Movistar mobilnih korisnika.

Nekoliko aktivnosti je sprovedeno u okviru ovog plodnog partnerstva:

- **Virtuelni kurs o zaštiti djece na internetu** je razvijen od strane kompanije Telefónica uz tehničku podršku Capital Humano y Social Alternativo. Ovaj kurs je sada otvoreno dostupan na internet stranici Telefónice, a kompanija prati broj ljudi koji se upišu i uspješno završavaju kurs. Peruansko ministarstvo obrazovanja složilo se da će uključiti pristup ovom virtuelnom kursu putem svoje službene internet stranice.
- **Knjižica o bezbjednosti na internetu** napravljena je od strane Capital Humano y Social Alternativo, a kompanija Telefónica je distribuira u preko 300 mobilnih prodajnih centara. Cilj je podići svijest korisnika Telefónice o bezbjednosti na internetu i rizicima povezanim sa seksualnim iskorištavanjem i zlostavljanjem djece na internetu.
- **Interaktivnu igru o seksualnom iskorištavanju i zlostavljanju djece na internetu** razvila je kompanija Telefónica uz tehničku podršku Capital Humano y Social Alternativo, koju njeni korisnici mogu igrati dok čekaju svoje redove u trgovinama

Nadovezujući se na uspjeh sa Telefónicom, Capital Humano y Social Alternativo udružila se sa kompanijom **Econocable**, provajderom interneta i kablovskih usluga koji radi u udaljenim područjima u Peruu sa niskim prihodima.

3.5 Promovisanje digitalne tehnologije kao načina za povećanje građanskog angažmana

Član 13. Konvencije o pravima djeteta UN-a kaže da “dijete ima pravo na slobodu izražavanja; to pravo mora, nezavisno o granicama, uključivati slobodu traženja, primanja i širenja obavijesti i ideja svake vrste, usmeno ili pismeno, štampanjem, umjetničkim oblikovanjem ili putem bilo kojeg drugog sredstva prema izboru djeteta." Kompanije mogu ispuniti svoju dužnost poštovanja građanskih i političkih prava djece i mladih osiguravajući da tehnologija i primjena zakona i politika razvijenih za zaštitu djece i mladih od štete na internetu nemaju nenamjerne posljedice suzbijanja njihovog prava na učešće i izražavanje ili sprečavanje pristupa informacijama koje su važne za njihovu dobrobit. Neophodno je osigurati da sistemi provjere starosti ne ugrožavaju istinsku potrebu određenih starosnih grupa za pristup sadržajima koji su relevantni za njihov razvoj.

Istovremeno, preduzeća i IKT kompanije takođe mogu podržati prava djece i mladih pružajući mehanizme i alate za olakšavanje učešća mladih. Oni mogu naglasiti sposobnost interneta da olakša pozitivan angažman u širem građanskom životu, pokreće društveni napredak i utiče na održivost i otpornost zajednica, na primjer, učestvovanjem u socijalnim i ekološkim kampanjama i pozivanjem na odgovornost onih koji su odgovorni. Uz odgovarajuće alate i informacije, djeca i mladi su u boljoj poziciji da pristupe mogućnostima za zdravstvenu zaštitu, obrazovanje i zapošljavanje te da izraze svoja mišljenja i potrebe u školama, zajednicama i zemljama. Osposobljavaju se za pristup informacijama o svojim pravima i traženje informacija o stvarima koje ih lično pogađaju, poput njihovog seksualnog zdravlja, i o političkoj i vladinoj odgovornosti.

Kompanije takođe mogu ulagati u stvaranje internetskih iskustava primjerenih djeci i mladima i porodicama. One mogu podržati razvoj tehnologije i sadržaja koji podstiču i omogućavaju djeci i mladima da uče, stvaraju inovacije i prave rješenja. Uvijek bi trebali da imaju na umu bezbijednost po dizajnu u svojim proizvodima.

Pored toga, kompanije mogu proaktivno podržati prava djece i mladih radeći na uklanjanju digitalne podjele. Za učešće djece i mladih potrebna je digitalna pismenost
- sposobnost razumijevanja i interakcije u digitalnom svijetu. Bez ove mogućnosti, građani ne mogu učestvovati u mnogim društvenim funkcijama koje su postale digitalizovane, uključujući podnošenje prijava za porez, pružanje podrške političkim kandidatima, potpisivanje peticija na internetu, registraciju rođenja ili jednostavno nemaju pristup komercijalnim, zdravstvenim, obrazovnim ili kulturnim informacijama. Bez djelovanja, jaz između građana koji mogu pristupiti tim forumima i onih koji to ne mogu zbog nedostatka pristupa internetu ili digitalne pismenosti i dalje će se povećavati, što će ove posljednje dovesti u značajan nedostatak. Kompanije mogu podržati multimedijske inicijative za njegovanje digitalnih vještina koje djeci i mladima trebaju da bi bili samopouzdani, povezani i aktivno uključeni građani.[17] U mnogim zemljama digitalna i medijska pismenost i napori na uklanjanju digitalne podjele dio su misije javnih medijskih servisa posljednjih godina. Italijanski parlament, na primjer, predložio je da prioriteti nacionalnih emitera uključuju uklanjanje digitalne podjele i osiguranje zaštite djece izvan interneta i na internetu, primjer koji bi mogle slijediti druge zemlje.

[17] Primjere učešća mladih iz mobilne zajednice pogledajte ovdje.

Dobre prakse: Višeagencijska saradnja

Nedavno se Microsoft pridružio globalnoj kampanji Power of ZERO, koju vodi organizacija No Bully, čiji je cilj pomoći maloj djeci i odraslima koji brinu o njima, da nauče dobro koristiti digitalne tehnologije i da razviju glas, saosjećanje i inkluzivnost koji su srce digitalnog građanstva. Inicijativa nudi edukatorima male djece (kampanja je usmjerena na djecu uzrasta do 8 godina) i porodicama besplatan materijal za učenje kako bi pomogla maloj djeci da gaje "12 moći za dobro" (Moć Zerovih 12 životnih vještina ili "moći", za djecu da se uspješno kreću u online i offline svijetu, uključujući otpornost, poštovanje, inkluzivnost i kreativnost) i postavljaju im snažne temelje u ranom uzrastu.

4. Opšte smjernice za IKT kompanije

Tabela 1. daje široke smjernice za IKT kompanije za identifikaciju, sprječavanje i ublažavanje bilo kakvih negativnih uticaja proizvoda i usluga na prava djece i mladih, te za promociju pozitivne upotrebe IK tehnologija od strane djece i mladih.

Imajte na umu da neće svi koraci navedeni u Tabeli 1 biti prikladni za sve kompanije i usluge, niti se svi potrebni koraci za svaku uslugu nalaze u ovoj Tabeli. Opšte smjernice za IKT kompanije dopunjuju se kontrolnom listom po karakteristikama (vidi odjeljak 5) i obratno. Kontrolne liste po karakteristikama u Tabelama 2-5 ističu dodatne korake koji su najvažniji za pojedine usluge. Imajte na umu da se kontrolne liste po karakteristikama mogu preklapati i da više kontrolnih lista mogu biti relevantne za istu uslugu.

Tabela 1: Opšte smjernice za IKT kompanije

Razmatranja o integraciji prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja	IKT kompanije mogu da identifikuju, spriječe i ublaže negativne uticaje IK tehnologija na prava djece i mladih, i da identifikuju mogućnosti za podršku u napretku prava djece i mladih preduzimanjem sljedećih radnji:
	Osiguravanjem da određeni pojedinac i / ili tim budu imenovani odgovornim za ovaj proces i da ima pristup potrebnim internim i eksternim interesnim stranama. Davanjem ovlaštenja ovoj osobi ili timu da preuzmu vodeću ulogu u podizanju profila zaštite djece na internetu u cijeloj kompaniji.
	Razvijanjem politike zaštite i čuvanja djece i / ili integrisanjem posebnih rizika i mogućnosti koji se odnose na prava djece i mladih u opredjeljenja politike kompanije (npr. ljudska prava, privatnost, marketing i relevantni kodeksi ponašanja).
	Integrisanjem dubinske analize o pitanjima zaštite djece na internetu u postojeće okvire ljudskih prava ili procjene rizika (na nivou korporacije, proizvoda ili tehnologije i / ili države) kako bi se utvrdilo može li preduzeće ili IKT kompanije da svojim aktivnostima izaziva ili doprinosi negativnim uticajima ili da li se negativni uticaji mogu direktno pripisati njegovom poslovanju, proizvodima ili uslugama ili poslovnim odnosima.
	Prepoznavanjem uticaja na dječja prava različitih starosnih grupa kao rezultata poslovanja kompanije i dizajna, razvoja i uvođenja proizvoda i usluga, kao i mogućnosti za podršku pravima djece i mladih.

Razmatranja o integraciji prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja (nastavak)	Usvajanjem pristupa dječjoj zaštiti zasnovanoj na osnaživanju i obrazovanju. Uzimanjem u obzir prava deteta na zaštitu podataka, njihovog prava na privatnost i slobodu govora, istovremeno nudeći obrazovanje i smernice kroz usluge kompanije.
	Oslanjanjem na internu i eksternu stručnost i savjetovanje sa ključnim interesnim stranama, uključujući djecu i mlade, o mehanizmima za bezbjednost djece na internetu kako bi dobili stalne povratne informacije i smjernice o pristupima kompanije.
	U državama kojima nedostaju odgovarajući pravni okviri za zaštitu prava djece i mladih na privatnost i slobodu izražavanja, kompanije bi trebale osigurati da su politike i prakse u skladu sa međunarodnim standardima. Pogledati Rezoluciju Generalne skupštine Ujedinjenih nacija 68/167 o pravu na privatnost u digitalno doba.
	Osiguravanjem pristupa pravnom lijeku uspostavljanjem mogućnosti žalbi na operativnom nivou i kroz mehanizme prijavljivanja bilo kakvih kršenja prava djeteta (npr. materijal seksualnog zlostavljanja djece, neprimjeren sadržaj ili kontakt ili kršenje privatnosti).
	Imenovanjem rukovodioca politike zaštite djece ili druge određene osobe koja se može kontaktirati u vezi sa pitanjima zaštite djece na internetu. Ako je dijete u opasnosti od štete, rukovodilac politike zaštite djece treba odmah upozoriti odgovarajuće vlasti. Uredničke smjernice BBC-a (2019.), na primjer, određuju imenovanje rukovodioca politike zaštite djece, što se u javnim medijima smatra obaveznim.
Razvoj standarda IKT kompanija za zaštitu djece na internetu	Napraviti i primijeniti standarde za kompanije i IKT industriju za zaštitu djece i mladih, s obzirom na specifičnu industriju i karakteristike.
Razvoj standardnih postupaka za rukovanje materijalima seksualnog zlostavljanja djece	U saradnji sa vladom, organima za sprovođenje zakona, civilnim društvom i organizacijama linija za podršku, IKT kompanije imaju ključnu ulogu u borbi za suzbijanje materijala seksualnog zlostavljanja djece preduzimanjem sljedećih radnji:
	Zabraniti učitavanje, objavljivanje, prenos, deljenje ili stavljanje na raspolaganje sadržaja koji krši prava bilo koje strane ili krši bilo koji lokalni, državni, nacionalni ili međunarodni zakon.
	Komunicirati sa nacionalnim agencijama za sprovođenje zakona ili nacionalnim linijama za podršku kako bi prenijeli prijave materijala seksualnog zlostavljanja djece čim provajder sazna za njih. Osigurati da postoje interne procedure za usklađivanje odgovornosti za prijavljivanje prema lokalnim i međunarodnim zakonima. Kada kompanija posluje na tržištima sa manje razvijenim regulatornim nadzorom i nadzorom nad sprovođenjem zakona u vezi sa ovim pitanjem, ona može uputiti one koji žele podnijeti prijave na Međunarodno udruženje internetskih linija za podršku (INHOPE), gdje se može izvršiti prijava na bilo kojoj međunarodnoj liniji za podršku.

Razvoj standardnih postupaka za rukovanje materijalima seksualnog zlostavljanja djece **(nastavak)**	Uspostaviti interne procedure kako bi se osiguralo poštovanje lokalnih i međunarodnih zakona o borbi protiv materijala seksualnog zlostavljanja djece. Osnovati viši položaj ili tim posvećen integraciji ovih postupaka u organizaciju. Članovi IKT industrije bi zatim trebalo da izvještavaju o preduzetim radnjama i rezultatima koje je postigao ovaj tim u svom godišnjem izvještaju o korporaciji i održivosti. Kada nacionalni propisi ne pružaju dovoljnu zaštitu, IKT kompanije bi trebale poštovati, ali prevazići nacionalno zakonodavstvo i upotrijebiti svoje mogućnosti za lobiranje za zakonodavne promjene kako bi IKT kompanijama omogućili da se bore protiv materijala seksualnog zlostavljanja djece. Unutar organizacije treba uspostaviti viši položaj ili tim koji će biti posvećen integraciji ovih postupaka i praćenju operacija. Njihov rad bi trebao biti transparentno opisan u godišnjim izvještajima o korporaciji i održivosti i dostupan javnosti.
	Navesti da će preduzeće u potpunosti sarađivati u istragama organa za sprovođenje zakona u slučaju da se nezakonit sadržaj prijavi ili otkrije i da će se zabilježiti detalji u vezi sa kaznama kao što su novčane kazne ili ukidanje privilegija naplate.
	Koristiti uslove i odredbe za korisnike i / ili prihvatljive politike upotrebe za izričito navođenje stava kompanije o zloupotrebi njegovih usluga za čuvanje ili dijeljenje materijala seksualnog zlostavljanja djece i posljedicama bilo koje zloupotrebe.
	Razviti postupke obavještavanja, uklanjanja i izvještavanja koji omogućavaju korisnicima da prijave materijal seksualnog zlostavljanja djece ili neprimjeren kontakt i određeni profil / lokaciju gdje je otkriven. Uspostaviti izvještaj o pratećem postupku, dogovoriti se o procedurama za prikupljanje dokaza i brzo uklanjanje ili blokiranje pristupa materijalu seksualnog zlostavljanja djece. Osigurati da provajderi usluga, po potrebi, zatraže mišljenje stručnjaka (npr. nacionalnih tijela za borbu protiv materijala seksualnog zlostavljanja djece) prije uništavanja nezakonitog sadržaja. Osigurati da relevantne treće strane sa kojima je kompanija u ugovornom odnosu imaju uspostavljene isto tako snažne procese obavještavanja i uklanjanja.
	Trebaju biti spremne za rukovanje materijalom seksualnog zlostavljanja djece i da prijave slučajeve odgovarajućim vlastima. Ako odnos sa organima za sprovođenje zakona i nacionalnom linijom za podršku već nije uspostavljen, trebaju se angažovati da zajedno razvijaju procese.
	Raditi putem internih funkcija, kao što su briga o korisnicima, sprječavanje prevara i bezbjednost, kako bi se osiguralo da preduzeće može podnositi prijave za sumnju na nezakonit sadržaj direktno organima za sprovođenje zakona i linijama za podršku. U idealnom slučaju, to bi trebalo učiniti na način koji ne izlaže osoblje u prvom redu štetnom sadržaju niti ponovno pravi žrtvu od pogođenog djeteta / djece i mladih. Pozabaviti se situacijama u kojima osoblje može biti izloženo izopačenom materijalu, sprovesti politiku ili program za pružanje podrške za razvoj otpornosti, bezbjednosti i dobrobiti osoblja.

