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

Smjernice za IKT kompanije u pogledu sigurnosti djece na internetu

Priznanja

Ove su smjernice razvile Međunarodna unija za telekomunikacije (ITU) i radna skupina autora koji su dali doprinos, a dolaze iz vodećih institucija aktivnih u sektoru informacijskih i komunikacijskih tehnologija (IKT), kao i na pitanjima zaštite djece, a uključuju EBU, Globalno partnerstvo za zaustavljanje nasilja nad djecom, GSMA, Međunarodna alijansa za osobe s invaliditetom, The Internet Watch Foundation (IWF), Privately SA i UNICEF. Radnom skupinom predsjedao je Anjan Bose (UNICEF), a koordinirala 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 također 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 sigurnijim mjestom za djecu i mlade. ITU je zahvalan sljedećim partnerima koji dali 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 s 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 (Tiskana verzija)

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

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

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

Molimo vas da uzmete u obzir prirodni okoliš prije nego što tiskate ovo izvješće.

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 utječu na njihov život i njihove zajednice.

Ali širi i dostupniji pristup uslugama na internetu također predstavljaju značajne izazove za dječju sigurnost 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 s mnogim rizicima. Prijetnje se umnožavaju, a počinitelji sve više istodobno 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 obveza 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, prijenos uživo, kripto valute, Dark Web i snažni softveri za šifriranje. Međutim, oni također profitiraju od često nekoordiniranog i neodlučnog djelovanja tehnološkog sektora u cilju učinkovite borbe protiv problema.

Tehnologije u nastajanju mogu biti dio rješenja, primjerice Interpolova baza podataka o seksualnom zlostavljanju djece utemeljena na vještačkoj inteligenciji koja koristi softver za usporedbu slika i videozapisa za brzu uspostavu 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 njezine prednosti, zajednički i koordinirani 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 sigurnosti 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 s kojom se suočavaju djeca s invaliditetom, za koju svijet na internetu nudi posebno presudan spas za puno i ispunjeno društveno sudjelovanje.

Tehnološka industrija ima presudnu i proaktivnu ulogu u uspostavi temelja za zaštićeniju i sigurniju uporabu internetskih usluga i drugih tehnologija za današnju djecu i buduće generacije.

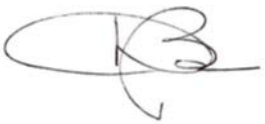
Poduzeće mora sve više stavljati dječje interese u središte svog rada, obraćajući posebnu pozornost na zaštitu privatnosti osobnih podataka mladih korisnika, čuvajući njihovo pravo na slobodu izražavanja, boreći se protiv rastuće pošasti materijala seksualnog zlostavljanja djece i osiguravajući da postoje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

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

Nadamo se da će ove smjernice IKT kompanijama poslužiti kao čvrst temelj na kojem 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 sudjelovali stručnjaci iz široke međunarodne zajednice kao koautori.

Također mi je drago predstaviti našu novu maskotu zaštite djece na internetu Sangoa: prijateljski nastrojenog i neustrašivog lika kojeg je u potpunosti dizajnirala skupina djece kao dio ITU-ovog novog međunarodnog programa informiranja mladih.

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



Doreen Bogdan-Martin
Ravnatelj
Biro za razvitak telekomunikacija, ITU

Kazalo

Tablica

1. Pregled

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

Kao alat, ove smjernice također imaju za cilj jačanje poslovnog uspjeha pomažući velikim i malim poduzećima 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 sigurnosti djece na internetu rezultat su konzultacija s članovima Inicijative za zaštitu djece na internetu, kao i širih konzultacija s članovima civilnog društva, gospodarstva, akademske zajednice, vlada, medija, međunarodnih organizacija i mladih.

Svrha ovog dokumenta je:

- uspostaviti zajedničku referentnu točku i smjernice za IK tehnologije i internetsku industriju i relevantne interesne strane;
- pružiti smjernice kompanijama o identifikaciji, sprječavanju i ublažavanju bilo kakvih negativnih utjecaja njihovih proizvoda i usluga na dječja prava;
- pružiti smjernice kompanijama o utvrđivanju načina na koje mogu promovirati dječja prava i odgovorno digitalno građanstvo među djecom;
- predložiti zajednička načela koja čine temelj nacionalnih ili regionalnih obveza u svim srodnim industrijama, imajući na umu da će se različite vrste poduzeća koristiti različitim modelima implementacije.

Opseg

Zaštita djece na internetu je složen izazov koji uključuje više različitih upravljačkih, političkih, operativnih, tehničkih i pravnih aspekata. Ove smjernice pokušavaju riješiti, organizirati i odrediti prioritete za mnoga od ovih područja, na temelju 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, razvitka 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 također fokusiraju i na druga pitanja koja se ne mogu definirati kao kaznena djela u svim nadležnostima. To uključuje nasilje među vršnjacima, cyber maltretiranje i uznemiravanje na internetu, kao i pitanja koja se odnose na privatnost ili opću dobrobit, prijevaru 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 uspostave sigurnog okruženja za djecu na internetu. Ove smjernice daju savjete o tome kako IKT kompanije mogu raditi na osiguranju dječje sigurnosti 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 sustave vođene vještačkom inteligencijom. Stoga pružaju pregled ključnih pitanja i izazova u vezi sa zaštitom djece na internetu i predlažu akcije za poduzeća i interesne strane za razvitak lokalnih i unutarnjih politika zaštite djece na internetu. Ove smjernice ne pokrivaju aspekte kao što su stvarni proces razvitka ili tekst koji bi politike IKT kompanija u vezi sa zaštitom djece na internetu mogle obuhvatiti.

Struktura

Odjeljak 1 - Pregled: Ovaj odjeljak ističe svrhu, opseg 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 s invaliditetom. Štoviše, 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 poduzeti mjere kako bi osigurale djeci sigurnu i pozitivnu uporabu IK tehnologija.

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

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

- Značajka A: Osigurati povezivanje, usluge skladištenja podataka i hostinga
- Značajka B: Ponuditi uređeni digitalni sadržaj
- Značajka C: Hostirati sadržaj koji generiraju korisnici i povezani korisnici
- Značajka D: Sustavi vođeni vještačkom inteligencijom

Ciljana publika

Nadovezujući se na Vodeća načela Ujedinjenih naroda o poslovanju i ljudskim pravima,[1] Dječja prava i poslovna načela pozivaju poduzeća da ispune svoju odgovornost da poštuju dječja prava izbjegavanjem bilo kakvih negativnih utjecaja povezanih s njihovim poslovanjem, proizvodima ili uslugama. Ova načela također artikuliraju razliku između poštovanja (minimuma koji je potreban poduzeću kako bi se izbjeglo nanošenje štete djeci) i potpore (primjerice, poduzimanjem dobrovoljnih akcija kojima se želi unaprijediti ostvarivanje dječjih prava). Poduzeća trebaju osigurati dječja prava kako na zaštitu na internetu, tako i na pristup informacijama i slobodu izražavanja, istodobno promovirajući pozitivnu uporabu IK tehnologija od strane djece.

[1] Vodeća načela Ujedinjenih naroda 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 tijekove u jednu struju koja doseže milijarde ljudi u svim dijelovima svijeta. Suradnja i partnerstvo su osnove uspostavljanja temelja za zaštićeniju i sigurniju uporabu interneta i povezanih tehnologija. Vlade, privatni sektor, kreatori politika, edukatori, civilno društvo, roditelji i skrbnici imaju vitalnu ulogu u postizanju ovog cilja. IKT industrija može djelovati u pet ključnih područja, kako je opisano u odjeljku 3.

2. Što je zaštita djece na internetu?

Tijekom posljednjih 10 godina, uporaba i uloga interneta u životima ljudi znatno su se promijenili. Zahvaljujući rasprostranjenosti pametnih telefona i tableta, dostupnosti Wi-Fi i 4G tehnologije i razvitku 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, s podjednakom uporabom interneta između korisnika od 16. do 24. godine i od 35. do 44. godine. Na globalnoj razini, svaki treći korisnik interneta je dijete (0-18 godina), a UNICEF procjenjuje da je 71% mladih već na internetu.[2] Širenje pristupnih točaka internetu, mobilne tehnologije i sve većeg spektra uređaja s mogućnošću pristupa internetu, u kombinaciji s ogromnim resursima koji se mogu naći u cyber prostoru, pružaju neviđene mogućnosti za učenje, dijeljenje i komunikaciju.

Prednosti uporabe IK tehnologija uključuju širi pristup informacijama o socijalnim uslugama, obrazovnim resursima i zdravstvenim savjetima. Dok djeca i mladi i obitelji 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. Operateri usluga dječje zaštite također koriste IK tehnologije za prikupljanje i prijenos podataka, što olakšava registraciju rođenja, vođenje slučajeva, traženje obitelji, prikupljanje podataka i mapiranje nasilja, između ostalog.

Štoviše, 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. Uporaba IK tehnologija omogućuje djeci i mladima da ostvare svoja prava i izraze svoja mišljenja, a također im omogućuje da se povežu i komuniciraju sa svojim obiteljima i prijateljima. IK tehnologije također služe kao najvažniji način kulturne razmjene i izvor zabave.

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

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

druge i njihove dugoročne „digitalne otiske“. Također 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 utječu na njih u skladu sa njihovim razvojnim kapacitetima. Konvencija također 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 utječu na njih. Roditelji, skrbnici, 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 dječjih 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. Štoviše, sve je veći konsenzus da bi promocija digitalnog građanstva među djecom i mladima, i razvitak proizvoda i platformi koji olakšavaju djeci pozitivnu uporabu 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 također mogu predstavljati nove rizike za sigurnost djece i mladih. Mogu izložiti djecu i mlade potencijalnim rizicima i štetama u vezi sa pitanjima privatnosti, nezakonitog sadržaja, uznemiravanja, cyber maltretiranja, zlouporabe osobnih 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 osobnih podataka ili na internetu ili putem „sextinga“, što je način na koji korisnici šalju seksualno eksplicitne poruke, fotografije ili slike između mobilnih telefona. Oni se također suočavaju s rizicima vezanim uz privatnost na internetu kada koriste internet. Djeca, po prirodi svojih godina i zrelosti, često nisu u stanju u potpunosti shvatiti rizike povezane s internetskim svijetom i moguće negativne posljedice za druge i sebe zbog svog neprimjerenog ponašanja.

Usprkos prednostima, postoje i nedostatci u uporabi novih i naprednijih tehnologija. Razvitak vještačke inteligencije i strojnog učenja, virtualne i proširene stvarnosti, velikih podataka, robotike i interneta stvari ima za cilj još više transformirati medijsku praksu djece i mladih. Iako se ove tehnologije pretežno razvijaju kako bi proširile opseg pružanja usluga i poboljšale pogodnost (putem, primjerice, 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 zaštićenog i sigurnog internetskog okruženja za djecu i omladinu zahtijeva djelotvorno sudjelovanje vlada, privatnog sektora i svih interesnih strana. Fokusiranje na digitalne vještine i pismenost roditelja i edukatora također mora biti jedan od prvih ciljeva, u čijem postizanju IKT kompanije mogu imati vitalnu i održivu ulogu.

[3] Konvencija o pravima djeteta UN-a. Sve zemlje osim tri (Somalija, Južni Sudan i Sjedinjene Američke Države) ratificirale 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, posebice među ranjivim skupinama. Prema cilju 16.2 Ciljeva održivog razvitka Ujedinjenih nacija - 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 s više interesnih strana koju je pokrenuo ITU, imala je za cilj podizanje svijesti o riziku za djecu na internetu i da odgovori na te rizike. Inicijativa okuplja partnere iz svih sektora globalne zajednice kako bi djeci svuda osigurali zaštićeno i sigurno internetsko iskustvo. Kao dio Inicijative, ITU je 2009. godine objavio set smjernica za zaštitu djece na internetu za četiri skupine: djecu, roditelje, skrbnike i edukatore; IKT kompanije; i kreatore politika. Zaštita djece na internetu podrazumijeva se u ovim smjernicama kao sveobuhvatan pristup da se odgovori na sve potencijalne prijetnje i štete s kojima se djeca i mladi mogu suočiti bilo na internetu ili na nekoj od internetskih tehnologija. U ovom dokumentu zaštita djece na internetu također uključuje štetu nanijetu djeci koja se dogodi izvan interneta, ali je povezana s dokazima o nasilju i zlostavljanju na internetu. Pored razmatranja dječjeg ponašanja i aktivnosti djece na internetu, zaštita djece na internetu također se odnosi na zlouporabu 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 stječu digitalnu pismenost i otpornost u pogledu njihove dobrobiti i zaštite na internetu.