Razvoj standardnih postupaka za rukovanje materijalima seksualnog zlostavljanja djece (nastavak)	Uključiti politike zadržavanja i čuvanja podataka za podršku organima za sprovođenje zakona u slučaju krivičnih istraga kroz aktivnosti kao što je prikupljanje dokaza. Dokumentovanje prakse kompanije prilikom rukovanja materijalom seksualnog zlostavljanja djece, počevši od praćenja i nastavljajući se do konačnog prenosa i uništavanja sadržaja. U dokumentaciju uključiti spisak cijelog osoblja odgovornog za rukovanje materijalom.
	Promovisati mehanizme prijavljivanja materijala seksualnog zlostavljanja djece i osigurati da korisnici znaju kako podnijeti prijavu ako otkriju takav sadržaj. Ako je dostupna nacionalna linija za podršku, ponudite vezu do te linije za podršku sa korporativne internet stranice i sa bilo kojih relevantnih usluga sa sadržajima koje kompanija promoviše.
	Koristiti se svim relevantnim uslugama / skupovima podataka kako bi spriječili širenje poznatog sadržaja seksualnog zlostavljanja djece putem svojih usluga ili platformi.
	Redovno aktivno procjenjivati sav sadržaj hostiran na serverima kompanije, uključujući komercijalne (brendirane provajdere sadržaja ili one ugovorene sa trećim licima). Razmislite o upotrebi alata kao što su heš skeniranje poznatih slika seksualnog zlostavljanja djece, softver za prepoznavanje slika ili blokiranje internet adresa za borbu protiv materijala seksualnog zlostavljanja djece.
Stvaranje bezbjednijeg okruženja na internetu prilagođenog uzrastu	IKT kompanije mogu pomoći u stvaranju bezbjednijeg, ugodnijeg digitalnog okruženja za djecu i mlade svih uzrasta preduzimanjem sljedećih radnji:
	Usvojiti principe bezbjednosti i privatnosti po dizajnu u tehnologijama i uslugama kompanija i dati prioritet rješenjima koja smanjuju količinu podataka koji se odnose na djecu na minimum.
	Primijeniti dizajne prilagođene uzrastu u ponuđenim uslugama. Predstaviti djeci informacije o pravilima internet stranice na pristupačan način i primjereno njihovom uzrastu, pružajući odgovarajuću količinu detalja. Pored odredbi i uslova prilagođenih uzrastu i koji su pristupačni, IKT kompanije bi na sličan način trebale i jasno prenositi informacije, poput pravila i ključnih politika. One bi trebale da naglase prihvatljivo i neprihvatljivo ponašanje prilikom korištenja usluge, posljedice kršenja bilo kojih pravila, specifičnosti usluge i ono na šta korisnik pristaje prijavljivanjem. Takve informacije trebaju biti posebno usmjerene na mlade korisnike i njihove roditelje i staratelje.
	Koristiti uslove usluge ili uslove i odredbe kako biste skrenuli pažnju korisnicima na sadržaj na internetskim uslugama kompanije koji možda nije primjeren za sve uzraste. Uslovi i odredbe takođe treba da uključuju jasne mehanizme za prijavljivanje i postupanje u slučaju kršenja takvih pravila.

Stvaranje bezbjednijeg okruženja na internetu prilagođenog uzrastu **(nastavak)**	Razmotriti mogućnost pružanja mehanizama kao što su softver za roditeljsku kontrolu i drugi alati koji omogućavaju roditeljima i starateljima da upravljaju pristupom djeci internetskim resursima, istovremeno im pružajući smjernice o njihovoj odgovarajućoj upotrebi kako se ne bi kršila dječja prava. Oni uključuju liste za blokiranje / dozvolu pristupa, filtere sadržaja, nadzor upotrebe, upravljanje kontaktima i vremenska / programska ograničenja.
	Ponuditi jednostavne opcije roditeljskog nadzora koje roditeljima i starateljima omogućavaju ograničavanje određenih usluga i sadržaja kojima djeca mogu pristupiti kada koriste elektronske uređaje. Ova ograničenja mogu uključivati kontrole na nivou interneta, uređaja i kontrole aplikacija. S obzirom da ovo ima ogromne implikacije na djetetovu sposobnost da unaprijedi svoje digitalne vještine i na smanjivanje negovih mogućnosti na internetu, ove bi kontrole trebale biti dizajnirane za vrlo malu djecu u skladu sa njihovim razvojnim kontekstom i sa odgovarajućim smjernicama za roditelje.
	Tamo gdje je to moguće, promovisati nacionalne službe podrške koje roditelji i staratelji mogu koristiti za prijavljivanje kršenja prava i traženje podrške u slučaju zlostavljanja ili iskorištavanja.
	Izbjegavati štetne ili neprimjerene reklamne sadržaje na internetu i uspostaviti obavezu za provajdere usluga da otkrivaju klijente sa sadržajem koji je namijenjen odrasloj publici i može biti štetan za djecu i mlade. Štetno oglašavanje takođe može uključivati oglašavanje hrane i pića koja sadrže puno masti, šećera ili soli. Uskladiti poslovne prakse sa propisima i savjetima o marketingu i oglašavanju za djecu i mlade. Pratiti gdje, kada i kako djeca i mladi mogu naići na potencijalno štetne reklamne poruke namijenjene drugom segmentu tržišta.
	Osigurati da se politike prikupljanja podataka pridržavaju relevantnih zakona koji se tiču privatnosti djece i mladih, uključujući razmatranje da li je potreban pristanak roditelja prije nego što komercijalna preduzeća mogu prikupiti lične podatke od djeteta ili o djetetu.
	Prilagoditi i primijeniti povišena podrazumijevana podešavanja privatnosti za prikupljanje, obradu, skladištenje, prodaju i objavljivanje ličnih podataka, uključujući informacije u vezi sa lokacijom i navike pregledanja, prikupljene od osoba mlađih od 18 godina. Podrazumijevana podešavanja privatnosti i informacije o važnosti privatnosti trebale bi odgovarati uzrastu korisnika i prirodi usluge.
	Primijeniti tehničke mjere, kao što su odgovarajući alati za roditeljsku kontrolu, bezbjednost po dizajnu, različita iskustva za različite uzraste, sadržaj zaštićen lozinkom, liste za blokiranje / dozvolu pristupa, kontrole kupovine / vremena, funkcije odjave, filtriranje i moderiranje, kako bi se spriječio pristup i izloženost maloljetnika neprimjerenom sadržaju ili uslugama. Primijeniti tehnologiju koja može identifikovati uzrast korisnika i predstaviti im verziju aplikacije koja odgovara uzrastu. Za sadržaj ili usluge osjetljive na uzrast, interesne strane u IKT industriji bi trebale preduzeti korake za provjeru starosti korisnika. Tamo gdje je moguće, koristiti provjeru starosti da bi ograničili pristup sadržaju ili materijalu koji je, bilo zakonom ili politikom, namijenjen samo osobama starijim od određenog uzrasta. Kompanije bi takođe trebale prepoznati potencijal zloupotrebe takvih tehnologija sa ciljem ograničavanja prava djece i mladih na slobodu izražavanja i pristupa informacijama ili ugrožavanja njihove privatnosti.

Stvaranje bezbjednijeg okruženja na internetu prilagođenog uzrastu **(nastavak)**	Osigurati da su sadržaj i usluge koji nisu prikladni za korisnike svih starosnih grupa: • klasifikovani u skladu sa nacionalnim standardima i kulturnim normama; • u skladu sa postojećim standardima u ekvivalentnim medijima; • identifikovani sa istaknutim opcijama prikaza za kontrolu pristupa; • u ponudi zajedno sa provjerom starosti, gdje je to moguće i uz jasne uslove koji se odnose na brisanje bilo kojih podataka koji se mogu koristiti za ličnu identifikaciju koji su dobijeni kroz postupak provjere. Na primjer, s obzirom na medijske standarde, sva regulatorna tijela za medije postavljaju niz zahtjeva koji se odnose na sadržaj prilagođen uzrastu, a provajderi interneta moraju da prilagode spremišta i da primijene smjernice na svoju ponudu sadržaja. Pogledati, Ofcom u Ujedinjenom Kraljevstvu, CSA u Francuskoj i AGCOM u Italiji.
	Ponuditi jasne alate za prijavljivanje i razviti prateći postupak na prijavu o neprimjerenom sadržaju, kontaktima i zloupotrebama, a korisnicima usluga pružiti detaljne povratne informacije o procesu koji se odnosi na prijavu.
	Osigurati predmoderaciju interaktivnih prostora dizajniranih za djecu i mlade na načine koji se podudaraju sa pravima djece na privatnost i njihovim razvojnim kapacitetima. Aktivna moderacija može podstaknuti atmosferu u kojoj nasilje i uznemiravanje nisu prihvatljivi. Neprihvatljivo ponašanje uključuje: • objavljivanje neugodnih ili prijetećih komentara na nečijem profilu; • otvaranje lažnih profila ili internet sajtova mržnje radi ponižavanja žrtve; • slanje lančanih poruka i priloga sa štetnom namjerom; • hakovanje nečijeg profila radi slanja uvrjedljivih poruka drugima.
	Preduzeti posebne mjere opreza sa članovima osoblja ili saradnicima koji rade sa djecom i mladima, za koje može biti potrebna prethodna provjera kaznene evidencije kod policijskih vlasti.
	Bilo koji incident sumnje na vrbovanje odmah uputite internetskom ili interaktivnom izvršnom rukovodećem timu koji je odgovoran za prijavljivanje odgovarajućim vlastima: • prijaviti vrbovanje izvršnom rukovodećem timu i imenovanom rukovodiocu politike zaštite djece, gdje je to moguće; • omogućiti korisnicima da direktno prijave nadležnim organima slučajeve vrbovanja; • uspostaviti mogućnost direktnog kontakta putem adresa e-pošte radi upozorenja i prijavljivanja.
	U svakom trenutku dati prioritet bezbjednosti i dobrobiti djeteta. Djelovati uvijek u profesionalnim granicama i osigurati da je svaki kontakt sa djecom važan za uslugu, program, događaj, aktivnost ili projekat. Nikada ne preuzimajte isključivu odgovornost za dijete. Ako je djetetu potrebna njega, upozoriti roditelja, staratelja ili pratioca. Slušati i poštovati djecu u svako doba. Ako se neko ponaša neprimjereno u blizini djece, prijavite to ponašanje lokalnom kontaktu za zaštitu djece.

Stvaranje bezbjednijeg okruženja na internetu prilagođenog uzrastu **(nastavak)**	Uspostaviti jasan skup pravila koja su na vidnom mjestu i oslikavaju ključne tačke iz uslova usluge i smjernica prihvatljive upotrebe. Jezikom koji je razumljiv za korisnike ova pravila bi trebala da definišu: • prirodu usluge i šta se očekuje od njenih korisnika; • šta je prihvatljivo a šta nije u smislu sadržaja, ponašanja i jezika, kao i zabrana nezakonite upotrebe; • posljedice proporcionalne kršenju, na primjer, prijavljivanje organima za sprovođenje zakona ili suspenzija korisničkog profila.
	Olakšati korisnicima da prijave zabrinutost zbog zloupotrebe službi za brigu o korisnicima, putem uspostavljenih standardnih i pristupačnih postupaka za rješavanje različitih problema, kao što je primanje neželjenih komunikacija (npr. neželjene SMS poruke).
	Biti transparentan i pružiti korisnicima jasne informacije o prirodi ponuđenih usluga, na primjer: • vrsta sadržaja / usluge i troškovi; • minimalna starosna granica potrebna za pristup; • dostupnost roditeljskog nadzora, uključujući ono što kontrole pokrivaju (npr. internet) ili ne pokrivaju (npr. Wi-Fi) i obuku o tome kako ih koristiti; • vrsta prikupljenih korisničkih podataka i kako se koriste.
	Promovisati nacionalne službe podrške koje omogućavaju djeci i mladima da prijave i potraže podršku u slučaju zlostavljanja ili iskorištavanja (pogledati, na primjer, Child Helpline International).
Edukacija djece, roditelja i edukatora o bezbjednosti djece i njihovoj odgovornoj upotrebi IK tehnologija	IKT kompanije mogu dopuniti tehničke mjere obrazovnim aktivnostima i aktivnostima osnaživanja preduzimanjem sljedećih radnji:
	Jasnog opisa dostupnog sadržaja i odgovarajuće roditeljske kontrole ili porodičnih bezbjedonosnih postavki. Učiniti jezik i terminologiju dostupnim, vidljivim, jasnim i relevantnim za sve korisnike, uključujući djecu, roditelje i staratelje, posebno u odnosu na odredbe i uslove, troškove uključene u upotrebu sadržaja ili usluga, politike privatnosti, bezbjednosne informacije i mehanizme prijavljivanja.
	Obučiti korisnike o načinu rješavanja problema vezanim za upotrebu interneta, uključujući neželjenu poštu, krađu podataka i neprimjeren kontakt, poput maltretiranja i vrbovanja, i opisati koje radnje korisnici mogu preduzeti i kako mogu iznijeti zabrinutost zbog neprimjerene upotrebe.
	Uspostaviti mehanizme i edukovati roditelje da se uključe u IKT aktivnosti svoje djece i mladih, posebno onih koji imaju mlađu djecu, tako što će, na primjer, omogućiti roditeljima da pregledaju postavke privatnosti djece i mladih.
	Sarađivati sa vladom i edukatorima kako bi izgradili kapacitete roditelja za podršku i razgovor sa svojom djecom i mladima o tome da budu odgovorni digitalni građani i korisnici IK tehnologija.

Edukacija djece, roditelja i edukatora o bezbjednosti djece i njihovoj odgovornoj upotrebi IK tehnologija **(nastavak)**	Na osnovu lokalnog konteksta, treba obezbijediti obrazovne materijale za upotrebu u školama i domovima kako bi poboljšali upotrebu IK tehnologija kod djece i mladih i razvili kritičko razmišljanje kako bi im omogućili da se ponašaju bezbjedno i odgovorno kada koriste usluge IK tehnologija.
	Podržite korisnike širenjem smjernica o porodičnoj bezbjednosti na internetu koje podstiču roditelje i staratelje da: • se upoznaju sa proizvodima i uslugama koje koriste djeca i mladi; • osiguraju umjerenu upotrebu elektronskih uređaja od strane djece i mladih kao dijela zdravog i uravnoteženog načina života; • pažljivo obrate pažnju na ponašanje djece i mladih kako bi utvrdili promjene koje bi mogle ukazivati na sajber zlostavljanje ili uznemiravanje.
	Pružiti roditeljima potrebne informacije da bi razumjeli kako njihova djeca i mladi koriste usluge IK tehnologija, rješavali probleme u vezi sa štetnim sadržajem i ponašanjem i bili spremni da uče djecu i mlade odgovornoj upotrebi. To se može olakšati upotrebom alata i interakcijom sa školskim distriktima za pružanje nastavnih planova i programa za djecu i obrazovnih materijala za roditelje u vezi sa bezbjednosti na internetu.
Korištenje tehnološkog napretka za zaštitu i obrazovanje djece	Vještačka inteligencija koja čuva privatnost, a koja razumije tekstove, slike, razgovore i kontekst, može otkriti i riješiti čitav niz šteta i prijetnji na internetu i koristiti te informacije za osnaživanje i obrazovanje djece da se nose s njima. Kada se koristi internet u okruženju pametnih uređaja, oni mogu zaštititi podatke i privatnost mladih, a istovremeno im dati podršku.
	Javni servis i nacionalni mediji mogu igrati ključnu ulogu kroz svoje programske ponude (offline i online) za obrazovanje roditelja i djece i njihovo osvješćivanje o rizicima i mogućnostima internetskog svijeta
Promovisanje digitalne tehnologije kao načina za povećanje građanskog angažmana	IKT kompanije mogu ohrabriti i osnažiti djecu i mlade podržavajući njihovo pravo na učešće kroz sljedeće radnje:
	Pružanje informacija o usluzi kako bi istakli koristi koje djeca ostvaruju ponašajući se primjerno i odgovorno, poput upotrebe usluge u kreativne svrhe.
	Uspostaviti pisane postupke koji osiguravaju dosljedno sprovođenje politika i procesa koji štite slobodu izražavanja za sve korisnike, uključujući djecu i mlade, kao i dokumentaciju o usklađenosti sa tim politikama.

Promovisanje digitalne tehnologije kao načina za povećanje građanskog angažmana (nastavak)	Izbjegavajte prekomjerno blokiranje legitimnog i razvojno odgovarajućeg sadržaja. Da se zahtjevi i alati za filterisanje ne bi zloupotrebljavali za ograničavanje pristupa informacijama djeci i mladima, obezbijediti transparentnost blokiranog sadržaja i uspostaviti postupak za korisnike koji prijavljuju nenamjerno blokiranje. Ovaj postupak trebao bi biti dostupan svim potrošačima, uključujući webmastere. Svaki postupak izvještavanja treba pružiti jasne, odgovorne i procijenjene uslove pružanja usluge.
	Razviti online platforme koje promovišu pravo djece i mladih na izražavanje; olakšati njihovo učešće u javnom životu; i podsticati njihovu saradnju, preduzetništvo i građansko učestvovanje.
	Razviti obrazovni sadržaj za djecu i mlade koji podstiče učenje, kreativno razmišljanje i rješavanje problema.
	Promovirsati digitalnu pismenost, izgradnju kapaciteta i IKT vještine kako bi se djeca i mladi, posebno oni u ruralnim područjima i područjima sa nedovoljno visokim nivoom usluga, opremili za korištenje IKT resursa i potpuno sigurno učešće u digitalnom svijetu.
	Sarađujte sa lokalnim civilnim društvom i vladom na nacionalnim i lokalnim prioritetima za širenje univerzalnog i ravnopravnog pristupa IKT-ima, platformama i uređajima kao i osnovnoj infrastrukturi za podršku istih.
	Obavijestite i uključite kupce, uključujući roditelje, njegovatelje, djecu i mlade, o ponuđenim uslugama, poput: • vrsta sadržaja i odgovarajuća roditeljska kontrola; • mehanizmi prijavljivanja slučajeva pogrešne upotrebe, zloupotrebe i neprimjerenog ili nezakonitog sadržaja; • postupci praćenja izvještaja; • vrste usluga koje su starosno ograničene; • sigurno i odgovorno korištenje interaktivnih usluga „vlastitog brenda“.
	Bavite se širim pitanjima u vezi sa sigurnim i odgovornim digitalnim građanstvom, na primjer internetskom reputacijom i digitalnim otiskom, štetnim sadržajem i njegom. Razmislite o partnerstvu sa lokalnim stručnjacima, poput dječjih nevladinih organizacija, dobrotvornih organizacija i roditeljskih grupa, kako biste pomogli oblikovati poruku kompanije i imali željenu publiku.
	Ako kompanija već radi s djecom ili školama, na primjer, kroz programe korporativne društvene odgovornosti, istražite mogućnost da se ovaj angažman proširi na obrazovanje i interakciju sa djecom i mladima kao i na edukatore o porukama u vezi sa zaštitom djece na internetu.
Investiranje u digitalno istraživanje	Uložite u istraživanje zasnovano na dokazima i u dubinsku analizu tehnologija, uticaj tehnologija na djecu, razmatranje zaštite djece i prava djeteta s obzirom na digitalno okruženje, integrisanje online sistema zaštite u usluge koje koriste djeca i mladi i bolje razumijevanje koje vrste intervencija su najefikasnije u poboljšanju dječijih online iskustava.

Tipologija IKT kompanija

Iako su ove smjernice Međunarodne unije za telekomunikacije usmjerene na IKT industriju u cjelini, važno je prepoznati da se usluge koje pružaju IKT kompanije, način njihovog rada, regulatorne šeme u okviru kojih funkcionišu i predmet i opseg njihovih ponuda veoma razlikuju. Bilo koja tehnološka kompanija čiji su proizvodi i usluge usmjereni direktno ili indirektno na djecu može imati koristi od ranije navedenih opštih principa i može se prilagoditi na osnovu svog specifičnog područja djelovanja. Osnovna ideja je podržati i voditi IKT industriju u preduzimanju pravih mjera za bolju zaštitu djece na internetu od opasnosti nanošenja štete, istovremeno osnažujući djecu da se kreću online svijetom na najbolji mogući način. Tipologija u nastavku će pomoći da se pruži jasnije razumijevanje nekih iz ciljne publike i kako se isti uklapaju u kontrolne liste u sljedećem odjeljku. Treba napomenuti da su ovo samo neki specifični primjeri kategorija i da nisu konačni:

(a) Provajderi internetskih usluga, uključujući fiksne širokopojasne usluge ili usluge mobilnih mrežnih operatera: iako ovo obično odražava usluge koje se pružaju na dugoročnijoj bazi pretplaćenim kupcima, moglo bi se proširiti i na preduzeća koja pružaju besplatan ili plaćen javni WI -FI žarišta.

(b) Društvene mreže odnosno platforme za razmjenu poruka i platforme za online igre.

(c) Proizvođači hardvera i softvera, poput dobavljača ručnih uređaja, uključujući mobilne telefone, igraće konzole, kućne uređaje zasnovane na glasovnoj pomoći, Internet stvari i pametne dječje igračke povezane s Internetom.

(d) Kompanije koje pružaju digitalne medije (kreatori sadržaja, omogućavanje pristupa ili hosting sadržaja).

(e) Kompanije koje pružaju usluge prenosa, uključujući prenose uživo.

(f) Kompanije koje nude usluge digitalnog skladištenja datoteka, dobavljači usluga u oblaku.

5. Kontrolna lista po karakteristikama

Ovo poglavlje dopunjuje prethodni opšti popis za industriju nudeći preporuke za preduzeća koja pružaju usluge sa specifičnim karakteristikama za poštivanje i podršku dječijih prava na mreži. Sljedeće kontrolne liste za određene karakteristike navode načine dopunjavanja zajedničkih principa i pristupa predstavljenih u Tabeli 1 budući da oni važe za različite usluge te bi ih stoga trebalo uzeti u obzir kao dodatak koracima iz Tabele 1.

Ovde istaknute karakteristike se presijecaju i nekoliko kontrolnih lista specifičnih za karakteristike može biti relevantno za istu kompaniju.

Sljedeće kontrolne liste su organizovane i pozivaju se na iste ključne oblasti kao i opšte smjernice u Tabeli 1. Svaka lista za provjeru karakteristika razvijena je sa ključnim saradnicima i zbog toga postoje manje razlike u tabelama.

5.1 Karakteristika A: Obezbijediti povezivanje, usluge skladištenja podataka i hostinga

Pristup internetu je osnovni za ostvarivanje dječjih prava, a povezanost može djeci otvoriti čitav svijet. Provajderi usluga povezivanja, skladištenja podataka i hostinga imaju ogromne mogućnosti da u svoje ponude za djecu i mlade ugrade sigurnost i privatnost. Ova funkcija je između ostalog namijenjena mobilnim operaterima, provajderima internet usluga, sistemima za skladištenje podataka i uslugama hostinga.

Mobilni operateri omogućavaju pristup internetu i nude niz mobilnih usluga prenosa podataka. Mnogi operateri su se već prijavili na kodekse prakse zaštite djece na internetu i nude niz alata i informativnih izvora radi podrške svojoj posvećenosti zaštiti djece na internetu.

Većina provajdera internetskih usluga djeluje i kao kanal koji pruža pristup internetu i sa interneta i kao skladište podataka putem svojih usluga hostinga, keš memorisanja i skladištenja. Kao rezultat toga, oni su primarno odgovorni za zaštitu djece na internetu.

Pristup internetu na javnim mjestima

Sve je uobičajenije da opštine, trgovci, transportne kompanije, lanci hotela i druga preduzeća i organizacije pružaju pristup internetu putem Wi-Fi i hot-spotova. Takav pristup je obično besplatan ili se pruža uz minimalne troškove, a ponekad uz minimalne formalnosti prilikom prijave kao javna usluga ili od strane kompanije da privuče kupce u svoje prostorije ili navede više ljudi da koriste njene usluge.

Promovisanje Wi-Fi mreže je efkasan način da se obezbijedi dostupnost interneta u određenom području. Međutim, treba voditi računa kada je takav pristup omogućen u javnim prostorima u kojima je vjerovatno da će djeca redovno da borave. Korisnici moraju imati na umu činjenicu da Wi-Fi signali mogu biti dostupni prolaznicima, a korisnički podaci ugroženi. Zbog toga provajder Wi-Fi mreže neće uvijek biti u mogućnosti da podrže ili nadziru upotrebu internet konekcije koju je isporučio i korisnici zato moraju preduzeti mjere predostrožnosti da izbjegavaju dijeljenje osjetljivih informacija putem javno dostupne Wi-Fi mreže.

U javnim prostorima, provajderi Wi-Fi mreže će možda razmisliti o uvođenju dodatnih mjera za zaštitu djece i mladih, kao što su:

- Proaktivno blokiranje pristupa web adresama za koje se zna da sadrže sadržaj koji je neprikladan za široku publiku, pored njihovih napora da blokiraju pristup materijalu seksualnog zlostavljanja djece.
- Uvrštavanje klauzula u odredbe i uslove upotrebe kojima se zabranjuje upotreba Wi-Fi usluga za pristup ili prikazivanje bilo kojeg materijala koji je možda neprikladan u okruženju u kome borave djeca. Odredbe i uslovi takođe trebaju sadržavati jasne mehanizme u vezi sa posljedicama kršenja takvih pravila.
- Preduzimanje svih mjera za zaštitu od neovlaštenog pristupa, što za rezultat može imati manipulaciju ili gubitak ličnih podataka.
- Instaliranje filtera na Wi-Fi sistem radi podrške primjeni pravila o neprikladnom materijalu.
- Obezbijeđenje procedura i softvera za putokaz i nuđenje opcione roditeljske kontrole koja se odnosi na pristup djece i mladih internetskim sadržajima.