Zaštita djece i mladih zajednička je odgovornost svih interesnih strana. Kako bi se to dogodilo, kreatori politika, IKT kompanije, roditelji, skrbnici, 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 sigurnih, prikladnih za sve uzraste, inkluzivnih i participativnih digitalnih prostora za djecu i mlade, koje karakteriziraju:

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

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

2.1 Osnovne informacije

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

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

zabavu, obrazovanje, sudjelovanje 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 definiranu minimalnu starosnu granicu koje se tehnološka industrija mora pridržavati, pa bi zato obrazovanje uz mjere zaštite trebalo integrirati 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), s procijenjenih 4.1 milijardu korisnika. Na globalnoj razini, svaki treći korisnik interneta je dijete mlađe od 18 godina[1]. Prema UNICEF-u, diljem svijeta 71% mladih već je na internetu[2]. Usprkos 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 obiteljski ili potrošački proizvod ili usluga koja je sastavni dio načina na koji obitelji, djeca i mladi žive svoj život.

U 2017. godini, na regionalnoj razini, pristup internetu za djecu i mlade bio je čvrsto povezan s razinom nacionalnog dohotka. Zemlje s niskim prihodima imaju tendenciju da imaju manje djece korisnika interneta nego zemlje s 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, ovisno o zemlji.

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

[2] Povjerenstvo za širokopojasni pristup, „Sigurnost djece na internetu: Smanjenje rizika od nasilja, zlostavljanja i iskorištavanja na internetu (2019),” *Povjerenstvo za širokopojasni pristup za održivi razvitak,* oktobar 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

[3] BBC, “Uporaba socijalnih medija od strane maloljetnika ‘raste’, kaže Ofcom”.

Uporaba interneta

Među djecom i mladima najpopularniji uređaj za pristup internetu je mobilni telefon, a slijede ga stolni računari i laptopi. Djeca i mladi provode u prosjeku dva sata dnevno na internetu tijekom tjedna 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 putem više uređaja, a oni koji se barem jednom tjedno 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 videoisječaka. Više od tri četvrtine djece i mladih koji koriste internet kažu da videoisječke gledaju na internetu barem jednom tjedno, bilo sami ili s drugim članovima svoje obitelji. 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 također bave politikom putem interneta i njihov se glas čuje putem blogova.

Ukupna razina sudjelovanja u igranju na internetu razlikuje se od zemlje do zemlje i približno je sukladna lakoći 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.

Tjedno se 10%-30% djece i mladih koji se koriste internetom - koja su konzultirana 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 svakog tjedna. Čini se da starija djeca imaju veći apetit za informacijama nego mlađa djeca.

[1] Livingstone, S., Kardefelt Winther, D., i Hussein, M. (2019.). Global Kids Online uporedno izvješće, izvješće o istraživanju Innocenti. UNICEF-ov ured 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 milijun dosjea materijala o zlostavljanju djece. U 2019. taj broj se popeo na 70 milijuna, što je skoro 50% više u odnosu na brojke iz 2018. godine. Pored toga, prvi put su videozapisi zlostavljanja premašili broj fotografija u prijavama nadležnim tijelima, što pokazuje potrebu za novim alatima za suočavanje s ovim trendom. Žrtve seksualnog iskorištavanja i zlostavljanja djece na internetu pripadaju svim starosnim skupinama, ali postaju sve mlađe. Godine 2018. mreža linija za potporu INHOPE zabilježila je promjenu profila žrtava s pubertetskih na prijepubertetske. Pored toga, istraživanje ECPAT Internationala i INTERPOL-a u 2018. godini pokazalo je kako su mlađa djeca bila podložnija biti podvrgnuta teškom zlostavljanju, uključujući mučenje, nasilno silovanje ili sadizam. To uključuje novorođenčad koja su stara samo nekoliko dana, tjedana ili mjeseci. Iako su djevojčice pogođenije, zlostavljanje dječaka može biti teže. Isto izvješće pokazuje da su 80% žrtava o kojima se govori u izvješćima bile djevojčice, a 17% dječaci. Djeca oba spola navedena su u 3% procijenjenih izvješća.[1]

Snimka podataka[2]

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

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

1 ECPAT i Interpol, “U susret globalnom pokazatelju o neidentificiranim žrtvama u materijalu seksualnog iskorištavanja djece: sažeto izvješće”, 2018.
2 Zaustavljanje nasilja nad djecom, “Sigurni na internetu”.

2.1.2 Utjecaj 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 omogućuju da istražuju svoje osobne identitete u sigurnom okruženju. Imati odgovarajuće vještine i znati kako riješiti pitanja vezana uz privatnost i reputaciju važno je za mlade ljude.

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

Međutim, budući da istraživanja pokazuju da većina djece koristi društvene medije prije navršenih trinaest godina, a usluge provjere godišta su uglavnom slabe ili ih nema, rizici s kojima se djeca mogu susresti mogu biti veoma veliki. Dalje, dok djeca žele naučiti digitalne vještine, da postanu digitalni građani i da kontroliraju postavke privatnosti, oni obično razmišljaju o privatnosti u odnosu na svoje prijatelje i poznanike - „Što mogu vidjeti moji prijatelji?“ - a manje u odnosu na strance i treće strane. Ovo, u kombinaciji s dječjom prirodnom znatiželjom i općenito s 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 videozapisa putem mobilnih aplikacija, a posebice korištenje platformi za strimovanje uživo od strane djece predstavlja daljnju zabrinutost u vezi s 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 generirane slike. Od toga je 76% pokazivalo djevojke uzrasta od 11 do 13 godina, većinom u svojim spavaćim sobama ili drugim sobama u okruženju doma. Za neku, posebno stariju djecu, to se može smatrati prirodnim istraživanjem seksualnosti i seksualnog identiteta, dok za drugu, osobitu mlađu djecu, često postoji prisila odrasle osobe ili drugog djeteta. Bez obzira na slučaj, rezultirajući sadržaj je u mnogim zemljama nezakonit i može izložiti djecu riziku od kaznenog gonjenja ili se može koristiti za daljnje iskorištavanje djeteta, vrbovanje ili iznuđivanje.

Slično tomu, **igre na internetu** omogućuju djeci da ispune svoje temeljno pravo na igru, kao i da grade mreže, provode vrijeme s prijateljima i upoznaju nove prijatelje i razvijaju važne vještine. Iako ovo može biti veoma pozitivno, u nekim slučajevima, i ako nema nadzora i potpore odgovorne odrasle osobe, platforme za igre također mogu predstavljati rizik za djecu. To uključuje pretjerano igranje, financijske rizike povezane s prekomjernim kupovinama u igri, prikupljanje i unovčavanje osobnih podataka djece od strane aktera iz IKT industrije, cyber zlostavljanje, govor mržnje, nasilje i izlaganje neprimjerenom ponašanju ili sadržaju, vrbovanje korištenjem stvarnih, kompjutorski generiranih ili čak slika iz virtualne realnosti i videozapisa koji prikazuju i normaliziraju 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 razvitak doveo je do pojave "**interneta stvari**", gdje je sve veći broj i opseg uređaja s 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 cyber maltretiranja, Microsoft je proveo istraživanje digitalne sigurnosti i cyber maltretiranja. Godine 2012. anketirao je djecu od 8 do 17 godina u 25 zemalja o negativnom ponašanju na internetu. Rezultati su pokazali da je u prosjeku 54% sudionika navelo da se brinu da će biti maltretirani na internetu, 37% je izjavilo da su doživjeli cyber maltretiranje, a 24% je otkrilo da su nekoga maltretirali. Isto istraživanje je pokazalo da je manje od troje od deset roditelja razgovaralo s djecom o nasilju na internetu. Od 2016. Microsoft provodi **redovito istraživanje** rizika na internetu dajući godišnja Izvješća o indeksu digitalne učtivosti.

FACES je multimedijalni program koji su proizveli NHK Japan i konzorcij različitih javnih servisa s pričama o žrtvama nasilja na internetu i izvan njega diljem svijeta. Serija se sastoji od portreta adolescenata u kojima protagonisti pred kamerama objašnjavaju kako su reagirali na napade putem interneta. Seriju, koja je također proizvedena u dvominutnim klipovima, prihvatili su Facebook, UNESCO, i Vijeće Europe, i dostupna je na mnogim jezicima.

U 2019. godini, UNICEF je objavio diskusijski 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, sudjelovanje 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 podatcima, besplatne igre i unovčavanje, nedostatak transparentnosti u komercijalnom sadržaju).

Dobre prakse: Tehnologija

Googleov laboratorij za virtualnu realnost ispituje kako virtualna realnost može pomoći u ohrabrivanju mladih da se bore protiv nasilja izvan interneta i na internetu.[1]

U rujnu 2019. BBC je pokrenuo mobilnu aplikaciju koja se zove **Own IT**, aplikaciju za sigurnost namijenjenu djeci od 8 do 13 godina koja dobivaju prvi pametni telefon. Aplikacija je dio BBC-jeve posvećenosti u pružanju potpore mladim ljudima u današnjem promjenjivom medijskom okruženju i prati uspješno pokretanje internet stranice Own IT u 2018. godini. Aplikacija kombinira najsuvremeniju tehnologiju strojnog 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 sigurna na internetu, nudeći prijateljske i podupiruće poticaje kada njihovo ponašanje počne odudarati od normalnog. Korisnici mogu pristupiti aplikaciji kada traže pomoć, ali im je na raspolaganju i pružanje trenutačnih savjeta i potpore na ekranu kada im je potrebna putem posebno razvijene tastature. Značajke uključuju:

- podsjećanje korisnika da dobro razmisle prije nego što podijele osobne podatke poput brojeva mobilnih telefona na društvenim medijima;
- pomoć da razumiju kako bi drugi mogli shvatiti poruke prije nego što pritisnu slanje;
- praćenje njihovog raspoloženja tijekom vremena i pružanje smjernica kako poboljšati situaciju ako je to potrebno;
- pružanje informacija o temama poput korištenja telefona kasno navečer i utjecaja na dobrobit korisnika.

Aplikacija sadrži posebice dopušten sadržaj s 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 izvješća ili povratne informacije, a niti jedan podatak neće napustiti uređaje korisnika. Aplikacija ne prikuplja nikakve osobne podatke ili sadržaj generiran od korisnika dok se cijelo strojno učenje odvija u aplikaciji i na uređaju korisnika. Strojevi se posebice podešavaju s podatcima koji se koriste za testiranje kako bi se osiguralo da nema kršenja privatnosti.

[1] Za više informacija pogledajte Alexa Hasse i dr., "Mladi i cyber 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 s invaliditetom suočavaju se s 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 s invaliditetom često se suočavaju s isključenošću, stigmatizacijom i preprekama (fizičkim, ekonomskim, društvenim i u stavovima) u sudjelovanju u svojim zajednicama. Ova iskustva mogu imati negativan utjecaj na dijete s invaliditetom i navesti ga da traži socijalne

[4] Pogledati Vijeće Europe, "Dva klika naprijed i jedan klik nazad: Izvješće 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 potpore, one također mogu takvu djecu izložiti većem riziku slučajevima vrbovanja, poticanja 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, vjerojatno će biti žrtve i na internetu. To djecu s invaliditetom stavlja u veći rizik na internetu, ali imaju i veću potrebu biti na internetu. Istraživanja pokazuju da će djeca s invaliditetom vjerojatnije doživjeti zlostavljanje bilo koje vrste,[6] a osobito je vjerojatno da će doživjeti seksualnu viktimizaciju.[7] Viktimizacija može uključivati maltretiranje, uznemiravanje, isključenje i diskriminaciju na temelju 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.

Počinitelji vrbovanja, poticanja putem interneta i / ili seksualnog uznemiravanja djece i mladih s invaliditetom mogu uključivati ne samo prijestupnike s preferencijama koji ciljaju djecu i mlade, već i one koji ciljaju djecu i mlade s invaliditetom. Takvi počinitelji mogu biti „privrženici“ - osobe koje nemaju invaliditet a koje seksualno privlače osobe s invaliditetom (najčešće osobe s 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 videozapisa djece i mladih s 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 potporom ili savjetom, što može kao rezultat imati da njihovo dijete stavlja u rizik kršenja privatnosti u tom trenutku i u budućnosti. Takvi roditelji također riskiraju da budu na meti neupućenih ili nesavjesnih ljudi koji nude tretmane, terapije ili "lijekove" za djetetov invaliditet. Jednako tako, neki roditelji djece i mladih s 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 s invaliditetom mogu se suočiti s 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 s ekrana ili prilagodljivih računarskih kontrola), ili potreba za odgovarajućom potporom (npr. podučavanje kako se koristi oprema, potpora jedan na jedan za navigaciju u društvenim interakcijama).[11]

---

5 Andrew Schrock i dr., “Poticanje, uznemiravanje i problematičan sadržaj”, Berkmanov centar za internet i društvo, 2008.