Dobra praksa: Propisi o telekomunikacijama većine država članica Evropske unije predviđaju, na primjer, da pristup mreži mora biti identifikovan putem pojedinačnih SIM kartica ili drugih alata za identifikaciju.

kojenude

Tabela 2 sadrži smjernice za provajdere usluga povezivanja, skladištenja podataka i hosting usluga o radnjama koje mogu preduzeti u cilju poboljšanja dječje online zaštite i dječjeg učešća.

Tabela 2: Kontrolna lista zaštite djece na internetu za Karakteristiku A: Obezbijediti uređaje za povezivanje, skladištenje i hosting podataka

Uvrštavanje pitanja prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja	Provajderi usluga povezivanja, skladištenja podataka i hostinga mogu da identifikuju, spriječe i ublaže negativne učinke IK tehnologija na prava djece i mladih i da identifikuju mogućnosti za podršku napretku djece i mladih.
	Vidi opšte smjernice u Tabeli 1.
Razvoj standardnih procesa radi rješavanja problema materijala seksualnog zlostavljanja djece	U saradnji sa vladom, organima za sprovođenje zakona, civilnim društvom i organizacijama SOS servisa, provajderi usluga povezivanja, skladištenja podataka i hosting usluga mogu igrati ključnu ulogu u borbi protiv materijala seksualnog zlostavljanja djece preduzimanjem sljedećih radnji:
	Saradnja sa vladom, organima za sprovođenje zakona, civilnim društvom i organizacijama SOS servisa u borbi protiv materijala seksualnog zlostavljanja djece i radi prijavljivanja slučajeva odgovarajućim organima. Ako saradnja sa policijom i SOS telefon za pomoć još nije uspostavljen, angažujte se na zajedničkom uspostavljanju saradnje.
	Provajderi usluga povezivanja, skladištenja podataka ili hostinga mogu takođe izvršiti obuku policije iz oblasti IK tehnologija.
	Ako kompanija posluje na tržištima sa manje razvijenim pravnim i zakonskim nadzorom ovog pitanja, ista može uputiti one koji žele podnijeti prijave na Međunarodno udruženje operatera internet mehanizama za prijave INHOPE (International Association of Internet Hotlines) Gdje se prijave mogu podnijeti kod bilo kog međunarodnog internet mehanizma za prijave.
	Razmislite o postavljanju međunarodno priznatih popisa za blokiranje URL-ova ili web lokacija koje su kreirale odgovarajuća tijela (npr. Nacionalna agencija za provođenje zakona ili vruća linija za prijavljivanje, Cybertip Canada, Interpol, IWF), kako bi korisnicima otežali pristup identifikovanom zlostavljačkom materijalu.
	Razviti postupke obavještavanja, uklanjanja i prijavljivanja te povezati prijave zloupotrebe sa tim procesima putem sporazuma o javnoj službi o postupku odgovora i vremenu uklanjanja.
	Pogledajte, na primjer, UNICEF-ov i GSMA vodič o politikama i praksi obavještavanja i uklanjanja.
	Uspostavite mehanizam prijavljivanja sa jasnim informacijama o njegovoj upotrebi, na primjer, davanjem smjernica o ilegalnom sadržaju i ponašanju koje treba prijaviti i pojašnjavanjem toga koji se materijali ne mogu priložiti uz izvještaj kako bi se izbjegla dalja distribucija na internetu.

Razvoj standardnih procesa radi rješavanja problema materijala seksualnog zlostavljanja djece (*nastavak*)	Podržite provođenje zakona u slučaju krivičnih istraga kroz aktivnosti kao što je prikupljanje dokaza. Koristite uslove i odredbe usluge da biste posebno zabranili upotrebu usluga za skladištenje, dijeljenje ili distribuciju materijala seksualnog zlostavljanja djece. Obavezno navedite da ovi uslovi jasno navode da se materijal seksualnog zlostavljanja djece neće tolerisati. Obavezno navedite da u uslovima usluge i odredbama navodi da će kompanija u potpunosti sarađivati u krivičnim istragama u slučaju otkrivanja ili prijave materijala seksualnog zlostavljanja djece.
	Trenutno postoje dva rješenja za prijavljivanje materijala seksualnog zlostavljanja djece na internetu na nacionalnom nivou: vruće linije i portali za prijavljivanje. Potpunu ažurnu listu svih postojećih telefonskih linija i portala možete pronaći na web stranici INHOPE. Vruće linije: Ako nacionalna vruća linija nije dostupna, potražite mogućnosti za uspostavljanje iste (pogledajte Vodič za vruće linije GSMA INHOPE za niz opcija, uključujući rad s INHOPE i Fondacijom INHOPE. Dostupna je interaktivna verzija GSMA INHOPE vodiča koja sadrži smjernice o tome kako razviti interne procese za osoblje za brigu o klijentima koje će podnositi izvještaje sumnjivog sadržaja policiji i mreži INHOPE. Portalii za prijavljivanje: IWF nudi rješenje portala za prijavljivanje koje omogućava korisnicima interneta u zemljama i zemljama bez vrućih linija da direktno IWF-u prijavljuju slike i videozapise za koje sumnjaju da mogu predstavljati seksualno zlostavljanje djece i to putem posebne mrežne stranice portala.
	Za provajdere usluga povezivanja, skladištenja podataka i hosting usluga čije usluge uključuju neku vrstu hostinga sadržaja, potrebno je imati uspostavljene postupke obavještavanja i uklanjanja.
Stvaranje bezbjednijeg i starosno prikladnog digitalnog okruženja	Provajderi usluga internet konekcije, skladištenja podataka i hostinga mogu pomoći u stvaranju sigurnijeg, ugodnijeg digitalnog okruženja za djecu svih uzrasta preduzimanjem sljedećih radnji:
	Provajderi usluga skladištenja/hostinga podataka trebali bi razmotriti predstavljanje funkcije prijavljivanja na svim web stranicama i servisima kao i razviti i dokumentovati jasne procese za brzo upravljanje izvještajima o zloupotrebi ili drugim kršenjima uslova i odredbi.
	Internet provajderi bi trebalo da ponude tehničku kontrolu vlastitog brenda ili da označe dostupnost alata koje su kreirali specijalizovani provajderi usluga koji su primjereni ponuđenim uslugama, a krajnji korisnici ih mogu lako primijeniti i ponuditi mogućnost blokiranja ili filterisanja pristupa internetu putem korporativne mreže. Obezbijedite odgovarajuće mehanizme za provjeru starosti ako kompanija nudi sadržaj ili usluge (uključujući usluge vlastitog brenda ili usluge treće strane koje kompanija promoviše), koje su legalne ili odgovarajuće za odrasle korisnike (npr. određene nagradne igre, lutrije).

Edukacija djece, roditelja i nastavnika o dječjoj bezbjednosti i njihovoj odgovornoj upotrebi IK tehnologija	Provajderi usluga povezivanja, skladištenja podataka i hostinga trebali bi ponoviti ključne poruke iz odredbi i uslova iz smjernica zajednice napisanih na jeziku prilagođenom korisnicima da podrže djecu i njihove roditelje i staratelje. U okviru same usluge, u trenutku prenošenja sadržaja, uvrstiti podsjetnike na teme kao što je vrsta sadržaja koja se smatra neprikladnom.
	Pružite djeci i mladima informacije o bezbjednijoj upotrebi Interneta. Razmotrite kreativne načine za promociju ključnih poruka, kao što su sljedeće: "Nikada ne dijelite nikakve kontakt informacije sa nepoznatim licima, uključujući vašu fizičku lokaciju i telefonski broj. „Nikada nemojte pristati da se sami sastanete sa nekim koga ste upoznali na mreži bez prethodnog savjetovanja sa odraslom osobom. Uvijek recite pouzdanom prijatelju gdje se nalazite " „Ne odgovarajte na maltretiranje, nepristojne ili uvredljive poruke. „Ali sačuvajte dokaze - ne brišite poruku. " "Recite odrasloj osobi ili prijatelju od povjerenja ako vam je zbog nečega ili nekoga neprijatno." “Nikada ne dajte lozinku ili korisničko ime naloga! Imajte na umu da drugi ljudi na mreži mogu davati lažne podatke da bi vas uvjerili da podijelite svoje privatne podatke. "
	Provajderi usluga se mogu udružiti s organizacijama koje su u dobrom položaju radi edukacije i podrške djecu o sigurnijoj upotrebi interneta i o srodnim pitanjima. Pogledajte International Helpline za djecu i praktični vodič za GSMA za dječje linije za podršku i mobilne operatere: Zajednički rad na zaštiti dječjih prava.
Promovisanje digitalne tehnologije kao načina za povećanje civilnog angažmana	*Vidi opšte smjernice u Tabeli 1.*

5.2 Karakteristika B: Ponuditi organizovani digitalni sadržaj

Internet pruža sve vrste sadržaja i aktivnosti, od kojih su mnogi namijenjeni djeci i mladima. Servisi koji nude profesionalno uređen sadržaj imaju ogromne mogućnosti da u svoje ponude za djecu i mlade ugrade sigurnost i privatnost.

Ova usluga se odnosi na preduzeća koja kreiraju vlastiti sadržaj kao i na ona koja omogućavaju pristup digitalnom sadržaju. Između ostalog, ovo se odnosi na usluge streaminga vijesti i multimedije, nacionalnu i javnu radiodifuziju i industriju igara na sreću.

Tabela 3 sadrži smjernice za provajdere usluga koje nude profesionalno uređen sadržaj o politikama i radnjama koje mogu preduzeti u cilju poboljšanja dječje online zaštite i dječjeg učešća.

Tabela 3: Kontrolna lista zaštite djece na internetu za Karakteristiku B: Ponuditi organizovani digitalni sadržaj

Uvrštavanje pitanja prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja	Servisi koji nude profesionalno uređen sadržaj mogu da pomognu da se identifikuju, spriječe i ublaže negativni uticaji IK tehnologija na prava djece i mladih i da identifikuju mogućnosti za podršku napretku djece i mladih preduzimanjem sljedećih radnji:
	Razviti politike koje štite dobrobit djece i mladih koji doprinose sadržajima na mreži kako bi se uzela u obzir fizička i emocionalna dobrobit i dostojanstvo lica mlađih od 18 godina koje su uključena u programe, filmove, igre, vijesti itd, bez obzira na pristanak koji je mogao dati roditelj ili drugo odraslo lice.
Razvijanje standardnih procesa za borbu protiv materijala seksualnog zlostavljanja djece	U saradnji sa državom, policijom, civilnim društvom i organizacija vrućih linija za podršku, kompanije koje nude profesionalno uređen digitalni sadržaj mogu igrati ključnu ulogu u borbi protiv MSZD putem sljedećih aktivnosti: U slučajevima MSZD, na primjer putem funkcija "komentarisanja" ili "pregleda", pri čemu korisnici imaju kapacitet za učitavanje sadržaja, osoblje bi trebalo da kontaktira izvršni rukovodeći tim odgovoran za prijavljivanje takvog materijala odgovarajućim organima. Pored toga, potrebno je: • odmah upozoriti nacionalne agencije za provođenje zakona; • upozoriti rukovodstvo agencije i prijaviti materijal menadžeru politike zaštite djece; • kontaktirati službu interne istrage telefonom ili e-poštom sa detaljima incidenta i zatražiti savjet; • prije brisanja materijala, skladištenja u zajednički prostor ili prosljeđivanja pričekajte savjet nadležne agencije.
	• implementirati brzu i efikasnu strategiju eskalacije ako je materijal seksulnog zlostavljanja djece objavljen ili se sumnja na nezakonito ponašanje. U tu svrhu: • ponuditi korisnicima jednostavan i lako dostupan način upozoravanja proizvođača sadržaja na kršenje bilo kojih pravila online zajednice; • ukloniti sadržaj kojim se krše pravila; • ponuditi korisnicima jednostavan i lako dostupan način upozoravanja proizvođača sadržaja na kršenje bilo kojih pravila online zajednice; • ukloniti sadržaj kojim se krše pravila; • prije slanja profesionalno uređenog sadržaja sa starosnim ograničenjem na društvene mreže, pripazite na uslove i odredbe web stranice. Pratite minimalne starosne zahtjeve na različitim stranicama za društveno umrežavanje. • odredbe i uslovi svakog internetskog prostora trebaju takođe sadržavati jasne mehanizme izvještavanja o kršenju takvih pravila.

Razvoj standardnih procesa radi rješavanja problema materijala seksualnog zlostavljanja djece

Ako je materijal identifikovan, treba ga prijaviti direktno organizaciji specijalizovanoj za internetsku bezbjednost koja upravlja sistemom izvještavanja putem javne telefonske linije i IT profesionalcima radi prijavljivanja specifičnih oblika potencijalno ilegalnih internetskih sadržaja.
Na primjer, na osnovu svoje politike zaštite djece, BBC je objavio uredničke smjernice o interakciji sa djecom i mladima na internetu. BBC je razvio dodatne kontrolne liste i kodekse ponašanja za rad sa djecom i mladima na internetu, koje se takođe odnose na podizvođače i vanjske provajdere usluga.
Politika zaštite djece regulatora za komunikacije u Velikoj Britaniji (Ofcom) odvojeno se bavi online sadržajem, mobilnim uređajima i igraćim konzolama.