6 UNICEF, „Izvješće o stanju djece u svijetu: Djeca s invaliditetom,” 2013.

7 Katrin Mueller-Johnson i dr., “Seksualna viktimizacija mladih s tjelesnim invaliditetom: Ispitivanje razine rasprostranjenosti, rizika, i zaštitnih čimbenika”, 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 diskusijski rad 2017-03 .

10 UNICEF, “Postoji li ljestvica dječjeg sudjelovanja na internetu?”, Innocenti istraživački sažetak, 2019.

11 Za smjernice o ovim pravima, vidi Konvenciju UN-a o pravima osoba s invaliditetom i Fakultativni protokol, posebice članak 9. o pristupačnosti i članak 21. o slobodi izražavanja i mišljenja i pristupu informacijama.

2.2 Postojeći nacionalni i transnacionalni modeli za zaštitu djece na internetu

Na globalnoj razini 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 utemeljene 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 učinkovitije stvoriti „sigurne prostore“ kako bi se spriječilo zlostavljanje.

Suradnja IKT kompanija

Tehnološka koalicija je primjer uspješne suradnje 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 trebale razmatrati samo radnje koje moraju poduzeti na pravnoj razini, već i koje aktivnosti mogu obavljati i, gdje je to moguće, nastojati provoditi inicijative na globalnoj razini. Neki od modela koji pružaju načela za takve inicijative uključuju:

- Ministarska dragovoljna načela pet država za borbu protiv seksualnog iskorištavanja i zlostavljanja djece (2020);
- Povjerenstvo za širokopojasni pristup za održivi razvitak, Sigurnost 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, Sigurno za učenje: Poziv na akciju;
- Dječje dostojanstvo u digitalnom svijetu, Savez za dostojanstvo djeteta: Izvješće radne skupine za Tehnologiju (2018);
- Direktiva (EU) 2018/1808 Europskog parlamenta i Vijeća: Direktiva o audiovizualnim medijskim uslugama;
- Opća uredba Europske komisije o zaštiti podataka (2018);
- Preporuka OECD-a u pogledu sigurnosti 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 s regulatornim politikama, standardima i suradnjom s drugim sektorima. U svrhu ovog dokumenta istaknuta su ključna načela takvih modela, koji se primjenjuju na IKT kompanije.

Kodeks dizajna prilagođenog uzrastu, Velika Britanija

Početkom 2019. godine Ured povjerenika za informacije objavio je prijedloge za svoj kodeks za dizajniranje prilagođeno uzrastu radi unaprjeđenja zaštite dječjih podataka. Predloženi kodeks utemeljen 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 osobnih 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 cyber zlostavljanje je okarakterizirano kao specifično kazneno djelo i fokusira se na širok raspon šteta, od cyber maltretiranja do pornografije iz osvete. Cilj mu je obeshrabriti, spriječiti i umanjiti štetnu digitalnu komunikaciju, čineći nezakonitim postavljanje digitalne komunikacije s namjerom da se izazove ozbiljna emocionalna uznemirenost kod druge osobe, i postavlja niz od 10 načela komunikacije. Omogućuje korisnicima da se žale neovisnoj organizaciji ako su ova načela prekršena ili se primjenjuju na sudske naloge protiv autora ili domaćina komunikacije ako problem nije riješen.

Povjerenik eSafety, Australija

Utemeljen 2015. godine, australijski Povjerenik eSafety prva je svjetska vladina agencija posvećena borbi protiv zlouporabe na internetu i održavanju sigurnosti svojih građana na internetu. Kao nacionalni neovisni regulator za sigurnost 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 eSafetyju ovlasti da brzo ukloni cyber maltretiranje, zlostavljanje utemeljeno na slikama i nezakonit sadržaj na internetu. Ova široka nadležnost omogućuje eSafety-ju da se brine o sigurnosti na internetu na višestran, cjelovit i proaktivan način.

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

1) **Odgovornosti pružatelja usluga**: teret sigurnosti nikada ne bi trebao pasti na krajnjeg korisnika. Mogu se poduzeti preventivni koraci kako bi se osiguralo da se poznate i predviđene štete procijene u dizajnu i pružanju usluga na internetu, zajedno s koracima kako bi se smanjila vjerojatnoća 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 omogućujući korisnicima veću kontrolu, upravljanje i regulaciju vlastitih iskustava.
3) **Transparentnost i odgovornost**: ovo su obilježja snažnog pristupa sigurnosti, koje pružaju jamstva da službe djeluju sukladno objavljenim sigurnosnim ciljevima, kao i edukacija i davanje mogućnosti javnosti da poduzmu mjere radi rješavanja sigurnosnih problema.

Globalni savez WeProtect

U središtu strategije WePROTECT Globalnog saveza je potpora zemljama da razviju koordinirane odgovore više interesnih strana za borbu protiv seksualnog iskorištavanja djece na internetu, vođene svojim Modelima nacionalnog odgovora, koji djeluju kao nacrt za djelovanje na nacionalnoj razini. 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 obveza za IKT kompanije koje se odnose na:

- postupke obavještavanja i uklanjanja;
- prijavljivanje seksualnog iskorištavanja i zlostavljanja djece (CSEA);
- razvitak tehnoloških rješenja; i
- investiranje u učinkovite preventivne programe i usluge reagiranja 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 glavni tajnik Ujedinjenih naroda 2016. godine s jednim ciljem: katalizirati i podržati akciju za zaustavljanje svih oblika nasilja nad djecom do 2030. godine, kroz jedinstvenu suradnju više od 400 partnera iz svih sektora.

Fokus rada je na spašavanju i pružanju potpore žrtvama, tehnološkim rješenjima za otkrivanje i sprječavanje prekršaja, pružanju potpore tijelima za provedbu zakona, zakonodavnim i političkim reformama, i generiranju podataka i dokaza o razmjerima 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 poduzeti mjere za zaštitu djece i mladih kada koriste IK tehnologije i da promoviraju njihovu pozitivnu uporabu IK tehnologija.

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

Razmatranje integracije prava djeteta zahtijeva da kompanije poduzmu odgovarajuće mjere za identificiranje, sprječavanje, ublažavanje i, po potrebi, saniranje potencijalnih i stvarnih negativnih utjecaja na dječja prava. Vodeća načela UN-a o poslovanju i ljudskim pravima pozivaju sva poduzeća 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 pozornost djeci i mladima kao ranjivoj skupini s obzirom na njihovu zaštitu podataka i slobodu izražavanja. Rezolucija Opće skupštine Ujedinjenih naroda 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 Vijeća 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 razvitku i potvrđuje da ista prava koja ljudi imaju izvan interneta također 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 pratiti pojačanu dubinsku analizu kako bi osigurale da su politike i prakse sukladne međunarodnom pravu. 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 operativnoj razini koji će osigurati format za pogođene pojedince da izraze zabrinutost zbog potencijalnih prekršaja. Mehanizmi na operativnoj razini trebaju biti dostupni djeci, njihovim obiteljima i onima koji zastupaju njihove interese. Načelo 31 Vodećih načela o poslovanju i ljudskim pravima pojašnjava da takvi mehanizmi trebaju biti legitimni, dostupni, predvidljivi, nepristrasni, transparentni, kompatibilni s pravima, izvor kontinuiranog učenja i utemeljeni na angažiranju i dijalogu. Zajedno s internim procesima za rješavanje negativnih utjecaja, 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 trebaju zauzeti pristup prema IKT sigurnosti utemeljen na usklađenosti koji se fokusira na ispunjavanje nacionalnog zakonodavstva, slijeđenje međunarodnih smjernica kada nema nacionalnog zakonodavstva i izbjegavanje negativnih utjecaja na prava djece i mladih, i da kompanije proaktivno promoviraju razvitak i dobrobit djece i mladih volonterskim akcijama koje unaprjeđuju prava djece i mladih na pristup informacijama, slobodu izražavanja, sudjelovanje, obrazovanje i kulturu.

Dobre prakse: Dizajn koji odgovara politici i uzrastu

Kompanija za razvitak 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 sigurne dječje privatnosti CORPA programa za certifikaciju sigurnih utočišta.

LEGO® Life je primjer sigurne platforme društvenih medija za djecu mlađu od 13 godina za dijeljenje svojih LEGO kreacija, za dobijanje inspiracije i sigurnu interakciju. Ovdje se od djece ne traže nikakvi osobni podatci za stvaranje profila, za što je samo potrebna adresa e-pošte roditelja ili skrbnika. Aplikacija stvara priliku djeci i obiteljima da razgovaraju o sigurnosti na internetu i privatnosti u pozitivnom okružju.

Primjeri dizajna primjerenog uzrastu uključuju specifične ponude nekih od velikih javnih servisa za određene starosne skupine: primjerice, 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 skupinama.

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, trenutačno se proaktivno pojavljuju korištenjem tehnologije, umjesto da se oslanjaju na prijavljivanje Twitteru. Nova tehnologija se koristi za bavljenje političkim sadržajima polja privatnog informiranja, osjetljivim medijima, ponašanjem iz mržnje, zlostavljanjem i lažnim predstavljanjem.

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

3.2 Razvitak 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 tisuće slika i videozapisa. Od slika nad kojima je IWF poduzela 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, tijela za provedbu zakona i civilnog društva u borbi za prevenciju materijala seksualnog zlostavljanja djece.

[13] IWF, "Zašto. Kako. Tko. I rezultati. Godišnje izvješće 2019".

Iako se mnoge vlade bore protiv širenja i distribucije materijala seksualnog zlostavljanja djece donošenjem zakona, progonom i procesuiranjem nasilnika, podizanjem svijesti i pružanjem potpore djeci i mladima u oporavku od zlostavljanja ili iskorištavanja, postoje mnoge zemlje koje još uvijek nemaju uspostavljene odgovarajuće sustave. U svakoj zemlji su potrebni mehanizmi koji će omogućiti široj javnosti da prijavi nasilni i eksploatacijski sadržaj ove prirode. IKT kompanije, tijela za provedbu zakona, vlade i civilno društvo moraju surađivati kako bi osigurali uspostavu odgovarajućeg pravnog okvira sukladno međunarodnim standardima. Takvi okviri bi trebalo inkriminirati sve oblike seksualnog iskorištavanja i zlostavljanja djece, uključujući i materijal seksualnog zlostavljanja djece, i zaštititi djecu koja su žrtve takvog zlostavljanja ili iskorištavanja. Ti okviri moraju osigurati da procesi prijavljivanja, istrage i uklanjanja sadržaja rade što učinkovitije.

IKT kompanije bi trebale osigurati veze do nacionalnih linija za potporu ili drugih lokalno dostupnih linija za potporu, poput IWF portala u nekim zemljama, a u nedostatku lokalnih mogućnosti prijavljivanja, osigurati veze do drugih međunarodnih linija za potporu po potrebi, kao što je Američki nacionalni centar za nestalu i zlostavljanu djecu (NCMEC) ili Međunarodna udruga internetskih linija za potporu (INHOPE), gdje se bilo koja međunarodna linija za potporu 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 uvjete i odredbe ili kodekse ponašanja koji izričito zabranjuju takav sadržaj ili ponašanje;[14] razvijanje snažnih procesa obavještavanja i uklanjanja; te rad i potpora nacionalnim linijama za potporu.

Pored toga, neke kompanije primjenjuju tehničke mjere kako bi spriječile zlouporabu svojih usluga ili mreža za dijeljenje poznatog materijala seksualnog zlostavljanja djece. Primjerice, neki operateri 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 potporu. 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 obvezati 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 poticanje odgovorne i sigurne uporabe tehnologije, s fokusom na samu tehnologiju, samoupravljanje, partnerstva i obrazovanje i dopiranje do potrošača. Microsoft je također ugradio funkcije koje daju mogućnost pojedincima da učinkovitije upravljaju sigurnošću na internetu. "Obiteljska sigurnost" je jedna od takvih značajki koja omogućuje roditeljima i skrbnicima da nadgledaju uporabu interneta svoje djece.

Microsoft provodi politike protiv uznemiravanja na svojim platformama, a korisnici koji zlouporabljavaju ove propise podliježu ukidanju profila ili, u slučaju ozbiljnijih kršenja, mjerama za provedbu 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 uspoređuje ih s bazom podataka heševa koji su već identificirani i za koje je potvrđeno da su materijal seksualnog zlostavljanja djece. Ako pronađe podudaranje, slika se blokira. Ovaj je alat omogućio operaterima sadržaja uklanjanje milijuna nezakonitih fotografija s 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 videozapisa bio je logičan sljedeći korak. Međutim, ovaj alat ne koristi tehnologiju prepoznavanja lica niti može identificirati osobu ili predmet na slici. Ali s pojavom PhotoDNA for Video stvari su poprimile novi zaokret. PhotoDNA for Video rastavlja videozapis u ključne kadrove i u osnovi stvara heševe 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 videozapis koji bi u protivnom mogao izgledati bezazlen.

Štoviše, Microsoft je u skorije vrijeme objavio novi alat za prepoznavanje dječjih predatora koji u chatovima na internetu vrbuju djecu zbog zlostavljanja. Projekt Artemis, razvijen u suradnji s kompanijama The Meet Group, Roblox, Kik i Thorn, nadovezuje se na Microsoftovu patentiranu tehnologiju i putem Thorna će biti dostupan besplatno kvalificiranim uslužnim kompanijama na internetu koje nude funkciju chata. Projekt Artemis je tehnički alat koji daje upozorenja administratorima kada je potrebna moderacija u chat-sobama. Ovom tehnikom otkrivanja vrbovanja moći će otkriti, reagirati 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, osigurane kvalitete;
- heš listu poznatog kriminalnog sadržaja koji se odnosi na materijal seksualnog zlostavljanja djece;
- jedinstvenu lista ključnih riječi tajnih izraza za koje se zna da su povezane s materijalima seksualnog zlostavljanja djece;
- popis detalja o nazivima domena koje su poznate po hostiranju sadržaja seksualnog zlostavljanja djece kako bi se omogućilo brzo uklanjanje domena u kojima se nalazi nezakoniti sadržaj.

3.3 Stvaranje sigurnijeg okruženja na internetu prilagođenog uzrastu

Vrlo malo stvari u životu može se smatrati apsolutno sigurnim i bez rizika sve vrijeme. Čak se i u gradovima u kojima je kretanje prometa visoko regulirano i strogo kontrolirano, nesreće se i dalje dešavaju. Na isti način, cyber prostor nije bez rizika, osobito za djecu i mlade. O djeci i mladima se može razmišljati kao o primateljima, sudionicima i akterima u njihovom okružju na internetu. Rizici s kojima se suočavaju mogu se podijeliti u četiri područja:[15]

[15] Sonia Livingstone i dr., "EU Kids Online: Završno izvješće", Londonska škola ekonomije, 2009.

- *Neprimjeren sadržaj* - Djeca i mladi mogu naići na neprimjeren i nezakonit sadržaj dok traže nešto drugo klikom na vjerojatno bezazlen link u instant poruci, na blogu ili prilikom dijeljenja datoteka. Oni također 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 promovira zlouporabu opojnih droga, rasnu mržnju, rizično ponašanje, samoubojstvo, anoreksiju ili nasilje.
- *Neprimjereno ponašanje* - Djeca i odrasli mogu koristiti internet za uznemiravanje ili čak iskorištavanje drugih ljudi. Djeca mogu ponekad emitirati 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 web kameru ili drugi uređaj za snimanje, ili će pokušati ugovoriti osobni sastanak i fizički kontakt. Ovaj se proces često naziva „vrbovanje“.
- *Komercijalni rizici* - Ova kategorija odnosi se na rizike narušavanja privatnosti podataka koji se odnose na prikupljanje i uporabu dječjih podataka, kao i digitalni marketing. Sigurnost na internetu je izazov zajednice i prilika za IKT kompanije, vlade i civilno društvo da rade zajedno na uspostavi sigurnosnih načela i praksi. IKT kompanije mogu ponuditi čitav niz tehničkih pristupa, alata i usluga za roditelje, djecu i mlade, i prije svega treba napraviti proizvode koji su jednostavni za uporabu, sigurni po dizajnu i primjereni uzrastu za njihov širok spektar korisnika. Dodatni pristupi uključuju ponudu alata za razvitak odgovarajućih sustava 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 s kojima djeca mogu imati kontakt ili vrijeme u kojem mogu koristiti internet. Ono što je najvažnije, okviri „sigurnost po dizajnu“[16], uključujući i privatnost, moraju biti uključeni u procese razvijanja inovacija i dizajna proizvoda. Dječja sigurnost i odgovorno korištenje tehnologije moraju se pažljivo razmotriti i o njima se ne smije misliti naknadno.

Neki programi omogućuju 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 obitelji.

Politike prihvatljive uporabe jedan su od načina na koji IKT kompanije mogu utvrditi kakvo se ponašanje potiče 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 pravodobno pružanje informacija o statusu prijave. Iako kompanije mogu različito primjenjivati prateće mehanizme od slučaja do slučaja, bitno je postaviti jasan vremenski okvir za reagiranje, priopćiti odluku donesenu u vezi s prijavom i ponuditi način rješavanja ako korisnik nije zadovoljan odgovorom.

16 Povjerenik eSafety, Pregled sigurnosti po dizajnu, 2019.

Dobre prakse: Izvještavanje

Facebook je, u nastojanju da suzbije seksualno uznemiravanje na digitalnim platformama, sufinancirao projekt deSHAME s Europskom unijom, suradnju između Childnet, Save the Children, Kek Vonal i UCLan. Cilj ovog projekta je povećati prijavljivanje seksualnog uznemiravanja putem interneta među maloljetnicima i poboljšati multisektorsku suradnju u prevenciji i reagiranju na ovakvo ponašanje.

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

Operateri sadržaja i usluga na internetu mogu također opisati prirodu sadržaja ili usluga koje pružaju i predviđeni ciljni starosni raspon. Ovi bi opisi trebali biti usklađeni s postojećim nacionalnim i međunarodnim standardima, relevantnim propisima i savjetima o marketingu i oglašavanju za djecu koje odgovarajuća tijela za klasifikaciju stavljaju na raspolaganje. Ovaj proces postaje sve kompliciraniji s rastućim spektrom interaktivnih usluga koje omogućuju objavljivanje korisničkog sadržaja, primjerice putem oglasnih ploča, chat soba i usluga društvenih mreža. Kada kompanije posebice 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 sigurnosti bit će mnogo veća.

Kompanije se također 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 osobne posljedice otkrivanja ili pristanka na dijeljenje svojih osobnih podataka na internetu ili na uporabu njihovih osobnih podataka u komercijalne svrhe. Usluge usmjerene na ili koje bi vjerojatno privukle kao glavnu publiku djecu i mlade moraju uzeti u obzir rizike u kojima se mogu naći zbog pristupa ili prikupljanja i uporabe osobnih podataka (uključujući podatke o lokaciji) i osigurati da se ti rizici rješavaju na pravi način i da su korisnici informirani. 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 osobni podatci, pomažu razumijevanju i pomažu korisnicima u upravljanju zaštitom njihove privatnosti na jasan i jednostavan način i da objašnjavaju na što pristaju jasnim, razumljivim jezikom.

Dobre prakse: Inovacija

U 2018. – 2019. UNICEF-ov Regionalni ured za Istočnu Aziju i Pacifik organizirao je pet okruglih stolova s više interesnih strana radi razmjene obećavajućih praksi IKT kompanija za borbu protiv seksualnog iskorištavanja i zlostavljanja djece na internetu. Sudionici 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 Međunarodnu liniju za pomoć djeci.

U sklopu istog projekta, u veljači 2020. godine, UNICEF je pokrenuo Think Tank kako bi ubrzao liderstvo u IKT kompanijama u istočnoj Aziji i pacifičkoj regiji kako 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 razvitak utjecajnih obrazovnih materijala i identifikaciju najučinkovitijih platformi za isporuku, kao i za razvitak okvira za evaluaciju koji može izmjeriti utjecaj ovih obrazovnih materijala i poruka usmjerenih na djecu. Think Tank čine Facebook, Telenor, akademski stručnjaci, agencije Ujedinjenih naroda, 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 Tanka, 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 temelju preuzimanja sigurnosnih materijala i poruka na internetu.

3.4 Edukacija djece, roditelja i edukatora o sigurnosti djece i njihovoj odgovornoj uporabi IK tehnologija

Tehničke mjere mogu biti važan dio osiguranja zaštite djece i mladih od potencijalnih rizika na internetu, ali one su samo jedan element jednadžbe. **Alati za roditeljsku kontrolu, podizanje svijesti** i obrazovanje također su ključne komponente koje će pomoći u osnaživanju i informiranju djece i mladih svih uzrasta, kao i roditelja, skrbnika i edukatora. Iako kompanije imaju važnu ulogu u poticanju djece i mladih da koriste IK tehnologije na odgovoran i siguran način, tu odgovornost dijele s 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, skrbnicima i edukatorima u usmjeravanju djece i mladih prema sigurnijim, 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, uvjeti pretplate i način otkazivanja pretplate jasno priopćavaju. Promoviranje poštovanja uvjeta minimalne starosne granice od strane društvenih medija u svim zemljama u kojima je moguće provjeravanje starosti također bi pomoglo u zaštiti djece omogućavanjem pristupa uslugama odgovarajućem uzrastu. Važno razmatranje koje treba uskladiti s ovom preporukom je dodatno prikupljanje osobnih podataka koje ovo može podrazumijevati i potreba da se ograniči prikupljanje i čuvanje ovih podataka i njihova obrada.

Također je važno pružiti informacije djeci i mladima izravno o sigurnijoj uporabi IK tehnologija i pozitivnom i odgovornom ponašanju. Pored podizanja svijesti o sigurnosti, 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 poduzeti 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 nego djeca i mladi. Štoviše, spajanje mobilnih uređaja i internet usluga otežava roditeljski nadzor. IKT kompanije mogu raditi u suradnji s 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 uporabu IK tehnologija od strane djece i mladih samo na roditelje, već prepoznati da su roditelji u boljoj poziciji odlučiti što je prikladno za njihovu djecu i da ih treba upoznati sa svim rizicima kako bi bolje zaštitili svoju djecu i osnažiti ih za poduzimanje 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 surađivati sa školskim distriktima kako bi se pripremili nastavni planovi i programi o sigurnosti na internetu i odgovornoj uporabi 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 poduzimaju ako se dijete suočava s maltretiranjem ili vrbovanjem na internetu, kako izbjeći neželjenu poštu i upravljati podešavanjima privatnosti i kako razgovarati s dječacima i djevojčicama različitih starosnih skupina 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 sigurnog uživanja u njoj. Iako je važno djecu naučiti odgovornom korištenju interneta, znamo da djeca vole eksperimentirati, riskirati, 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 učinak 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 utjecaj neugodnog iskustva i pretvoriti ga u korisnu lekciju za budućnost.

Dobre prakse: Obrazovanje

NHK Japan vodi kampanju prevencije samoubojstava za mlade na Twitteru: U Japanu samoubojstva 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. kolovoza. Povezujući televiziju, prijenos uživo i društvene medije, NHK je uspješno stvorio "mjesto" na kojem su tinejdžeri mogli bez straha podijeliti svoja osjećanja.

Dobre prakse: Obrazovanje

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

Projekat deSHAME, koji sufinanciraju Facebook i Europska unija, također omogućuje stvaranje resursa za širok raspon starosnih skupina, s 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 reagiranja. Projekt će ove materijale za učenje prenijeti drugim europskim zemljama i partnerima diljem svijeta u svrhu promocije digitalnih prava mladih.

Google je razvio niz obrazovnih inicijativa, resursa i alata koji pomažu u promociji sigurnosti za mlade na internetu. Jedna od njih je kampanja Budi sjajan na internetu organizirana oko digitalnog građanstva, kreirana u suradnji s organizacijama kao što su ConnectSafely, Obiteljski institut za sigurnost na internetu i koalicija Internet Keep Safe. Ova je kampanja usmjerena na mlade ljude uzrasta od 8 do 11 godina. Sadrži internetsku igru za mlade (Interland) koja podučava osnovama digitalne sigurnosti i resurse za edukatore, poput digitalnog građanstva i sigurnosnog plana i programa. Sigurnosni plan i program nudi planove lekcija za pet ključnih tematskih područja kampanje, od kojih se jedno fokusira na cyber maltretiranje. Kao dodatak ovome Google je napravio kurs digitalnog građanstva i sigurnosti na internetu za edukatore učenika svih starosnih skupina, pružajući daljnju potporu za integriranje digitalnog građanstva i sigurnosnih aktivnosti u učionici. Google također nudi nekoliko programa koji pomažu mladima da se izravno uključe u napore na polju sigurnosti na internetu i na polju digitalnog građanstva. Globalna inicijativa Web Rangers jedan je od takvih programa koji mlade podučava o sigurnosti na internetu i potiče ih da kreiraju vlastite kampanje oko pozitivne i sigurne uporabe 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 **Eurovizijskoj razmjeni vijesti za mlade**, Europska radiodifuzna unija okuplja 15 europskih televizijskih kuća kako bi razmjenjivale programe, formate i rešenja 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 operaterom internetskih, kablovskih i telefonskih usluga u Peruu, sa 14.4 milijuna korisnika, uključujući više od 8 milijuna Movistar mobilnih korisnika.