Stvaranje bezbjednijeg i starosno prikladnog digitalnog okruženja	Kompanije koje nude profesionalno uređeni digitalni sadržaj mogu pomoći u stvaranju sigurnijeg i prijatnijeg digitalnog okruženja za djecu i mlade svih uzrasta preduzimanjem sljedećih radnji:
	Sarađujte sa drugima iz branše da biste razvili sisteme klasifikacije/ocjenjivanja sadržaja koji se zasnivaju na prihvaćenim nacionalnim ili međunarodnim standardima i u skladu sa pristupima koji se zauzimaju u ekvivalentnim medijima. Gdje je to moguće, klasifikacija sadržaja trebalo bi da bude konzistentna na različitim medijskim platformama, na primjer, najava filma u bioskopu i na pametnom telefonu korisnicima bi prikazivala iste klasifikacije.
	Razviti proizvode prilagođene djeci i starosno prilagođene sadržaje za djecu i mlade koji su osmišljeni kao sigurni i nadograđeni pouzdanim sistemom provjere starosti.
	Da biste pomogli roditeljima i drugima da odluče da li je sadržaj starosno primjeren za djecu i mlade, izgradite aplikacije i usluge na svim medijima kako bi se uskladili sa sistemima ocjenjivanja sadržaja. Usvojite odgovarajuće metode provjere starosti kako biste spriječili djecu i mlade da pristupaju starosno osjetljivom sadržaju, web lokacijama, proizvodima ili interaktivnim uslugama. Pružite savjete i podsjetnike o prirodi i starosnoj klasifikaciji sadržaja koji koriste.
	Kompanija koja nudi audiovizuelne i multimedijske usluge možda želi dati lični identifikacioni broj korisnicima koji žele da pristupe sadržaju koji može biti štetan za djecu i mlade.
	Obezbijedite transparentnost cijena za proizvode i usluge i prikupljene informacije o korisnicima. Pobrinite se da se politike prikupljanja podataka pridržavaju relevantnih zakona koji se tiču privatnosti djece i mladih, uključujući i to da li je potreban pristanak roditelja prije nego što komercijalna preduzeća mogu prikupljati lične podatke od djeteta ili o njemu.
	Pobrinite se da oglašavanje ili komercijalna komunikacija budu jasno prepoznatljivi kao takvi. Nadgledajte sadržaj koji je dostupan online i prilagodite ga korisničkim grupama koje će mu vjerovatno pristupiti, na primjer, uspostavljanjem odgovarajućih pravila za online oglašavanje djeci i mladima. Ako ponuda sadržaja podržava interaktivni element, kao što je komentarisanje, online forumi, društvene mreže, platforme za igre, chat sobe ili oglasne ploče, uspostavite jasan skup „kućnih pravila“ na jeziku prilagođenom kupcima u okviru usluga i korisničkih smjernica .
	Odlučite koji je nivo angažmana potreban prije pokretanja online usluge. Usluge usmjerene na privlačenje djece trebale bi predstavljati samo sadržaje koji su prikladni za mladu publiku. Ako postoje sumnje, mogu se konsultovati državna tijela nadležna za zaštitu djece.
	Obezbediti jasno i istinito označavanje sadržaja. Imajte na umu da korisnici mogu doći do neprimjerenog sadržaja slijedeći veze na web lokacijama trećih strana koje zaobilaze stranice za kontekstualizaciju sadržaja.

Edukacija djece, roditelja i edukatora o dječjoj bezbjednosti i njihovoj odgovornoj upotrebi IK tehnologija	Kompanije koje nude profesionalno uređen digitalni sadržaj mogu dopuniti tehničke mjere obrazovnim aktivnostima koje osnažuju djecu preduzimanjem sljedećih radnji:
	Pružite kupcima konkretne i jasne informacije o sadržaju, kao što su vrsta sadržaja, starosne ocjene odnosno ograničenja, uvredljiv jezik ili nasilje i odgovarajuće dostupne roditeljske kontrole; i informacije o tome kako prijaviti zloupotrebu i neprimjeren ili nezakonit sadržaj i kako će se postupati s izvještajima. U interaktivnom svijetu ove informacije se daju u obliku oznaka sadržaja za svaki program.
	Podstaknite odrasle, posebno roditelje, njegovatelje i staratelje, da budu uključeni u potrošnju internetskog sadržaja djece i mladih da bi mogli pomoći i usmjeravati djecu i mlade u izboru sadržaja prilikom kupovine i pomoći u uspostavljanju pravila ponašanja. Pomozite djeci (i roditeljima i starateljima) da nauče upravljati svojim vremenom ispred ekrana i razumiju kako koristiti tehnologiju na način koji im odgovara, uključujući i to kada treba prestati i raditi nešto drugo.
	Prenesite pravila upotrebe na jasnom i dostupnom jeziku koji podstiču djecu i mlade na oprez i odgovornost kada surfuju internetom.
	Kreireajte alate prilagođene starosti, poput tutorijala i centara za pomoć. Po potrebi sarađujte sa internetskim ili ličnim preventivnim programima i terapeutskim klinikama. Na primjer, ako postoji rizik da se djeca i mladi previše bave tehnologijom, što im otežava razvijanje ličnih odnosa ili učešće u zdravim fizičkim aktivnostima, web stranca može dati link za liniju za pomoć ili terapeutsku službu. Neka sigurnosne informacije, poput linkova za savjete, budu istaknute, lako dostupne i jasne kada bude velika mogućnost da će online sadržaj privući veliki broj djece i mladih.
	Ponudite alat za roditeljsko navođenje, kao što je „brava“ za kontrolu sadržaja kojem se može pristupiti putem određenog pretraživača.
	Sarađujte sa roditeljima kako biste bili sigurni da ih informacije objavljene na Internetu o djeci ne izlažu riziku. Način prepoznavanja djece u profesionalno uređenom sadržaju zahtijeva pažljivo razmatranje i varira u zavisnosti od konteksta. Pribavite informisani pristanak djece kada ih prikazujete u programima, filmovima, video zapisima itd, gdje god je to moguće, i poštujte svako odbijanje učešća.

Promovisanje digitalne tehnologije kao načina ka dodatnom civilnom angažmanu	Kompanije koje nude profesionalno uređeni digitalni sadržaj mogu ohrabriti i osnažiti djecu i mlade podržavajući njihovo pravo na učešće kroz sljedeće aktivnosti:
	Kreirajte odnosno ponudite niz visokokvalitetnih, izazovnih, edukativnih, prijatnih i zanimljivih sadržaja koji odgovaraju uzrastu i pomažu djeci i mladima da shvate svijet u kojem žive. Osim što je atraktivan i upotrebljiv, pouzdan i siguran, takav sadržaj može doprinijeti fizičkom, mentalnom i socijalnom razvoju djece i mladih pružajući nove mogućnosti za zabavu i obrazovanje. Potrebno je snažno podsticati sadržaje koji djeci omogućavaju da prihvate različitost i budu pozitivni uzori.

5.3 Karakteristika C: Skladištiti sadržaj koji generišu korisnici i povežite korisnike

Ranije su internet svijetom dominirali odrasli, ali sada je jasno da su djeca i mladi glavni učesnici na više platformi u stvaranju i dijeljenju eksplozije sadržaja koji generišu korisnici. Ova funkcija se, između ostalog, bavi uslugama društvenih medija, aplikacijama i web lokacijama povezanim sa kreativnom realizacijom.

Servisi koji međusobno povezuju korisnike mogu se podijeliti u tri kategorije:

- Prvenstveno aplikacije za razmjenu poruka (Facebook Messenger, Groupme, Line, Tinder, Telegram, Viber, WhatsApp).
- Prvenstveno usluge društvenih mreža koje traže i skladište sadržaj koji generišu korisnici i koji omogućavaju korisnicima da dijele sadržaj i povezuju se unutar i izvan svojih mreža (Instagram, Facebook, SnapChat, TikTok).
- Prvenstveno aplikacije za streaming uživo (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

Provajderi usluga zahtijevaju minimalnu starost za prijavu na platforme, ali to je teško provesti jer se provjera starosti oslanja na prijavljenu starost. Većina usluga koje međusobno povezuju nove korisnike takođe omogućavaju funkcije dijeljenja lokacije, što čini djecu i mlade koji koriste ove usluge još osjetljivijima na opasnosti van interneta.

Tabela 4, koja je prilagođena pravilima koja primjenjuje jedna od najvećih društvenih mreža, pruža smjernice za provajdere usluga koji vrše hosting sadržaja koji kreiraju korisnici i povezuju nove korisnike o politikama i radnjama koje mogu preduzeti kako bi unaprijedili online zaštitu i uključenost djece.

Tabela 4: Kontrolna lista zaštite djece na internetu za Karakteristiku C: Skladištiti sadržaj koji generišu korisnici i povežite korisnike

Uvrštavanje pitanja prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja	Servisi koji vrše hosting sadržaja koji generišu korisnici i koji povezuju korisnike mogu da identifikuju, spriječe i ublaže negativne učinke IK tehnologija na prava djece i mladih i da identifikuju mogućnosti za podršku napretku djece i mladih.
	Vidi opšte smjernice u Tabeli 1.
Razvoj standardnih procesa radi rješavanja problema materijala seksualnog zlostavljanja djece	U saradnji s vladom, organima za sprovođenje zakona, civilnim društvom i organizacijama SOS servisa, kompanije koje vrše hosting sadržaja koji generišu korisnici i koje povezuju korisnike mogu igrati ključnu ulogu u borbi protiv materijala seksualnog zlostavljanja djece preduzimanjem sljedećih radnji:
	Uspostavite procedure za sve lokacije za pružanje neposredne pomoći policiji tokom vanrednih situacija i za rutinske istrage.
	Navedite da će preduzeće u potpunosti sarađivati u istragama u slučaju da se nezakoniti sadržaj prijavi ili otkrije i zabilježite detalje u vezi sa takvim kaznama kao što su novčane kazne ili ukidanje privilegija naplate.
	Radite sa internim funkcijama kao što su briga o kupcima, sprečavanje prevara i bezbjednost da biste bili sigurni da kompanija može podnositi izvještaje o sumnji na ilegalni sadržaj direktno policiji i linijama za podršku. U idealnom slučaju, to bi trebalo uraditi na način koji ne izlaže sadržaju osoblje koje radi direktno sa klijentima niti ponovo viktimizuje ugroženo dijete/djecu i mlade. Da biste se pozabavili situacijama u kojima osoblje može biti izloženo nasilnom materijalu, implementirajte politiku ili program za podršku otpornosti, sigurnosti i dobrobiti osoblja.
	Primijenite uslove iz ugovora o vršenju usluge i uslove za zabranu ilegalnog sadržaja i ponašanja, ističući da: • štetni sadržaji, uključujući sumnju na pedofilsko zbližavanaje sa djecom sa namjerom bilo fizičkog ili nefizičkog zlostavljanja, neće biti tolerisani: • protivzakoniti sadržaj, uključujući upload ili dalje širenje materijala seksualnog zlostavljanja djece, neće biti tolerisan; • kompanija će se obratiti i u potpunosti sarađivati u krivičnim istragama u slučaju da se prijavi ili otkrije protivzakoniti sadržaj ili bilo koje kršenje politike zaštite djece.
	Dokumentujte praksu kompanije za rukovanje materijalom seksualnog zlostavljanja djece, počevši od nadgledanja i proširivanja do konačnog prenosa i uništavanja sadržaja. U dokumentaciju uvrstite spisak svog osoblja odgovornog za rukovanje materijalom.
	Usvojite politike u vezi sa vlasništvom nad sadržajem koji kreireju korisnici, uključujući opciju uklanjanja sadržaja koji kreiraju korisnici na zahtjev korisnika. Uklonite sadržaj kojim se krše pravila provajdera, a o kršenju upozorite korisnika.

Uspostavljanje standardnih procesa za borbu protiv MSZD **(*nastavak*.)**	Navedite da će nepoštovanje politika od strane korisnika imati posljedice, uključujući: • uklanjanje sadržaja, suspenziju ili zatvaranje naloga prekršioca; • opoziv opcije dijeljenja određenih vrsta sadržaja ili korištenja određenih opcija; • sprečavanje kontakta sa djecom; • prijavljivanje slučaja nadležnim organima
Uspostavljanje standardnih procesa za borbu protiv MSZD	Promovišite mehanizme izvještavanja za MSZD ili bilo koji drugi ilegalni sadržaj i obezbijedite uslove da klijenti znaju podnijeti prijavu ako otkriju takav sadržaj. Uspostavite sisteme i obezbijedite obučeno osoblje za procjenu pojedinačnih slučajeva i preduzimanje odgovarajućih mjera. Uspostavite dobro organizovane i sveoubuhvatne operativne timove za korisničku podršku. teams. Idealno bi bilo da se ovi timovi obuče za rješavanje različitih vrsta incidenata da bi se dao adekvatan odgovor i preduzele odgovarajuće radnje. Kada korisnik podnese žalbu, zavisno od vrste incidenta, potrebno je korisnika uputiti odgovarajućem osoblju. Kompanija bi takođe mogla uspostaviti posebne timove za rješavanje žalbi korisnika u slučajevima kada su izvještaji možda podneseni greškom.
	Uspostavite procese za trenutno uklanjanje ili blokiranje pristupa materijalu seksualnog zlostavljanja djece, uključujući procese obavještavanja i uklanjanja ilegalnog sadržaja odmah nakon identifikovanja istog. Pobrinite se da treće strane sa kojima je kompanija u ugovornom odnosu imaju slične efikasne postupke obavještavanja i uklanjanja. Ako zakonodavstvo dozvoljava, materijal se može čuvati kao dokaz krivičnog djela u slučaju istrage.
	Uspostaviti tehničke sisteme koji mogu otkriti poznati ilegalni sadržaj i spriječiti njegovo učitavanje, uključujući i učitavanje u privatne grupe, ili ga označiti za trenutni pregled od strane bezbjednosnog tima kompanije. Preduzmite sve odgovarajuće mjere zaštite servisa od zloupotrebe u pogledu hostinga, distribuisanja ili kreiranja materijala seksualnog zlostavljanja djece. Gdje je to moguće, uspostavite proaktivne tehničke mjere za analizu predmeta i metapodataka povezanih sa profilom radi otkrivanja kriminalnog ponašanja ili obrazaca i preduzmite odgovarajuće mjere.
	Ako aplikacija ili usluga omogućava korisnicima da prenose i čuvaju fotografije na serverima koji su u vlasništvu kompanije ili kojima se kompanija služi, uspostavite procese i alate za prepoznavanje slika koje će najverovatnije sadržavati materijal seksualnog zlostavljanja djece. Razmotrite proaktivne tehnike identifikacije kao što su tehnologija skeniranja ili ljudski pregled.