Nekoliko aktivnosti je provedeno u okviru ovog plodnog partnerstva:

- **Virtualni tečaj o zaštiti djece na internetu** je razvijen od strane kompanije Telefónica uz tehničku potporu Capital Humano y Social Alternativo. Ovaj tečaj 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 virtualnom tečaju putem svoje službene internet stranice.
- **Knjižica o sigurnosti na internetu** napravljena je od strane Capital Humano y Social Alternativo, a kompanija Telefónica je distribuira u više od 300 mobilnih prodajnih centara. Cilj je podići svijest korisnika Telefónice o sigurnosti 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 potporu Capital Humano y Social Alternativo, koju njezini korisnici mogu igrati dok čekaju svoje redove u trgovinama

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

3.5 Promoviranje digitalne tehnologije kao načina za povećanje građanskog angažmana

Članak 13. Konvencije o pravima djeteta UN-a kaže da „dijete ima pravo na slobodu izražavanja; to pravo mora, neovisno o granicama, uključivati slobodu traženja, primanja i širenja obavijesti i ideja svake vrste, usmeno ili pismeno, tiskanjem, 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 sudjelovanje i izražavanje ili sprječavanje pristupa informacijama koje su važne za njihovu dobrobit. Neophodno je osigurati da sustavi provjere starosti ne ugrožavaju istinsku potrebu određenih starosnih skupina za pristup sadržajima koji su relevantni za njihov razvitak.

Istodobno, poduzeća i IKT kompanije također mogu podržati prava djece i mladih pružajući mehanizme i alate za olakšavanje sudjelovanja mladih. Oni mogu naglasiti sposobnost interneta da olakša pozitivan angažman u širem građanskom životu, pokreće društveni napredak i utječe na održivost i otpornost zajednica, primjerice, sudjelovanjem 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 osobno pogađaju, poput njihovog seksualnog zdravlja, i o političkoj i vladinoj odgovornosti.

Kompanije također mogu ulagati u stvaranje internetskih iskustava primjerenih djeci i mladima i obiteljima. One mogu podržati razvitak tehnologije i sadržaja koji potiču i omogućuju djeci i mladima da uče, stvaraju inovacije i prave rješenja. Uvijek bi trebali imati na umu sigurnost po dizajnu u svojim proizvodima.

Pored toga, kompanije mogu proaktivno podržati prava djece i mladih radeći na uklanjanju digitalne podjele. Za sudjelovanje djece i mladih potrebna je digitalna pismenost
- sposobnost razumijevanja i interakcije u digitalnom svijetu. Bez ove mogućnosti, građani ne mogu sudjelovati u mnogim društvenim funkcijama koje su postale digitalizirane, uključujući podnošenje prijava za porez, pružanje potpore 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 kako 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. Talijanski parlament, primjerice, 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 sudjelovanja mladih iz mobilne zajednice pogledajte ovdje.

Dobre prakse: Višeagencijska suradnja

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, suosjećanje i inkluzivnost koji su srce digitalnog građanstva. Inicijativa nudi edukatorima male djece (kampanja je usmjerena na djecu uzrasta do 8 godina) i obiteljima 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. Opće smjernice za IKT kompanije

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

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

Tablica 1. Opće smjernice za IKT kompanije

Razmatranja o integraciji prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja	IKT kompanije mogu identificirati, spriječiti i ublažiti negativne utjecaje IK tehnologija na prava djece i mladih, i identificirati mogućnosti za potporu u napretku prava djece i mladih poduzimanjem 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 ovlasti 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 integriranjem 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).
	Integriranjem dubinske analize o pitanjima zaštite djece na internetu u postojeće okvire ljudskih prava ili procjene rizika (na razini korporacije, proizvoda ili tehnologije i / ili države) kako bi se utvrdilo može li poduzeće ili IKT kompanije svojim aktivnostima izazivati ili doprinositi negativnim utjecajima ili mogu li se negativni utjecaji izravno pripisati njegovom poslovanju, proizvodima ili uslugama ili poslovnim odnosima.
	Prepoznavanjem utjecaja na dječja prava različitih starosnih skupina kao rezultata poslovanja kompanije i dizajna, razvitka i uvođenja proizvoda i usluga, kao i mogućnosti za potporu pravima djece i mladih.

Razmatranja o integraciji prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja (nastavak)	Usvajanjem pristupa dječjoj zaštiti utemeljenoj na osnaživanju i obrazovanju. Uzimanjem u obzir prava djeteta na zaštitu podataka, njihovog prava na privatnost i slobodu govora, istodobno nudeći obrazovanje i smjernice kroz usluge kompanije.
	Oslanjanjem na internu i eksternu stručnost i savjetovanje s ključnim interesnim stranama, uključujući djecu i mlade, o mehanizmima za sigurnost 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 sukladne međunarodnim standardima. Pogledati Rezoluciju Opće skupštine Ujedinjenih naroda 68/167 o pravu na privatnost u digitalno doba.
	Osiguravanjem pristupa pravnom lijeku uspostavom mogućnosti žalbi na operativnoj razini i kroz mehanizme prijavljivanja bilo kakvih kršenja prava djeteta (npr. materijal seksualnog zlostavljanja djece, neprimjeren sadržaj ili kontakt ili kršenje privatnosti).
	Imenovanjem rukovoditelja politike zaštite djece ili druge određene osobe koja se može kontaktirati u vezi s pitanjima zaštite djece na internetu. Ako je dijete u opasnosti od štete, rukovoditelj politike zaštite djece treba odmah upozoriti odgovarajuće vlasti. Uredničke smjernice BBC-a (2019.), primjerice, određuju imenovanje rukovoditelja politike zaštite djece, što se u javnim medijima smatra obvezatnim.
Razvitak 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 značajke.
Razvitak standardnih postupaka za rukovanje materijalima seksualnog zlostavljanja djece	U suradnji s vladom, tijelima za provedbu zakona, civilnim društvom i organizacijama linija za potporu, IKT kompanije imaju ključnu ulogu u borbi za suzbijanje materijala seksualnog zlostavljanja djece poduzimanjem sljedećih radnji:
	Zabraniti učitavanje, objavljivanje, prijenos, dijeljenje ili stavljanje na raspolaganje sadržaja koji krši prava bilo koje strane ili krši bilo koji lokalni, državni, nacionalni ili međunarodni zakon.
	Komunicirati s nacionalnim agencijama za provedbu zakona ili nacionalnim linijama za potporu kako bi prenijeli prijave materijala seksualnog zlostavljanja djece čim operater sazna za njih. Osigurati da postoje interne procedure za usklađivanje odgovornosti za prijavljivanje prema lokalnim i međunarodnim zakonima. Kada kompanija posluje na tržištima s manje razvijenim regulatornim nadzorom i nadzorom nad provedbom zakona u vezi s ovim pitanjem, ona može uputiti one koji žele podnijeti prijave na Međunarodnu udrugu internetskih linija za potporu (INHOPE), gdje se može izvršiti prijava na bilo kojoj međunarodnoj liniji za potporu.

Razvitak 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 trebali izvještavati o poduzetim radnjama i rezultatima koje je postigao ovaj tim u svom godišnjem izvješću o korporaciji i održivosti. Kada nacionalni propisi ne pružaju dovoljnu zaštitu, IKT kompanije bi trebale poštovati, ali prevazići nacionalno zakonodavstvo i uporabiti 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 izvješćima o korporaciji i održivosti i dostupan javnosti.
	Navesti da će poduzeće u potpunosti surađivati u istragama tijela za provedbu zakona u slučaju da se nezakonit sadržaj prijavi ili otkrije i da će se zabilježiti detalji u vezi s kaznama kao što su novčane kazne ili ukidanje privilegija naplate.
	Koristiti uvjete i odredbe za korisnike i / ili prihvatljive politike uporabe za izričito navođenje stava kompanije o zlouporabi njegovih usluga za čuvanje ili dijeljenje materijala seksualnog zlostavljanja djece i posljedicama bilo koje zlouporabe.
	Razviti postupke obavještavanja, uklanjanja i izvještavanja koji omogućuju korisnicima da prijave materijal seksualnog zlostavljanja djece ili neprimjeren kontakt i određeni profil / lokaciju gdje je otkriven. Uspostaviti izvješće o pratećem postupku, dogovoriti se o procedurama za prikupljanje dokaza i brzo uklanjanje ili blokiranje pristupa materijalu seksualnog zlostavljanja djece. Osigurati da operateri 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 s 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 prijaviti slučajeve odgovarajućim vlastima. Ako odnos s tijelima za provedbu zakona i nacionalnom linijom za potporu već nije uspostavljen, trebaju se angažirati da zajedno razvijaju procese.
	Raditi putem internih funkcija, kao što su briga o korisnicima, sprječavanje prijevara i sigurnost, kako bi se osiguralo da poduzeće može podnositi prijave za sumnju na nezakonit sadržaj izravno tijelima za provedbu zakona i linijama za potporu. 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, provesti politiku ili program za pružanje potpore za razvitak otpornosti, sigurnosti i dobrobiti osoblja.

Razvitak standardnih postupaka za rukovanje materijalima seksualnog zlostavljanja djece (nastavak)	Uključiti politike zadržavanja i čuvanja podataka za potporu tijelima za provedbu zakona u slučaju kaznenih istraga kroz aktivnosti kao što je prikupljanje dokaza. Dokumentiranje prakse kompanije prilikom rukovanja materijalom seksualnog zlostavljanja djece, počevši od praćenja i nastavljajući se do konačnog prijenosa i uništavanja sadržaja. U dokumentaciju uključiti spisak cijelog osoblja odgovornog za rukovanje materijalom.
	Promovirati mehanizme prijavljivanja materijala seksualnog zlostavljanja djece i osigurati da korisnici znaju kako podnijeti prijavu ako otkriju takav sadržaj. Ako je dostupna nacionalna linija za potporu, ponudite vezu do te linije za potporu s korporativne internet stranice i s bilo kojih relevantnih usluga sa sadržajima koje kompanija promovira.
	Koristiti se svim relevantnim uslugama / skupovima podataka kako bi spriječili širenje poznatog sadržaja seksualnog zlostavljanja djece putem svojih usluga ili platformi.
	Redovito aktivno procjenjivati sav sadržaj hostiran na serverima kompanije, uključujući komercijalne (brendirane operatere sadržaja ili one ugovorene s trećim osobama). Razmislite o uporabi 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 sigurnijeg okruženja na internetu prilagođenog uzrastu	IKT kompanije mogu pomoći u stvaranju sigurnijeg, ugodnijeg digitalnog okruženja za djecu i mlade svih uzrasta poduzimanjem sljedećih radnji:
	Usvojiti načela sigurnosti 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 uvjeta 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 naglasiti 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 skrbnike.
	Koristiti uvjete usluge ili uvjete i odredbe kako biste skrenuli pažnju korisnicima na sadržaj na internetskim uslugama kompanije koji možda nije primjeren za sve uzraste. Uvjeti i odredbe također trebaju uključiti jasne mehanizme za prijavljivanje i postupanje u slučaju kršenja takvih pravila.

Stvaranje sigurnijeg okruženja na internetu prilagođenog uzrastu **(nastavak)**	Razmotriti mogućnost pružanja mehanizama kao što su softver za roditeljsku kontrolu i drugi alati koji omogućuju roditeljima i skrbnicima da upravljaju pristupom djeci internetskim resursima, istodobno im pružajući smjernice o njihovoj odgovarajućoj uporabi kako se ne bi kršila dječja prava. Oni uključuju liste za blokiranje / dozvolu pristupa, filtere sadržaja, nadzor uporabe, upravljanje kontaktima i vremenska / programska ograničenja.
	Ponuditi jednostavne opcije roditeljskog nadzora koje roditeljima i skrbnicima omogućuju ograničavanje određenih usluga i sadržaja kojima djeca mogu pristupiti kada koriste elektroničke uređaje. Ova ograničenja mogu uključivati kontrole na razini interneta, uređaja i kontrole aplikacija. Budući da ovo ima ogromne implikacije na djetetovu sposobnost da unaprijedi svoje digitalne vještine i na smanjivanje njegovih mogućnosti na internetu, ove bi kontrole trebale biti dizajnirane za vrlo malu djecu sukladno njihovom razvojnom kontekstu i s odgovarajućim smjernicama za roditelje.
	Tamo gdje je to moguće, promovirati nacionalne službe potpore koje roditelji i skrbnici mogu koristiti za prijavljivanje kršenja prava i traženje potpore u slučaju zlostavljanja ili iskorištavanja.
	Izbjegavati štetne ili neprimjerene reklamne sadržaje na internetu i uspostaviti obvezu za operatere usluga da otkrivaju klijente sa sadržajem koji je namijenjen odrasloj publici i može biti štetan za djecu i mlade. Štetno oglašavanje također može uključivati oglašavanje hrane i pića koja sadrže puno masti, šećera ili soli. Uskladiti poslovne prakse s 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 poduzeća mogu prikupiti osobne podatke od djeteta ili o djetetu.
	Prilagoditi i primijeniti povišena podrazumijevana podešavanja privatnosti za prikupljanje, obradu, skladištenje, prodaju i objavljivanje osobnih podataka, uključujući informacije u vezi s 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, sigurnost 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 identificirati uzrast korisnika i predstaviti im verziju aplikacije koja odgovara uzrastu. Za sadržaj ili usluge osjetljive na uzrast, interesne strane u IKT industriji bi trebale poduzeti 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 također trebale prepoznati potencijal zlouporabe takvih tehnologija s ciljem ograničavanja prava djece i mladih na slobodu izražavanja i pristupa informacijama ili ugrožavanja njihove privatnosti.