Stvaranje bezbjednijeg i starosno prikladnog digitalnog okruženja	Provajderi usluga koji nude sadržaj kreiran od strane korisnika mogu pomoći u stvaranju sigurnijeg, ugodnijeg digitalnog okruženja za djecu svih uzrasta preduzimanjem sljedećih radnji:
	Na jeziku prilagođenom kupcima, a u okviru usluge i korisničkih smjernica, definišite jasan skup „kućnih pravila“ kojima se definiše sljedeće: • priroda usluge i ono što se očekuje od njenih korisnika; • šta jeste, a šta nije prihvatljivo u smislu sadržaja, ponašanja i jezika, kao i zabranu ilegalne upotrebe; • posljedice kršenja, kao na primjer prijavljivanje policiji i suspenzija korisničkog računa.
	Ključne bezbjednosne i pravne poruke trebale bi biti predstavljene u starosno prilagođenom formatu (tj. koristeći intuitivne ikone i simbole) prilikom registracije i prilikom preduzimanja različitih radnji na web stranici.
	Olakšajte klijentima da korisničkom servisu prijave problem zloupotrebe, koristeći uspostavljene standardne i pristupačne postupke za rješavanje različitih problema, poput primanja neželjenih komunikacija (neželjene pošte, maltretiranja) ili gledanja neprimjerenog sadržaja.
	Omogućite podešavanja vidljivosti i podjele sadržaja prilagođena uzrastu. Na primjer, neka postavke privatnosti i vidljivosti za djecu i mlade budu po defaultu restriktivnije od postavki za odrasle.
	Uspostavite minimalne starosne zahtjeve i podržite istraživanje i razvoj novih sistema za provjeru starosti, poput biometrije, koristeći poznate međunarodne standarde za razvoj takvih alata. Preduzmite korake za identifikovanje i uklanjanje maloljetnih korisnika koji su pogrešno prikazali svoju starost da bi dobili pristup. Potrebno je razmotriti dodatno prikupljanje ličnih podataka koje moglo obuhvatiti i ovaj problem, kao i potrebu ograničenja prikupljanja i čuvanja ovih podataka i njihove obrade. Ako to već nije uspostavljeno, uspostavite odgovarajuće procese prijave da biste utvrdili jesu li korisnici dovoljno stari za pristup sadržaju ili usluzi bez ugrožavanja njihovog identiteta, lokacije i ličnih podataka. Koristite nacionalno uspostavljene funkcionalne sisteme za provjeru starosti prema potrebi, tamo gdje postoje relevantne mjere za zaštitu privatnosti podataka djece. Funkcija izvještavanja ili služba za pomoć/centar koja može podstaknuti korisnike da prijave ljude koji su pogrešno prikazali svoju starost.

Stvaranje bezbjednijeg i starosno prikladnog digitalnog okruženja (*nastavak*)	Zaštitite mlađe korisnike od neželjene komunikacije i obezbijedite da se uspostave smjernice o privatnosti i prikupljanju informacija.
	Pronađite načine da pregledate uskladištene slike i videozapise i izbrišete neprikladne kad ih otkrijete. Alati kao što su *hash* skeniranje poznatih slika i softver za prepoznavanje slika su vam na raspolaganju kao pomoć. U uslugama usmjerenim na djecu, fotografije i videozapisi mogu se prethodno provjeriti kako bi se osiguralo da djeca ne objavljuju osjetljive lične podatke o sebi ili drugima.
	Brojne mjere mogu se koristiti za kontrolu pristupa sadržaju koji generišu korisnici i za zaštitu djece i mladih na mreži od neprikladnog ili ilegalnog sadržaja. Obavezno koristite bezbjedne lozinke kao korak u cilju zaštite djece i mladih u igrama i drugim postavkama društvenih medija. Ostale tehnike uključuju: • pregled diskusionih grupa radi utvrđivanja štetnih predmeta, govora mržnje i nezakonitog ponašanja i brisanje takvog sadržaja kada se utvrdi da krši uslove korištenja; • pregled diskusionih grupa radi utvrđivanja štetnih predmeta, govora mržnje i nezakonitog ponašanja i brisanje takvog sadržaja kada se utvrdi da krši uslove korištenja; • pre-moderisanje oglasnih ploča sa timom specijalizovanih moderatora za djecu i mlade koji proveravaju sadržaj koji je u suprotnosti s objavljenim "kućnim redom". Svaka poruka se može provjeriti prije objavljivanja, a moderatori takođe mogu uočiti i označiti sumnjive korisnike, kao i korisnike u nevolji; • uspostavljanje tima domaćina zajednice (*host*) koji služe kao prva tačka kontakta za moderatore kada imaju problem u vezi sa korisnikom.
	Budite odgovorni za pregled komercijalnog sadržaja, uključujući forume, društvene mreže i web lokacije za igre.

Edukacija djece, roditelja i edukatora o bezbjednosti djece i njihovoj odgovornoj upotrebi IK tehnologija	Provajderi usluga koji nude sadržaj koji generišu korisnici mogu dopuniti tehničke mjere obrazovnim aktivnostima i aktivnostima osnaživanja preduzimanjem sljedećih radnji:
	Kreirajte dio posvećen bezbjednosnim savjetima, člancima, karakteristikama i dijalogu o digitalnom državljanstvu, kao i linkovima do korisnog sadržaja nezavisnih stručnjaka. Bezbjednosni savjeti moraju biti lako uočljivi i napisani lako razumljivim jezikom. Takođe se provajderi platformi podstiču da imaju jedinstveni navigacioni interfejs na različitim uređajima, poput računara, tableta ili mobilnih telefona.
	Ponudite roditeljima jasne informacije o vrstama sadržaja i dostupnim uslugama, uključujući, na primjer, objašnjenje web lokacija društvenih mreža i usluga zasnovanih na lokaciji, način pristupa internetu putem mobilnih uređaja i opcije dostupne roditeljima za primjenu kontrola.
	Obavijestite roditelje o načinu prijavljivanja zloupotrebe, pogrešne upotrebe i neprimjerenog ili nezakonitog sadržaja kao i o načinu na koji će prijava biti rješavana. Obavijestite ih koje su usluge ograničene na starost i druge načine za sigurno i odgovorno ponašanje prilikom korištenja interaktivnih usluga.
	Uspostavite sistem zasnovan na “povjerenju i ugledu“ da bi se podstaklo dobro ponašanje i omogućilo vršnjacima da primjerom prenose najbolje prakse. Promovišite važnost društvenog izvještavanja, koje omogućava ljudima da se obrate drugim korisnicima ili pouzdanim prijateljima da bi pomogli u rješavanju sukoba ili započeli razgovor o zabrinjavajućem sadržaju.
	Pružite savjete i podsjetnike o prirodi date usluge ili sadržaja i o tome kako sigurno uživati u njemu. Ugradite smjernice zajednice u interaktivne usluge, na primjer, sa pop-up obavještenjima koji podsjećaju korisnike na odgovarajuće i sigurno ponašanje, poput nedavanja njihovih kontakt informacija.
	Sarađujte sa roditeljima da biste bili sigurni da ih informacije objavljene na internetu o djeci ne izlažu riziku. Pribavite informisani pristanak djece kada ih prikazujete u programima, filmovima, video zapisima itd, gdje god je to moguće, i poštujte svako odbijanje učešća.
Promovisanje digitalne tehnologije kao načina za povećanje građanskog angažmana	Kompanije koje nude profesionalno uređeni digitalni sadržaj mogu ohrabriti i osnažiti djecu i mlade podržavajući njihovo pravo na učešće.
	Vidi opšte smjernice u Tabeli 1.

5.4 Karakteristika D: Sistemi vođeni vještačkom inteligencijom

Sa povećanom pažnjom koja se daje tehnologijama za učenje, pojmovi “vještačka inteligencija“, “mašinsko učenje“ i “duboko učenje“ široko su u upotrebi u istom značenju kao odraz koncepta replikacije “inteligentnog“ ponašanja u mašinama. U ovom dijelu se fokusiramo na načine na koje procesi mašinskog učenja i dubokog učenja utiču na dječiji život i, konačno, na njihova ljudska prava.

“Zbog eksponencijalnog napretka tehnologija zasnovanih na vještačkoj inteligenciji u posljednjih nekoliko godina, trenutni međunarodni okvir koji štiti dječja prava ne bavi se izričito mnogim pitanjima koja su pokrenuta razvojem i upotrebom vještačke inteligencije. Međutim, ovaj okvir identifikuje nekoliko prava koja mogu biti implicirana ovim tehnologijama i na taj način pruža važno polazište za svaku analizu toga kako nove tehnologije mogu pozitivno ili negativno uticati na dječija prava, poput prava na privatnost, obrazovanje i igranje, kao i prava na nediskriminaciju."

Primjena vještačke inteligencije može uticati na efekat na djecu različitih usluga koje se koriste na društvenim mrežama, poput platformi za streaming video zapisa. Tehnologija ekrana osetljivog na dodir i dizajn ovih platformi omogućavaju vrlo maloj deci da pregledaju i kreću se ovim sadržajem. Posebna je zabrinutost da algoritmi koji koriste preporučene videozapise mogu zarobiti djecu u “filter mjehurićima“ lošeg ili neprikladnog sadržaja. Kako su djeca posebno podložna preporukama za sadržaj, šokantni "povezani videozapisi" im mogu privući pažnju i odvratiti ih od programiranja prilagođenijeg djeci.

Vještačka inteligencija takođe ima uticaja na online zaštitu djece s obzirom na pametne igračke. Različiti procesi koji su uključeni u rad pametnih igračaka dolaze sa svojim vlastitim izazovima, tj. igračkom (koja se povezuje s djetetom), mobilnom aplikacijom koja se koristi kao pristupna tačka za Wi-Fi vezu i personalizovanim online nalogom igračke odnosno potrošača, gdje se podaci čuvaju. Takve igračke komuniciraju sa serverima zasnovanim na oblaku koji čuvaju i obrađuju podatke koje pružaju djeca koja komuniciraju s igračkom. Ovaj model ima bezbjednosne probleme ako se bezbjednost ne primjenjuje na svakom nivou, što su pokazali brojni slučajevi hakovanja u kojima su procurili lični podaci. Štaviše, neki hakovani uređaji (uključujući pametne uređaje s priključkom na internet, poput baby monitora, glasovnih pomoćnika itd.) Mogu se koristiti za nadzor korisnika bez njihovog znanja ili pristanka.

Pri integraciji mehanizama odgovora na otkrivene prijetnje djeci koja koriste ove uređaje, na primjer, davanjem savjeta i preporuka na osnovu otkrivenog ponašanja (kao što je ranije spomenuto u aplikaciji BBC Own It), presudno je da kompanije koje dizajniraju pametne uređaje zasnivaju ove preporuke na dokazima i razvijaju ih u dogovoru sa stručnjacima za zaštitu djece.

Iako neke kompanije unapređuju principe za etičku upotrebu vještačke inteligencije, nije jasno postoje li javne politike usmjerene na vještačku inteligenciju i djecu. Nekoliko tehnoloških i trgovinskih udruženja i grupa za informatiku izradili su etičke principe u vezi sa vještačkom inteligencijom. Međutim, oni se ne odnose izričito na prava djeteta, načine na koje ove tehnologije vještačke inteligencije mogu stvoriti rizik za djecu ili proaktivne planove za njihovo ublažavanje.

UNICEF i UC Berkeley, “Završni izvještaj: Vještačka inteligencija i dječja prava”, 2018.

19 Ibid.

20 Ibid.

21 Vidi Microsoft, "Najvažnija pitanja ljudskih prava”, Izvještaj - FY17; i Google, “Odgovorni razvoj vještačke inteligencije” (2018).

22 Zvanični blog Microsoft-a, “Kompjuterizovana budućnost: Vještačka inteligencija i njena društvena uloga ”, 2018.

The Guardian, “‘Partnerstvo u vezi vještačke inteligencije koje su formirali Google, Facebook, Amazon, IBM i Microsoft”, 2016.

„Poput korporacija, vlade širom svijeta usvojile su strategije za buduće lidere u razvoju i upotrebi vještačke inteligencije, podstičući okruženje pogodno za inovatore i korporacije.“ Međutim, nejasno je kako se takve nacionalne strategije direktno bave dječjim pravima.

Unapređenje pristupa Facebooka sadržaju povezanim sa samoubistvom i samopovređivanjem

U 2019 godini, Facebook je počeo organizovati redovne konsultacije sa stručnjacima iz cijelog svijeta radi razgovora o nekim težim temama povezanim sa samoubistvom i samopovređivanjem. Ove teme obuhvataju pitanja poput kako postupati oproštajnim pismima samoubica, rizicima povezanim sa depresivnim sadržajem na internetu i značajnim prikazima samoubistva. Dodatni detalji ovih sastanaka dostupni su na Facebookovoj novoj stranici za prevenciju samoubistava, u njegovom Bezbjednosnom centru. Ove konsultacije za rezultat su imale nekoliko poboljšanja u načinu na koji Facebook obrađuje ovu vrstu sadržaja. Na primjer, ojačana je politika u vezi sa samopovređivanjem da bi se zabranilo grafičko rezanje slika radi izbjegavanja nenamjernog promovisanja ili izazivanja samopovređivanja. Čak i kada neko traži podršku ili tvrdi da pomaže oporavak, Facebook sada prikazuje upozorenje preko slika zaliječenih posjekotina od samoozljeđivanja. Ova vrsta sadržaja sada se otkriva primjenom vještačke inteligencije, pri čemu se automatski mogu preduzeti radnje na potencijalno štetnom sadržaju, uključujući uklanjanje istog ili dodavanjem upozorenja da se radi o osjetljivom sadržaju. Od aprila do juna 2019. godine, Facebook je intervenisao kod više od 1,5 miliona sadržaja samoubistava i samopovređivanja na svojoj web lokaciji i otkrio više od 95 posto istih prije nego što ih je korisnik prijavio. U istom periodu, Instagram je intervenisao kod više od 800 hiljada sličnih sadržaja, od kojih je više od 77 posto otkriveno prije nego što ih je korisnik prijavio.

Identifikovanje potencijalnog maltretiranja ili vršnjačkog nasilja u stvarnom vremenu i slanje poruka

Instagram uspostavlja vještačku inteligenciju da bi iskorijenio ponašanje poput vrijeđanja, sramoćenja i nepoštovanja. Korištenjem sofistikovanih alata za izvještavanje, moderatori mogu brzo zatvoriti nalog počinioca online maltretiranja.

24 Ibid.

Dobra praksa: Upotreba vještačke inteligencije u identifikaciji materijala seksualnog zlostavljanja djece

Nadovezujući se na Microsoftov velikodušni doprinos PhotoDNA u borbi protiv eksploatacije djece i nedavno pokretanje Google API-ja za bezbjednost sadržaja, Facebook je takođe razvio tehnologije za otkrivanje sadržaja seksualnog zlostavljanja djece.

Poznate kao PDQ i TMK + PDQF, ove tehnologije su dio seta alata koje Facebook koristi za otkrivanje štetnog sadržaja. Ostali algoritmi i alati dostupni industriji uključuju pHash, aHash i dHash. Facebook algoritam za podudaranje fotografija, PDQ, duguje veliku inspiraciju pHash-u, iako je od temelja kreirean kao poseban algoritam sa nezavisnom softverskom implementacijom. Tehnologiju za podudaranje video zapisa, TMK + PDQF, zajednički su razvili Facebook-ov tim za istraživanje vještačke inteligencije i naučnici sa Univerziteta u Modeni i Reggio Emilia u Italiji.

Ove tehnologije stvaraju efikasan način skladištenja datoteka u obliku kratkih digitalnih haševa koji mogu utvrditi da li su dvije datoteke iste ili slične, čak i bez originalne slike ili video zapisa. Haševi se takođe mogu lakše dijeliti sa drugim kompanijama i neprofitnim organizacijama.

PDQ i TMK + PDQF su dizajnirani za rad u velikim razmjerama, podržavajući haširanje video-frejmova i aplikacija u realnom vremenu.

U tabeli 5 su date neke od preporuka preduzećima za usklađivanje svojih načela prilikom dizajniranja i implemenacije rješenja namijenjenih djeci, a zasnovanih na vještačkoj inteligenciji.

Ove preporuke se zasnivaju na UNICEF-ovom radu na izradi globalnih smjernica politike o vještačkoj inteligenciji i djeci, koje će biti namijenjene državama i stručnjacima iz ove oblasti.
Vidi https://www.unicef.org/globalinsight/featured-projects/ai-children za dodatne informacije o projektu. Preporuke se takođe oslanjaju na rad UNICEF-a i studije Univerziteta Kalifornije u Berkeleyu o vještačkoj inteligneciji i pravima djeteta.

UNICEF i UC Berkeley, “Završni izvještaj: Vještačka inteligencija i dječja prava”, 2018.

Tabela 5: Kontrolna lista zaštite djece na internetu za Karakteristiku D: Sistemi vođeni vještačkom inteligencijom

Uvrštavanje pitanja prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja	Provajderi sistema vođenih vještačkom inteligencijom mogu da identifikuju, spriječe i ublaže negativne učinke IK tehnologija na prava djece i mladih i da identifikuju mogućnosti za podršku napretku djece i mladih.
	Sistemi vještačke inteligencije trebaju se dizajnirati, razvijati, implementirati i istraživati da bi se poštovala, promovisala i ispunjavala dječja prava, kako je utvrđeno u Konvenciji o pravima djeteta. Djetinjstvo, koje se sve više odvija u digitalnom okruženju, vrijeme je posvećeno posebnoj njezi i pomoći. Sisteme vještačke inteligencije treba iskoristiti tako da ovu podršku pruže u punom potencijalu.
	Uvrstite inkluzivni pristup dizajnu pri razvoju proizvoda za djecu, čime se posvećuje maksimalna pažnja rodnoj, geografskoj i kulturnoj raznolikosti i uključuje širok spektar interesnih strana, poput roditelja, nastavnika, dječjih psihologa i, prema potrebi, same djece.
	Trebalo bi uspostaviti okvire upravljanja, uključujući etičke smjernice, zakone, standarde i regulatorna tijela radi nadzora procesa kojima se sprečava da se primjena sistema vještačke inteligencije ne krše dječija prava.
Razvoj standardnih procesa radi rješavanja problema materijala seksualnog zlostavljanja djece	U saradnji sa državom, organima za sprovođenje zakona, civilnim društvom i organizacijama za podršku na vrućim linijama, provajderi sistema vođenih vještačkom inteligencijom igraju ključnu ulogu u borbi protiv materijala seksualnog zlostavljanja djece preduzimanjem sljedećih radnji:
	Vidi opšte smjernice u Tabeli 1.

Stvaranje bezbjednijeg i starosno prikladnog digitalnog okruženja	Provajderi sistema vođenih vještačkom inteligencijom mogu pomoći u stvaranju sigurnijeg, ugodnijeg digitalnog okruženja za djecu svih uzrasta preduzimanjem sljedećih radnji:
	Usvojite multidisciplinarni pristup prilikom razvijanja tehnologija koje utiču na djecu i konsultujte se se sa civilnim društvom, uključujući akademsku zajednicu, kako bi se identifikovali potencijalni uticaji ovih tehnologija na prava različitih vrsta potencijalnih krajnjih korisnika.
	Primijenite planiranu bezbjednost i planiranu privatnost za proizvode i usluge kojima se djeca bave ili ih često koriste.
	Kako su sistemi vještačke inteligencije "gladni" podataka, kompanije koje koriste vještačku inteligenciju za svoje usluge trebalo bi da koriste posebnu budnost u pogledu prikupljanja, obrade, skladištenja, prodaje i objavljivanja ličnih podataka djece. Sistemi vještačke inteligencije bi trebalo da budu transparentni tako da bi moglo biti moguće otkriti kako i zašto je sistem donio određenu odluku ili, u slučaju robota, postupio na način na koji je postupio. Ova transparentnost je presudna za razvijanje povjerenja i olakšavanje revizije, istrage i nadoknade kada se sumnja na štetu djece. Pobrinite se da postoje funkcionalni i zakonski mehanizmi za pomoć ako djeca jesu ili ako tvrde da su oštećena sistemima vještačke inteligencije. Potrebno je uspostaviti procese za blagovremeno ispravljanje svih diskriminatornih rezultata i uspostaviti nadzorna tijela za žalbe i kontinuirano praćenje dječje bezbjednosti i zaštite. Odgovornost i mehanizmi za obeštećenje idu ruku pod ruku.
	Sačiniti planove za rukovanje posebno osjetljivim podacima, uključujući otkrivanja zloupotrebe ili druge štete koja se može podijeliti sa kompanijom putem njenih proizvoda. Digitalne platforme i sistemi vještačke inteligencije trebali bi smanjiti prikupljanje podataka o djeci i povećati dječju kontrolu nad podacima koje kreiraju. Uslovi upotrebe trebaju biti razumljivi djeci kako bi osnažili svoju svijest i sposobnost.
Edukacija djece, roditelja i edukatora o dječjoj bezbjednosti i njihovoj odgovornoj upotrebi IK tehnologija	Pružaoci sistema vođenih vještačkom inteligencijom mogu dopuniti tehničke mjere obrazovnim aktivnostima i aktivnostima osnaživanja.
	Trebalo bi biti moguće objasniti svrhu sistema sa vještačkom inteligencijom djeci korisnicima i njihovim roditeljima ili starateljima kako bi ih osnažili da odluče koristiti ili odbiti takve platforme.

Promovisanje digitalne tehnologije kao načina za povećanje građanskog angažmana	Kompanije koje nude sisteme vođene vještačkom inteligencijom mogu ohrabriti i osnažiti djecu i mlade podržavajući njihovo pravo na učešće. *Vidi opšte smjernice u Tabeli 1.*
Korištenje tehnologije	Sistemi vođeni vještačkom inteligencijom trebali bi se razvijati da bi podržali dječji napredak u zaštiti razvoja i blagostanja kao rezultat u cijelom dizajnu sistema, te edukovali djecu o razvoju i implementaciji. Njihova referentna tačka trebalo bi da budu najbolje dostupne i široko prihvaćene metrike razvoja i blagostanja. Kompanije bi trebalo da ulažu u istraživanje i razvoj etičkih alata zasnovanih na vještačkoj inteligenciji za otkrivanje radnji online materijala seksualnog zlostavljanja djece i online uznemiravanja i maltretiranja i to u saradnji sa ključnim stručnjacima za dječja prava i djecom. Napredak u tehnologiji vještačke inteligencije trebao bi se primijeniti na ciljani, starosno prilagođeni messaging servis za djecu i to bez ugrožavanja njihovog identiteta, lokacije i ličnih podataka.

Reference

Tekst Opšte uredbe o zaštiti podataka (Uredba (EU) 2016/679 Parlamenta i Savjeta Evrope od 27. aprila 2016. O zaštiti fizičkih lica u vezi sa obradom ličnih podataka i slobodnom kretanju tih podataka, a kojom se van snage stavlja Direktiva 95/46/EC (Opšta uredbe o zaštiti podataka) i tekst iste objavljen u Službenom listu EU.

Izmijenjena Direktiva o AVMS (uslugama audio-vizuelnih medija) kojom se van snage stavlja Direktiva 2010/13/EU o koordinaciji određenih odredbi propisanih zakonom, propisa ili upravnih radnji u državama članicama u vezi s pružanjem audiovizuelnih medijskih usluga (Direktiva o audiovizuelnim medijskim uslugama) s obzirom na promjenu tržišne stvarnosti i Teksta objavljenog u Službenom listu EU.

BBC politika:

- Politika zaštite djece i sprovođenja mjera zaštite djece verzija 2017., revidirana 2018. i ažurirana verzija 2019.
-
- Okvir za nezavisne producentske kuće koje rade na produkcijama BBC-a o pravilima eksternih provajdera o zaštiti djece;
- Smjernice: Interakcija sa djecom i mladima na mreži putem uredničkih smjernica za online aktivnosti

Istraga kojom se dokazuje nepoštovanje starosne verifikacije za društvene medije u Velikoj Britaniji: 2016, 2017; 2020.

Objašnjenja pojmova

Definicije u nastavku su uglavnom izvedene iz postojeće terminologije utvrđene u Konvenciji o pravima djeteta, 1989. godine, kao i od Međuagencijske radne grupe za seksualno iskorištavanje djece u Terminološkim smjernicama za zaštitu djece od seksualnog iskorištavanja i seksualnog zlostavljanja, 2016. (Luksemburške smjernice), Konvencije Savjeta Evrope o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja, 2007., kao i UNICEF-ovog Global Kids Online izvještaja, 2019.

Adolescent

Adoslescenti su lica starosti između 10 i 19 godina. Važno je napomenuti da "adolescenti" nisu obavezujući pojam prema međunarodnom pravu, a oni mlađi od 18 godina smatraju se djecom, dok se 18-godišnjaci smatraju odraslima osim ako je prag punoljetnosti niži prema ranije propisanom nacionalnom zakonu.

Vještačka inteligencija

U najširem smislu, izraz "vještačka inteligencija" se nejasno odnosi na sisteme koji su čista naučna fantastika (tzv. "jaka" vještačka inteligencija sa samosvjesnom formom) i sisteme koji su već operativni i sposobni za obavljanje vrlo složenih zadataka (ovi sistemi su opisani kao "slaba" ili "umjerena" vještačka inteligencija, poput prepoznavanja lica ili glasa i upravljanja vozilima.)

Sistemi vještačke inteligencije

Sistem vještačke inteligencije je sistem zasnovan na mašini koji može, za određeni skup ciljeva koje definiše čovjek, davati predviđanja, preporuke ili odluke koje utiču na stvarno ili virtuelno okruženje. Sistemi vještačke inteligencije su osmišljeni za funkcionisanje na različitim nivoima autonomije.

Alexa

Amazon Alexa, poznat jednostavno kao Alexa, virtuelni je asistent zasnovan na vještačkoj inteligenciji, a razvio ga je Amazon. Sposoban je za glasovnu interakciju, reprodukciju muzike, pravljenje lista obaveza, postavljanje alarma, streaming podcastova, reprodukciju audio knjiga i pružanje informacija o vremenu, saobraćaju, sportu i drugim informacijama u stvarnom vremenu poput vijesti. Alexa takođe može kontrolisati nekoliko pametnih uređaja koristeći samog sebe kao sistem za automatizaciju kuće. Korisnici mogu proširiti Alexine mogućnosti instaliranjem "vještina" (dodatna funkcionalnost koju su razvili nezavisni dobavljači, koje se u drugim postavkama češće nazivaju aplikacijama poput programa za vremensku prognozu i audio karakteristika).

UNICEF i ITU, "Smjernice za IKT kompanije u pogledu bezbjednosti djece na internetu", 2014.
Savjet Evrope, "Šta je vještačka inteligencija?".
OECD (2019), Preporuke Savjeta o vještačkoj inteligenciji, https://webcache.googleusercontent
UNICEF i ITU, "Smjernice za IKT kompanije u pogledu bezbjednosti djece na internetu", 2014.

Najbolji interes djeteta

Opisuje sve elemente potrebne za donošenje odluke u određenoj situaciji za određeno dijete ili grupu djece.

Dijete

U skladu sa članom 1. Konvencije o pravima djeteta, dijete je svako mlađi od 18 godina osim ako je prag punoljetnosti niži prema ranije propisanom nacionalnom zakonu.