Stvaranje sigurnijeg okruženja na internetu prilagođenog uzrastu **(nastavak)**	Osigurati da su sadržaj i usluge koji nisu prikladni za korisnike svih starosnih skupina: • klasificirani sukladno nacionalnim standardima i kulturnim normama; • sukladno postojećim standardima u ekvivalentnim medijima; • identificirani s istaknutim opcijama prikaza za kontrolu pristupa; • u ponudi zajedno s provjerom starosti, gdje je to moguće i uz jasne uvjete koji se odnose na brisanje bilo kojih podataka koji se mogu koristiti za osobnu identifikaciju koji su dobiveni kroz postupak provjere. Primjerice, s obzirom na medijske standarde, sva regulatorna tijela za medije postavljaju niz zahtjeva koji se odnose na sadržaj prilagođen uzrastu, a operateri interneta moraju prilagodiit spremišta i primijeniti 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 zlouporabama, 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 s 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 stranica mržnje radi ponižavanja žrtve; • slanje lančanih poruka i priloga sa štetnom namjerom; • hakiranje nečijeg profila radi slanja uvrjedljivih poruka drugima.
	Poduzeti posebne mjere opreza s članovima osoblja ili suradnicima koji rade s 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 rukovoditelju politike zaštite djece, gdje je to moguće; • omogućiti korisnicima da izravno prijave nadležnim tijelima slučajeve vrbovanja; • uspostaviti mogućnost izravnog kontakta putem adresa e-pošte radi upozorenja i prijavljivanja.
	U svakom trenutku dati prioritet sigurnosti i dobrobiti djeteta. Djelovati uvijek u profesionalnim granicama i osigurati da je svaki kontakt s djecom važan za uslugu, program, događaj, aktivnost ili projekt. Nikada ne preuzimajte isključivu odgovornost za dijete. Ako je djetetu potrebna njega, upozoriti roditelja, skrbnika ili pratioca. Slušati i poštovati djecu u svako doba. Ako se netko ponaša neprimjereno u blizini djece, prijavite to ponašanje lokalnom kontaktu za zaštitu djece.

Stvaranje sigurnijeg okruženja na internetu prilagođenog uzrastu **(nastavak)**	Uspostaviti jasan skup pravila koja su na vidnom mjestu i oslikavaju ključne točke iz uvjeta usluge i smjernica prihvatljive uporabe. Jezikom koji je razumljiv za korisnike ova pravila bi trebala definirati: • prirodu usluge i što se očekuje od njezinih korisnika; • što je prihvatljivo a što nije u smislu sadržaja, ponašanja i jezika, kao i zabrana nezakonite uporabe; • posljedice proporcionalne kršenju, primjerice, prijavljivanje tijelima za provedbu zakona ili suspenzija korisničkog profila.
	Olakšati korisnicima da prijave zabrinutost zbog zlouporabe 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, primjerice: • 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.
	Promovirati nacionalne službe potpore koje omogućuju djeci i mladima da prijave i potraže potporu u slučaju zlostavljanja ili iskorištavanja (pogledati, primjerice, Child Helpline International).
Edukacija djece, roditelja i edukatora o sigurnosti djece i njihovoj odgovornoj uporabi IK tehnologija	IKT kompanije mogu dopuniti tehničke mjere obrazovnim aktivnostima i aktivnostima osnaživanja poduzimanjem sljedećih radnji:
	Jasnog opisa dostupnog sadržaja i odgovarajuće roditeljske kontrole ili obiteljskih sigurnosnih postavki. Učiniti jezik i terminologiju dostupnim, vidljivim, jasnim i relevantnim za sve korisnike, uključujući djecu, roditelje i skrbnike, posebno u odnosu na odredbe i uvjete, troškove uključene u uporabu sadržaja ili usluga, politike privatnosti, sigurnosne informacije i mehanizme prijavljivanja.
	Obučiti korisnike o načinu rješavanja problema vezanih uz uporabu interneta, uključujući neželjenu poštu, krađu podataka i neprimjeren kontakt, poput maltretiranja i vrbovanja, i opisati koje radnje korisnici mogu poduzeti i kako mogu iznijeti zabrinutost zbog neprimjerene uporabe.
	Uspostaviti mehanizme i educirati roditelje da se uključe u IKT aktivnosti svoje djece i mladih, posebno onih koji imaju mlađu djecu, tako što će, primjerice, omogućiti roditeljima da pregledaju postavke privatnosti djece i mladih.
	Surađivati s vladom i edukatorima kako bi izgradili kapacitete roditelja za potporu i razgovor sa svojom djecom i mladima o tome da budu odgovorni digitalni građani i korisnici IK tehnologija.

Edukacija djece, roditelja i edukatora o sigurnosti djece i njihovoj odgovornoj uporabi IK tehnologija **(nastavak)**	Na temelju lokalnog konteksta, treba osigurati obrazovne materijale za uporabu u školama i domovima kako bi poboljšali uporabu IK tehnologija kod djece i mladih i razvili kritičko razmišljanje kako bi im omogućili da se ponašaju sigurno i odgovorno kada koriste usluge IK tehnologija.
	Podržite korisnike širenjem smjernica o obiteljskoj sigurnosti na internetu koje podstiču roditelje i skrbnike da: • se upoznaju s proizvodima i uslugama koje koriste djeca i mladi; • osiguraju umjerenu uporabu elektroničkih uređaja od strane djece i mladih kao dijela zdravog i uravnoteženog načina života; • pažljivo obrate pozornost na ponašanje djece i mladih kako bi utvrdili promjene koje bi mogle ukazivati na cyber 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 učiti djecu i mlade odgovornoj uporabi. To se može olakšati uporabom alata i interakcijom sa školskim distriktima za pružanje nastavnih planova i programa za djecu i obrazovnih materijala za roditelje u vezi sa sigurnosti 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 istodobno im dati potporu.
	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
Promoviranje digitalne tehnologije kao načina za povećanje građanskog angažmana	IKT kompanije mogu ohrabriti i osnažiti djecu i mlade podržavajući njihovo pravo na sudjelovanje kroz sljedeće radnje:
	Pružanje informacija o usluzi kako bi istakli koristi koje djeca ostvaruju ponašajući se primjerno i odgovorno, poput uporabe usluge u kreativne svrhe.
	Uspostaviti pisane postupke koji osiguravaju dosljednu provedbu politika i procesa koji štite slobodu izražavanja za sve korisnike, uključujući djecu i mlade, kao i dokumentaciju o usklađenosti s tim politikama.

Promoviranje digitalne tehnologije kao načina za povećanje građanskog angažmana (nastavak)	Izbjegavajte prekomjerno blokiranje legitimnog i razvojno odgovarajućeg sadržaja. Da se zahtjevi i alati za filtriranje ne bi zlorabili za ograničavanje pristupa informacijama djeci i mladima, osigurati 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 uvjete pružanja usluge.
	Razviti online platforme koje promoviraju pravo djece i mladih na izražavanje; olakšati njihovo sudjelovanje u javnom životu; i poticati njihovu suradnju, poduzetništvo i građansko sudjelovanje.
	Razviti obrazovni sadržaj za djecu i mlade koji podstiče učenje, kreativno razmišljanje i rješavanje problema.
	Promovirati digitalnu pismenost, izgradnju kapaciteta i IKT vještine kako bi se djeca i mladi, posebno oni u ruralnim područjima i područjima s nedovoljno visokom razinom usluga, opremili za korištenje IKT resursa i potpuno sigurno sudjelovanje u digitalnom svijetu.
	Surađujte s 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 potporu istih.
	Obavijestite i uključite kupce, uključujući roditelje, njegovatelje, djecu i mlade, o ponuđenim uslugama, poput: • vrste sadržaja i odgovarajuće roditeljske kontrole; • mehanizama prijavljivanja slučajeva pogrešne uporabe, zlouporabe i neprimjerenog ili nezakonitog sadržaja; • postupaka praćenja izvješća; • vrste usluga koje su starosno ograničene; • sigurnog i odgovornog korištenja interaktivnih usluga „vlastitog brenda“.
	Bavite se širim pitanjima u vezi sa sigurnim i odgovornim digitalnim građanstvom, primjerice internetskom reputacijom i digitalnim otiskom, štetnim sadržajem i njegom. Razmislite o partnerstvu s lokalnim stručnjacima, poput dječjih nevladinih organizacija, dobrotvornih organizacija i roditeljskih skupina, kako biste pomogli oblikovati poruku kompanije i imali željenu publiku.
	Ako kompanija već radi s djecom ili školama, primjerice, kroz programe korporativne društvene odgovornosti, istražite mogućnost da se ovaj angažman proširi na obrazovanje i interakciju s djecom i mladima kao i na edukatore o porukama u vezi sa zaštitom djece na internetu.
Investiranje u digitalno istraživanje	Uložite u istraživanje utemeljeno na dokazima i u dubinsku analizu tehnologija, utjecaj tehnologija na djecu, razmatranje zaštite djece i prava djeteta s obzirom na digitalno okruženje, integriranje online sustava zaštite u usluge koje koriste djeca i mladi i bolje razumijevanje koje vrste intervencija su najučinkovitije u poboljšanju dječjih 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 sheme u okviru kojih funkcioniraju i predmet i opseg njihovih ponuda veoma razlikuju. Bilo koja tehnološka kompanija čiji su proizvodi i usluge usmjereni izravno ili neizravno na djecu može imati koristi od ranije navedenih općih načela i može se prilagoditi na temelju svog specifičnog područja djelovanja. Osnovna ideja je podržati i voditi IKT industriju u poduzimanju pravih mjera za bolju zaštitu djece na internetu od opasnosti nanošenja štete, istodobno 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) Operateri 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 poduzeća koja pružaju besplatna ili plaćena javna 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 utemeljene 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 prijenosa, uključujući prijenose uživo.

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

5. Kontrolna lista po značajkama

Ovo poglavlje dopunjuje prethodni opći popis za industriju nudeći preporuke za poduzeća koja pružaju usluge sa specifičnim značajkama za poštivanje i potporu dječjih prava na mreži. Sljedeće kontrolne liste za određene značajke navode načine dopunjavanja zajedničkih načela i pristupa predstavljenih u Tablici 1. budući da oni važe za različite usluge te bi ih stoga trebalo uzeti u obzir kao dodatak koracima iz Tabele 1.

Ovdje istaknute značajke se presijecaju i nekoliko kontrolnih lista specifičnih za značajke može biti relevantno za istu kompaniju.

Sljedeće kontrolne liste su organizirane i pozivaju se na iste ključne oblasti kao i opće smjernice u Tablici 1. Svaka lista za provjeru značajki razvijena je s ključnim suradnicima i zbog toga postoje manje razlike u tablicama.

5.1 Značajka A: Osigurati povezivanje, usluge skladištenja podataka i hostinga

Pristup internetu je osnovni za ostvarivanje dječjih prava, a povezanost može djeci otvoriti čitav svijet. Operateri 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, operaterima internet usluga, sustavima za skladištenje podataka i uslugama hostinga.

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

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

Pristup internetu na javnim mjestima

Sve je uobičajenije da općine, trgovci, transportne kompanije, lanci hotela i druga poduzeća 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 njezine usluge.