Seksualno iskorištavanje i zlostavljanje djece

Opisuje sve oblike seksualno iskorištavanje i zlostavljanje djece, npr. (a) podsticanje ili prinuđavanje djeteta da se bavi bilo kojom nezakonitom seksualnom aktivnošću; (b) iskorištavanje djece za prostituciju ili druge nezakonite seksualne radnje; (c) izrabljivačka upotreba djece u pornografskim izvedbama i materijalima", kao i„ seksualni kontakt koji obično uključuje silu nad licem bez pristanka istog." Seksualno iskorištavanje i zlostavljanje djece se sve češće odvija preko interneta ili u vezi sa online okruženjem.

Brza evolucija IK tehnologija stvorila je nove oblike seksualnog iskorištavanja i zlostavljanja djece na internetu, koji se mogu odvijati virtuelno i ne moraju uključivati fizički susret licem u lice sa djetetom. Iako pravni sistemi u velikom broju država još uvijek označavaju slike i video zapise djeteta seksualnog zlostavljanja kao „dječju pornografiju" ili „nedolične slike djece", ove Smjernice se kolektivno odnose na subjekte kao materijal za seksualno zlostavljanje djece. Ovo je u skladu sa Smjernicama Komisije za širokopojasnu mrežu i odgovorom globalne saradnje u borbi protiv seksualnog iskorištavanja i zlostavljanja djece "WePROTECT Global Alliance Model National Response". Ovaj pojam preciznije opisuje sadržaj. Pornografija se odnosi na zakonitu, komercijalizovanu industriju, a kako luksemburške smjernice navode da upotreba ovog izraza:

"može (nenamjerno ili ne) doprinijeti smanjenju težine, banalizaciji ili čak legitimizaciji onoga što je zapravo seksualno zlostavljanje odnosno seksualno iskorištavanje djece […] Ovaj termin rizici "dječje pornografije" koji insinuira da se djela vrše uz pristanak djeteta i predstavljaju legitimni seksualni materijal " Izraz materijal za seksualno zlostavljanje djece odnosi se na materijal koji predstavlja djela koja su seksualno nasilna odnosno izrabljivačka po dijete. To između ostalog uključuje materijale kojima se snima seksualno zlostavljanje djece od strane odraslih; slike djece uključene u seksualno eksplicitno ponašanje; polni organi djece kada se slike proizvode ili koriste prvenstveno u seksualne svrhe.

Vidi Luksemburške smjernice za izraze poput "kompjuterski ili digitalno generisan materijal seksualne zloupotrebe djece".

Vidi Konvenciju UN o pravima djeteta.
UNICEF i ITU, "Smjernice za IKT kompanije u pogledu bezbjednosti djece na internetu", 2014.
Član 34 Konvencije UN o pravima djeteta.
"Terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i seksualne zloupotrebe" (Luksemburške smjernice), 2016.
Luksemburške smjernice (kako je gore navedeno), 2016 i Izvještaj mreže Global Kids Online, 2019.
Komisija o širokopojasnoj mreži za održivi razvoj, "Child Online Safety: Minimizacija rizika od online nasilja, zloupotrebe i iskorištavanja", 2019; WePROTECT Global Alliance, "Sprečavanje i borba protiv seksualnog iskorištavanja i zlostavljanja djece (CSEA):Model nacionalnog odgovora", 2016.

Djeca i mladi

Opisuje lica mlađa od 18 godina, pri čemu pojam "djeca", koja se u smjernicama takođe nazivaju i mlađom djecom, obuhvata sva lica mlađa od 15 godina i mlađa lica između 15 i 18 godina starosti.

Igračke sa internet konekcijom

Igračke sa internet konekcijom se povezuju na internet pomoću tehnologija kao što su Wi-Fi i Bluetooth i obično rade zajedno sa pratećim aplikacijama kako bi djeci omogućile interaktivnu igru. Prema Juniper Research-u, tržište online igračaka u 2015. dostiglo je 2,8 milijardi USD, a predviđa se da će se do 2020. povećati na 11 milijardi USD. Ove igračke prikupljaju i čuvaju lične podatke od djece, uključujući imena, geolokaciju, adrese, fotografije, audio i video zapise.

Sajber maltretiranje

Terminom sajber maltretiranje se opisuje namjerni agresivni čin koji su više puta izvršili grupa ili pojedinac koristeći digitalnu tehnologiju i ciljajući žrtvu koja se ne može lako braniti. To obično uključuje "upotrebu digitalne tehnologije i interneta za objavljivanje štetnih informacija o nekome, namjerno dijeljenje privatnih podataka. informacija, fotografija ili video zapisa na štetan način, slanje prijetećih ili uvredljivih poruka (putem e-pošte, razmjene trenutnih poruka, chata, tekstova), širenje glasina i lažnih podataka o žrtvi ili njihovo namjerno isključivanje iz online komunikacije "

Sajber mržnja, diskriminacija i nasilni ekstremizam

"Sajber mržnja, diskriminacija i nasilni ekstremizam su različiti oblik sajber nasilja jer ciljaju kolektivni identitet, a ne pojedince […] koji se često odnose na rasu, seksualnu orijentaciju, religiju, nacionalnost ili imigracioni status, pol/rod i politiku".

Digitalno građanstvo

Digitalno građanstvo se odnosi na sposobnost pozitivnog, kritičkog i kompetentnog uključivanja u digitalno okruženje, oslanjanja na vještine efikasne komunikacije i stvaranja, praktikovanje oblika društvene participacije koji poštuju ljudska prava i dostojanstvo odgovornom upotrebom tehnologije.

Jeremy Greenberg, "Opasne igre: Igračke sa internet konekcijom, Zakon o zaštiti dječje privatnosti i loša bezbjednost", Georgetown Law Technology Review, 2017.

Anna Costanza Baldry et al. "Sajber maltretiranje i sajber viktimizacija naspram roditeljskog nadzora, praćenja i kontrole online aktivnosti adolescenata", Pregled usluga za djecu i mlade, 2019.

Luksemburške smjernice 2016 i Izvještaj mreže Global Kids Online, 2019. (kako je gore navedeno), UNICEF Global Kids Online Report, 2019 (kako je gore navedeno).

Council of Europe, "Digitalno građanstvo i edukacija o digitalnom građanstvu"

Digitalna pismenost

Digitalna pismenost znači imati vještine potrebne za život, učenje i rad u društvu u kom se komunikacija i pristup informacijama sve više vrši putem digitalnih tehnologija poput internet platformi, društvenih medija i mobilnih uređaja. Uključuje jasnu komunikaciju, tehničke vještine i kritičko razmišljanje.

Digitalna otpornost

Ovaj pojam opisuje sposobnost djeteta da se emocionalno nosi sa povređivanjem na internetu. Takođe se odnosi na emocionalnu inteligenciju potrebnu da bi se razumjelo kada je dijete na mreži u opasnosti, znalo kako zatražiti pomoć, naučilo iz iskustva i kako bi se oporavilo kada stvari krenu po zlu.

Upravnici

Opisuje sva lica koja su na položaju u upravnoj ili rukovodećoj strukturi škole.

(Online) pedofilsko zbližavanje

Pedofilsko (online) zbližavanje, kako je definisano u Luksemburškim smjernicama, odnosi se na "postupak uspostavljanja/izgradnje odnosa sa djetetom lično ili putem interneta ili drugih digitalnih tehnologija kako bi se olakšao seksualni kontakt na internetu ili van njega". To je krivično aktivnost zbližavanja sa djetetom ... ,sa ciljem nagovaranja djeteta na seksualni odnos.

Informacione i komunikacione tehnologije

Informacione i komunikacione tehnologije (IKT) opisuju sve informacione tehnologije kojima se ističe aspekt komunikacije. To uključuje sve usluge i uređaje za internetsko povezivanje, između ostalog računare, laptope, tablete, pametne telefone, igraće konzole i pametne satove. Pored toga, uključuje usluge kao što su radio i televizija, širokopojasni, mrežni hardver i satelitske sisteme.

Igranje online igrica

"Online igranje" se definiše kao igranje bilo koje vrste pojedinačne ili višenamjenske komercijalne digitalne igre putem bilo kog uređaja povezanog na internet, uključujući namjenske konzole, desktop kompjutere, laptope, tablete i mobilne telefone. „Ekosistem online igara" definisan je tako da uključuje gledanje drugih kako igraju video igre putem e-sporta, streaminga ili platforme za razmjenu video zapisa, što obično pruža mogućnost gledaocima da komentarišu ili komuniciraju s igračima i ostalim članovima publike.

Western Sydney University, "Šta je digitalna pismenost?".
Dr Andrew K. Przybylski, et al., "Podijeljena odgovornost: Razvijanje online otpornosti djeteta", Virgin Media and Parent Zone, 2014.
UNICEF i ITU, "Smjernice za IKT kompanije u pogledu bezbjednosti djece na internetu", 2014.
(kako je navedeno iznad)
UNICEF, "Dječja prava i online igranje:Prilike i izazovi za djecu i IKT djelatnost", 2019.

Kontrolni alati roditelja

Softver koji omogućava korisnicima, obično roditelju, da kontrolišu neke ili sve funkcije računara ili drugog uređaja koji se mogu povezati na internet. Takvi programi obično mogu ograničiti pristup određenim vrstama ili klasama web lokacija ili mrežnih usluga. Neki programi takođe pružaju opseg upravljanja vremenom, tj. uređaj se može postaviti tako da ima pristup internetu samo u određenim terminima. Naprednije verzije mogu snimati sve tekstove poslane ili primljene sa uređaja. Ovi programi su obično zaštićeni lozinkom.

Lični podaci

Ovaj pojam opisuje informacije o osobi koje se mogu pojedinačno identifikovati i koje se prikupljaju online. To uključuje puno ime i prezime, kontakt informacije poput kućne adrese i adrese e-pošte, brojeve telefona, otiske prstiju ili materijala za prepoznavanje lica, brojeve osiguranja ili bilo koji drugi faktor koji omogućava fizičko ili online kontaktiranje ili lokalizaciju osobe. U ovom kontekstu, ovo se odnosi i na sve informacije o djetetu i njegovoj pratnji koje pružaoci usluga prikupljaju na mreži, uključujući povezane igračke i Internet stvari kao i bilo koju drugu tehnologiju povezanu na internet.

Privatnost

Privatnost se često mjeri u smislu dijeljenja ličnih podataka na mreži, posjedovanja javnog profila na društvenim mrežama, dijeljenja informacija sa ljudima koje su djeca upoznala na mreži, korištenja postavki privatnosti, dijeljenja lozinki sa prijateljima i brige o privatnosti.

Javni servisi

Riječ je o nacionalnim emiterima ili medijima koji su dozvolu za emitovanje dobili na osnovu niza ugovornih obaveza sa državom ili parlamentom. Ove obaveze u mnogim zemljama proteklih godina proširene su na suzbijanje posljedica digitalne transformacije putem medija i programa digitalne pismenosti i obaveza rješavanja digitalne podjele.

Sexting

Sexting se obično definiše kao slanje, primanje ili razmjena lično proizvedenog seksualnog sadržaja, uključujući slike, poruke ili video zapise putem mobilnih telefona odnosno interneta. Stvaranje, distribucija i posjedovanje seksualnih slika djece je nezakonito u većini zemalja. Ako se otkriju seksualne slike djece, odrasli ih ne bi trebalo da gledaju. Dijeljenje seksualnih slika odrasle osobe sa djetetom uvijek je krivično djelo koje može biti štetno i možda će biti potrebno prijaviti takve slike i ukloniti ih.

UNICEF i ITU, "Smjernice za IKT kompanije u pogledu bezbjednosti djece na internetu", 2014. (kako je navedeno iznad)
Komisija za trgovinu SAD (1998), Zakon o zaštiti privatnosti djece na digitalnim mrežama, 1998.
Luksemburške smjernice, 2016 (kako je navedeno iznad).

Seksualno iznuđivanje djece (“sextortion“)

Seksualno iznuđivanje je “ucjenjivanje osobe uz pomoć vlastitih slika te osobe kako bi se od iste iznudile seksualne usluge, novac ili druge koristi pod prijetnjom dijeljenja materijala mimo pristanka prikazane osobe (npr. objavljivanje slika na društvenim mrežama) ”

Internet stvari

Internet stvari predstavlja sljedeći korak ka digitalizaciji društva i ekonomije, gdje su predmeti i ljudi međusobno povezani komunikacionim mrežama i izvještavaju o svom statusu odnosno okruženju.

URL

Skraćenica od “jedinstveni lokator resursa“ (engl. *uniform resource locator*), što je adresa internetske stranice.

Virtuelna stvarnost

Virtuelna stvarnost je upotreba računarske tehnologije za stvaranje efekta interaktivnog trodimenzionalnog svijeta u kom objekti imaju osjećaj prostorne prisutnosti.

WI-FI

Wi-Fi (engl. *Wireless Fidelity*) je grupa je tehničkih standarda koji omogućavaju prenos podataka putem bežičnih mreža.

Luksemburške smjernice, 2016 (kako je navedeno iznad).
Evropska komisija, “Politika: Internet stvari".
UNICEF i ITU, “Smjernice za IKT kompanije u pogledu bezbjednosti djece na internetu”, 2014. (kako je navedeno iznad)
NASA, “Virtuelna stvarnost: Definicija i zahtjevi”.
Komisija za trgovinu SAD (1998), Zakon o zaštiti privatnosti djece na digitalnim mrežama, 1998.

With the support of:

EBU
OPERATING EUROVISION AND EURORADIO

End Violence Against Children

eWORLDWIDE GROUP

GSMA

International Disability Alliance

IWF Internet Watch Foundation

PRIVATELY

腾讯游戏追梦计划
Tencent Games Dreaming Plan

unicef
for every child

Međunarodna unija za telekomunikacije
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-30411-9

Objavljeno u Švajcarskoj
Ženeva, 2020 Fotografije:
Shutterstock