Promoviranje Wi-Fi mreže je učinkovit način da se osigura dostupnost interneta u određenom području. Međutim, treba voditi računa kada je takav pristup omogućen u javnim prostorima u kojima je vjerojatno da će djeca redovito boraviti. Korisnici moraju imati na umu činjenicu da Wi-Fi signali mogu biti dostupni prolaznicima, a korisnički podatci ugroženi. Zbog toga operater Wi-Fi mreže neće uvijek biti u mogućnosti podržati ili nadzirati uporabu internet konekcije koju je isporučio i korisnici zato moraju poduzeti mjere predostrožnosti da izbjegavaju dijeljenje osjetljivih informacija putem javno dostupne Wi-Fi mreže.

U javnim prostorima, operateri 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 uvjete uporabe kojima se zabranjuje uporaba Wi-Fi usluga za pristup ili prikazivanje bilo kojeg materijala koji je možda neprikladan u okruženju u kome borave djeca. Odredbe i uvjeti također trebaju sadržavati jasne mehanizme u vezi s posljedicama kršenja takvih pravila.
- Poduzimanje svih mjera za zaštitu od neovlaštenog pristupa, što za rezultat može imati manipulaciju ili gubitak osobnih podataka.
- Instaliranje filtera na Wi-Fi sustav radi potpore primjeni pravila o neprikladnom materijalu.
- Osiguravanje procedura i softvera za putokaz i nuđenje opcijske roditeljske kontrole koja se odnosi na pristup djece i mladih internetskim sadržajima.

Dobra praksa: Propisi o telekomunikacijama većine država članica Europske unije predviđaju, primjerice, da pristup mreži mora biti identificiran putem pojedinačnih SIM kartica ili drugih alata za identifikaciju.

Tablica 2. sadrži smjernice za operatere usluga povezivanja, skladištenja podataka i hosting usluga o radnjama koje mogu poduzeti u cilju poboljšanja dječje online zaštite i dječjeg sudjelovanja.

Tablica 2. Kontrolna lista zaštite djece na internetu za Značajku A: Osigurati uređaje za povezivanje, skladištenje i hosting podataka

Uvrštavanje pitanja prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja	Operateri usluga povezivanja, skladištenja podataka i hostinga mogu identificirati, spriječiti i ublažiti negativne učinke IK tehnologija na prava djece i mladih i identificirati mogućnosti za potporu napretku djece i mladih.
	Vidi opće smjernice u Tablici 1.
Razvitak standardnih procesa radi rješavanja problema materijala seksualnog zlostavljanja djece	U suradnji s vladom, tijelima za provedbu zakona, civilnim društvom i organizacijama SOS servisa, operateri usluga povezivanja, skladištenja podataka i hosting usluga mogu igrati ključnu ulogu u borbi protiv materijala seksualnog zlostavljanja djece poduzimanjem sljedećih radnji:
	Suradnja s vladom, tijelima za provedbu zakona, civilnim društvom i organizacijama SOS servisa u borbi protiv materijala seksualnog zlostavljanja djece i radi prijavljivanja slučajeva odgovarajućim tijelima. Ako suradnja s policijom i SOS telefon za pomoć još nije uspostavljen, angažirajte se na zajedničkoj uspostavi suradnje. Operateri usluga povezivanja, skladištenja podataka ili hostinga mogu također izvršiti obuku policije iz oblasti IK tehnologija. Ako kompanija posluje na tržištima s manje razvijenim pravnim i zakonskim nadzorom ovog pitanja, ista može uputiti one koji žele podnijeti prijave na Međunarodnu udrugu 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 provedbu zakona ili vruća linija za prijavljivanje, Cybertip Canada, Interpol, IWF), kako bi korisnicima otežali pristup identificiranom zlostavljačkom materijalu.
	Razviti postupke obavještavanja, uklanjanja i prijavljivanja te povezati prijave zlouporabe s tim procesima putem sporazuma o javnoj službi o postupku odgovora i vremenu uklanjanja. Pogledajte, primjerice, UNICEF-ov i GSMA vodič o politikama i praksi obavještavanja i uklanjanja.
	Uspostavite mehanizam prijavljivanja s jasnim informacijama o njegovoj uporabi, primjerice, davanjem smjernica o ilegalnom sadržaju i ponašanju koje treba prijaviti i pojašnjavanjem toga koji se materijali ne mogu priložiti uz izvješće kako bi se izbjegla daljnja distribucija na internetu.

Razvitak standardnih procesa radi rješavanja problema materijala seksualnog zlostavljanja djece (*nastavak*)	Podržite provedbu zakona u slučaju kaznenih istraga kroz aktivnosti kao što je prikupljanje dokaza. Koristite uvjete i odredbe usluge kako biste posebno zabranili uporabu usluga za skladištenje, dijeljenje ili distribuciju materijala seksualnog zlostavljanja djece. Obvezatno navedite da ovi uvjeti jasno navode da se materijal seksualnog zlostavljanja djece neće tolerirati. Obvezatno navedite da se u uvjetima usluge i odredbama navodi da će kompanija u potpunosti surađivati u kaznenim istragama u slučaju otkrivanja ili prijave materijala seksualnog zlostavljanja djece.
	Trenutačno postoje dva rješenja za prijavljivanje materijala seksualnog zlostavljanja djece na internetu na nacionalnoj razini: 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 uspostavu 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 izvješća sumnjivog sadržaja policiji i mreži INHOPE. Portali za prijavljivanje: IWF nudi rješenje portala za prijavljivanje koje omogućuje korisnicima interneta u zemljama i zemljama bez vrućih linija da izravno IWF-u prijavljuju slike i videozapise za koje sumnjaju da mogu predstavljati seksualno zlostavljanje djece i to putem posebne mrežne stranice portala.
	Za operatere usluga povezivanja, skladištenja podataka i hosting usluga čije usluge uključuju neku vrstu hostinga sadržaja, potrebno je imati uspostavljene postupke obavještavanja i uklanjanja.
Stvaranje sigurnijeg i starosno prikladnog digitalnog okruženja	Operateri usluga internet konekcije, skladištenja podataka i hostinga mogu pomoći u stvaranju sigurnijeg, ugodnijeg digitalnog okruženja za djecu svih uzrasta poduzimanjem sljedećih radnji:
	Operateri usluga skladištenja/hostinga podataka trebali bi razmotriti predstavljanje funkcije prijavljivanja na svim web-stranicama i servisima kao i razviti i dokumentirati jasne procese za brzo upravljanje izvješćima o zlouporabi ili drugim kršenjima uvjeta i odredbi.
	Internet operateri bi trebali ponuditi tehničku kontrolu vlastitog brenda ili označiti dostupnost alata koje su kreirali specijalizirani operateri usluga koji su primjereni ponuđenim uslugama, a krajnji korisnici ih mogu lako primijeniti i ponuditi mogućnost blokiranja ili filtriranja pristupa internetu putem korporativne mreže. Osigurajte odgovarajuće mehanizme za provjeru starosti ako kompanija nudi sadržaj ili usluge (uključujući usluge vlastitog brenda ili usluge treće strane koje kompanija promovira), koje su legalne ili odgovarajuće za odrasle korisnike (npr. određene nagradne igre, lutrije).

Edukacija djece, roditelja i nastavnika o dječjoj sigurnosti i njihovoj odgovornoj uporabi IK tehnologija	Operateri usluga povezivanja, skladištenja podataka i hostinga trebali bi ponoviti ključne poruke iz odredbi i uvjeta iz smjernica zajednice napisanih na jeziku prilagođenom korisnicima podržati djecu i njihove roditelje i skrbnike. 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 sigurnijoj uporabi interneta. Razmotrite kreativne načine za promociju ključnih poruka, kao što su sljedeće: "Nikada ne dijelite nikakve kontakt informacije s nepoznatim osobama, uključujući vašu fizičku lokaciju i telefonski broj. „Nikada nemojte pristati sami sastati se s nekim koga ste upoznali na mreži bez prethodnog savjetovanja s odraslom osobom. Uvijek recite pouzdanom prijatelju gdje se nalazite " „Ne odgovarajte na maltretiranje, nepristojne ili uvrjedljive 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 kako bi vas uvjerili da podijelite svoje privatne podatke. "
	Operateri usluga se mogu udružiti s organizacijama koje su u dobrom položaju radi edukacije i potpore djeci o sigurnijoj uporabi interneta i o srodnim pitanjima. Pogledajte International Helpline za djecu i praktični vodič za GSMA za dječje linije za potporu i mobilne operatere: Zajednički rad na zaštiti dječjih prava.
Promoviranje digitalne tehnologije kao načina za povećanje civilnog angažmana	*Vidi opće smjernice u Tablici 1.*

5.2 Značajka B: Ponuditi organizirani 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 se usluga odnosi na poduzeća koja kreiraju vlastiti sadržaj kao i na ona koja omogućuju pristup digitalnom sadržaju. Između ostalog, ovo se odnosi na usluge streaminga vijesti i multimedije, nacionalnu i javnu radiodifuziju i industriju igara na sreću.

Tablica 3. sadrži smjernice za operatere usluga koje nude profesionalno uređen sadržaj o politikama i radnjama koje mogu poduzeti u cilju poboljšanja dječje online zaštite i dječjeg sudjelovanja.

Tablica 3. Kontrolna lista zaštite djece na internetu za Značajku B: Ponuditi organizirani digitalni sadržaj

Uvrštavanje pitanja prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja	Servisi koji nude profesionalno uređen sadržaj mogu pomoći da se identificiraju, spriječe i ublaže negativni utjecaji IK tehnologija na prava djece i mladih i da identificiraju mogućnosti za potporu napretku djece i mladih poduzimanjem 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 osoba mlađih od 18 godina koja su uključene u programe, filmove, igre, vijesti itd., bez obzira na pristanak koji je mogao dati roditelj ili druga odrasla osoba.
Razvijanje standardnih procesa za borbu protiv materijala seksualnog zlostavljanja djece	U suradnji s državom, policijom, civilnim društvom i organizacijama vrućih linija za potporu, kompanije koje nude profesionalno uređen digitalni sadržaj mogu igrati ključnu ulogu u borbi protiv MSZD putem sljedećih aktivnosti: U slučajevima MSZD, primjerice putem funkcija „komentiranja“ ili „pregleda“, pri čemu korisnici imaju kapacitet za učitavanje sadržaja, osoblje bi trebalo kontaktirati izvršni rukovodeći tim odgovoran za prijavljivanje takvog materijala odgovarajućim tijelima. Pored toga, potrebno je: • odmah upozoriti nacionalne agencije za provedbu zakona; • upozoriti rukovodstvo agencije i prijaviti materijal menadžeru politike zaštite djece; • kontaktirati službu interne istrage telefonom ili e-poštom s detaljima incidenta i zatražiti savjet; • prije brisanja materijala, skladištenja u zajednički prostor ili prosljeđivanja pričekajte savjet nadležne agencije;
	• implementirati brzu i učinkovitu strategiju eskalacije ako je materijal seksualnog 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 uvjete i odredbe web-stranice. Pratite minimalne starosne zahtjeve na različitim stranicama za društveno umrežavanje. • Odredbe i uvjeti svakog internetskog prostora trebaju također sadržavati jasne mehanizme izvještavanja o kršenju takvih pravila.

Razvitak standardnih procesa radi rješavanja problema materijala seksualnog zlostavljanja djece

Ako je materijal identificiran, treba ga prijaviti izravno organizaciji specijaliziranoj za internetsku sigurnost koja upravlja sustavom izvještavanja putem javne telefonske linije i IT profesionalcima radi prijavljivanja specifičnih oblika potencijalno ilegalnih internetskih sadržaja.
Primjerice, na temelju svoje politike zaštite djece, BBC je objavio uredničke smjernice o interakciji s djecom i mladima na internetu. BBC je razvio dodatne kontrolne liste i kodekse ponašanja za rad s djecom i mladima na internetu,
koje se također odnose na podizvođače i vanjske operatere usluga.
Politika zaštite djece regulatora za komunikacije u Velikoj Britaniji (Ofcom) odvojeno se bavi online sadržajem, mobilnim uređajima i igraćim konzolama.

Stvaranje sigurnijeg 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 poduzimanjem sljedećih radnji:
	Surađujte s drugima iz branše kako biste razvili sustave klasifikacije/ocjenjivanja sadržaja koji se temelje na prihvaćenim nacionalnim ili međunarodnim standardima i sukladno pristupima koji se zauzimaju u ekvivalentnim medijima. Gdje je to moguće, klasifikacija sadržaja trebala bi biti konzistentna na različitim medijskim platformama, primjerice, najava filma u kinu 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 sustavom provjere starosti.
	Kako biste pomogli roditeljima i drugima da odluče je li sadržaj starosno primjeren za djecu i mlade, izgradite aplikacije i usluge na svim medijima kako bi se uskladili sa sustavima 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 audiovizualne i multimedijske usluge možda želi dati osobni identifikacijski broj korisnicima koji žele pristupiti sadržaju koji može biti štetan za djecu i mlade.
	Osigurajte 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 je li potreban pristanak roditelja prije nego što komercijalna poduzeća mogu prikupljati osobne 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 skupinama koje će mu vjerojatno pristupiti, primjerice, uspostavom odgovarajućih pravila za online oglašavanje djeci i mladima. Ako ponuda sadržaja podržava interaktivni element, kao što je komentiranje, 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 koja je razina angažmana potrebna 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 konzultirati državna tijela nadležna za zaštitu djece.
	Osigurati 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 sigurnosti i njihovoj odgovornoj uporabi IK tehnologija	Kompanije koje nude profesionalno uređen digitalni sadržaj mogu dopuniti tehničke mjere obrazovnim aktivnostima koje osnažuju djecu poduzimanjem sljedećih radnji:
	Pružite kupcima konkretne i jasne informacije o sadržaju, kao što su vrsta sadržaja, starosne ocjene, odnosno ograničenja, uvrjedljiv jezik ili nasilje i odgovarajuće dostupne roditeljske kontrole; i informacije o tome kako prijaviti zlouporabu i neprimjeren ili nezakonit sadržaj i kako će se postupati s izvješćima. U interaktivnom svijetu ove informacije se daju u obliku oznaka sadržaja za svaki program.
	Podstaknite odrasle, posebice roditelje, njegovatelje i skrbnike, da budu uključeni u potrošnju internetskog sadržaja djece i mladih kako bi mogli pomoći i usmjeravati djecu i mlade u izboru sadržaja prilikom kupovine i pomoći u uspostavi pravila ponašanja. Pomozite djeci (i roditeljima i skrbnicima) da nauče upravljati svojim vremenom ispred ekrana i razumjeti kako koristiti tehnologiju na način koji im odgovara, uključujući i to kada treba prestati i raditi nešto drugo.
	Prenesite pravila uporabe na jasnom i dostupnom jeziku koji potiču djecu i mlade na oprez i odgovornost kada surfaju internetom.
	Kreirajte alate prilagođene starosti, poput tutorijala i centara za pomoć. Po potrebi surađujte s internetskim ili osobnim preventivnim programima i terapeutskim klinikama. Primjerice, ako postoji rizik da se djeca i mladi previše bave tehnologijom, što im otežava razvijanje osobnih odnosa ili sudjelovanje 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.
	Surađujte s 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 ovisnosti o kontekstu. Pribavite informirani pristanak djece kada ih prikazujete u programima, filmovima, videozapisima itd., gdje god je to moguće, i poštujte svako odbijanje sudjelovanja.

Promoviranje 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 sudjelovanje 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 uporabljiv, 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 poticati sadržaje koji djeci omogućuju da prihvate različitost i budu pozitivni uzori.

5.3 Značajka C: Skladištiti sadržaj koji generiraju korisnici i povežite korisnike

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

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

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

Operateri 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 također omogućuju funkcije dijeljenja lokacije, što čini djecu i mlade koji koriste ove usluge još osjetljivijima na opasnosti izvan interneta.

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

Tablica 4. Kontrolna lista zaštite djece na internetu za Značajku C: Skladištiti sadržaj koji generiraju korisnici i povežite korisnike

Uvrštavanje pitanja prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja	Servisi koji vrše hosting sadržaja koji generiraju korisnici i koji povezuju korisnike mogu identificirati, spriječiti i ublažiti negativne učinke IK tehnologija na prava djece i mladih i identificirati mogućnosti za potporu napretku djece i mladih.
	Vidi opće smjernice u Tablici 1.
Razvitak standardnih procesa radi rješavanja problema materijala seksualnog zlostavljanja djece	U suradnji s vladom, tijelima za provedbu zakona, civilnim društvom i organizacijama SOS servisa, kompanije koje vrše hosting sadržaja koji generiraju korisnici i koje povezuju korisnike mogu igrati ključnu ulogu u borbi protiv materijala seksualnog zlostavljanja djece poduzimanjem sljedećih radnji:
	Uspostavite procedure za sve lokacije za pružanje neposredne pomoći policiji tijekom izvanrednih situacija i za rutinske istrage.
	Navedite da će poduzeće u potpunosti surađivati u istragama u slučaju da se nezakoniti sadržaj prijavi ili otkrije i zabilježite detalje u vezi s takvim kaznama kao što su novčane kazne ili ukidanje privilegija naplate.
	Radite s internim funkcijama kao što su briga o kupcima, sprječavanje prijevara i sigurnost kako biste bili sigurni da kompanija može podnositi izvješća o sumnji na ilegalni sadržaj izravno policiji i linijama za potporu. U idealnom slučaju, to bi trebalo uraditi na način koji ne izlaže sadržaju osoblje koje radi izravno s klijentima niti ponovo viktimizira ugroženo dijete/djecu i mlade. Kako biste se pozabavili situacijama u kojima osoblje može biti izloženo nasilnom materijalu, implementirajte politiku ili program za potporu otpornosti, sigurnosti i dobrobiti osoblja.
	Primijenite uvjete iz ugovora o vršenju usluge i uvjete za zabranu ilegalnog sadržaja i ponašanja, ističući da: • štetni sadržaji, uključujući sumnju na pedofilsko zbližavanje s djecom s namjerom bilo fizičkog ili nefizičkog zlostavljanja, neće biti tolerirani: • protuzakoniti sadržaj, uključujući upload ili daljnje širenje materijala seksualnog zlostavljanja djece, neće biti toleriran; • kompanija će se obratiti i u potpunosti surađivati u kaznenim istragama u slučaju da se prijavi ili otkrije protuzakoniti sadržaj ili bilo koje kršenje politike zaštite djece.
	Dokumentirajte praksu kompanije za rukovanje materijalom seksualnog zlostavljanja djece, počevši od nadgledanja i proširivanja do konačnog prijenosa i uništavanja sadržaja. U dokumentaciju uvrstite spisak svog osoblja odgovornog za rukovanje materijalom.
	Usvojite politike u vezi sa vlasništvom nad sadržajem koji kreiraju korisnici, uključujući opciju uklanjanja sadržaja koji kreiraju korisnici na zahtjev korisnika. Uklonite sadržaj kojim se krše pravila operatera, a o kršenju upozorite korisnika koji je postavio predmetni sadržaj.

Uspostava standardnih procesa za borbu protiv MSZD **(*nastavak*.)**	Navedite da će nepoštovanje politika od strane korisnika imati posljedice, uključujući: • uklanjanje sadržaja, suspenziju ili zatvaranje naloga prekršitelja; • opoziv opcije dijeljenja određenih vrsta sadržaja ili korištenja određenih opcija; • sprječavanje kontakta s djecom; • prijavljivanje slučaja nadležnim tijelima
Uspostava standardnih procesa za borbu protiv MSZD	Promovirajte mehanizme izvještavanja za MSZD ili bilo koji drugi ilegalni sadržaj i osigurajte uvjete da klijenti znaju podnijeti prijavu ako otkriju takav sadržaj. Uspostavite sustave i osigurajte obučeno osoblje za procjenu pojedinačnih slučajeva i poduzimanje odgovarajućih mjera. Uspostavite dobro organizirane i sveobuhvatne operativne timove za korisničku potporu. Idealno bi bilo da se ovi timovi obuče za rješavanje različitih vrsta incidenata kako bi se dao adekvatan odgovor i poduzele odgovarajuće radnje. Kada korisnik podnese žalbu, ovisno o vrsti incidenta, potrebno je korisnika uputiti odgovarajućem osoblju. Kompanija bi također mogla uspostaviti posebne timove za rješavanje žalbi korisnika u slučajevima kada su izvješća možda podnesena pogreškom.
	Uspostavite procese za trenutačno uklanjanje ili blokiranje pristupa materijalu seksualnog zlostavljanja djece, uključujući procese obavještavanja i uklanjanja ilegalnog sadržaja odmah nakon identificiranja istog. Pobrinite se da treće strane s kojima je kompanija u ugovornom odnosu imaju slične učinkovite postupke obavještavanja i uklanjanja. Ako zakonodavstvo dozvoljava, materijal se može čuvati kao dokaz kaznenog djela u slučaju istrage.
	Uspostaviti tehničke sustave koji mogu otkriti poznati ilegalni sadržaj i spriječiti njegovo učitavanje, uključujući i učitavanje u privatne skupine, ili ga označiti za trenutačni pregled od strane sigurnosnog tima kompanije. Poduzmite sve odgovarajuće mjere zaštite servisa od zlouporabe u pogledu hostinga, distribuiranja ili kreiranja materijala seksualnog zlostavljanja djece. Gdje je to moguće, uspostavite proaktivne tehničke mjere za analizu predmeta i metapodataka povezanih s profilom radi otkrivanja kriminalnog ponašanja ili obrazaca i poduzmite odgovarajuće mjere.
	Ako aplikacija ili usluga omogućuje 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 najvjerojatnije sadržavati materijal seksualnog zlostavljanja djece. Razmotrite proaktivne tehnike identifikacije kao što su tehnologija skeniranja ili ljudski pregled.

Stvaranje sigurnijeg i starosno prikladnog digitalnog okruženja	Operateri usluga koji nude sadržaj kreiran od strane korisnika mogu pomoći u stvaranju sigurnijeg, ugodnijeg digitalnog okruženja za djecu svih uzrasta poduzimanjem sljedećih radnji:
	Na jeziku prilagođenom kupcima, a u okviru usluge i korisničkih smjernica, definirajte jasan skup „kućnih pravila“ kojima se definira sljedeće: • priroda usluge i ono što se očekuje od njezinih korisnika; • što jeste, a što nije prihvatljivo u smislu sadržaja, ponašanja i jezika, kao i zabranu ilegalne uporabe; • posljedice kršenja, kao primjerice prijavljivanje policiji i suspenzija korisničkog računa.
	Ključne sigurnosne i pravne poruke trebale bi biti predstavljene u starosno prilagođenom formatu (tj. koristeći intuitivne ikone i simbole) prilikom registracije i prilikom poduzimanja različitih radnji na web-stranici.
	Olakšajte klijentima da korisničkom servisu prijave problem zlouporabe, 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. Primjerice, 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 razvitak novih sustava za provjeru starosti, poput biometrije, koristeći poznate međunarodne standarde za razvitak takvih alata. Poduzmite korake za identificiranje i uklanjanje maloljetnih korisnika koji su pogrešno prikazali svoju starost kako bi dobili pristup. Potrebno je razmotriti dodatno prikupljanje osobnih podataka koje bi 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 kako biste utvrdili jesu li korisnici dovoljno stari za pristup sadržaju ili usluzi bez ugrožavanja njihovog identiteta, lokacije i osobnih podataka. Koristite nacionalno uspostavljene funkcionalne sustave 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 sigurnijeg i starosno prikladnog digitalnog okruženja (*nastavak*)	Zaštitite mlađe korisnike od neželjene komunikacije i osigurajte 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 osobne podatke o sebi ili drugima.
	Brojne mjere mogu se koristiti za kontrolu pristupa sadržaju koji generiraju korisnici i za zaštitu djece i mladih na mreži od neprikladnog ili ilegalnog sadržaja. Obvezatno koristite sigurne zaporke kao korak u cilju zaštite djece i mladih u igrama i drugim postavkama društvenih medija. Ostale tehnike uključuju: • pregled diskusijskih skupina radi utvrđivanja štetnih predmeta, govora mržnje i nezakonitog ponašanja i brisanje takvog sadržaja kada se utvrdi da krši uvjete korištenja; • pre-moderiranje oglasnih ploča s timom specijaliziranih moderatora za djecu i mlade koji provjeravaju sadržaj koji je u suprotnosti s objavljenim "kućnim redom"; svaka poruka se može provjeriti prije objavljivanja, a moderatori također mogu uočiti i označiti sumnjive korisnike, kao i korisnike u nevolji; • uspostava tima domaćina zajednice (*host*) koji služe kao prva točka kontakta za moderatore kada imaju problem u vezi s korisnikom.
	Budite odgovorni za pregled komercijalnog sadržaja, uključujući forume, društvene mreže i web lokacije za igre.

Edukacija djece, roditelja i edukatora o sigurnosti djece i njihovoj odgovornoj uporabi IK tehnologija	Operateri usluga koji nude sadržaj koji generiraju korisnici mogu dopuniti tehničke mjere obrazovnim aktivnostima i aktivnostima osnaživanja poduzimanjem sljedećih radnji:
	Kreirajte dio posvećen sigurnosnim savjetima, člancima, značajkama i dijalogu o digitalnom državljanstvu, kao i linkovima do korisnog sadržaja neovisnih stručnjaka. Sigurnosni savjeti moraju biti lako uočljivi i napisani lako razumljivim jezikom. Također se operateri platformi podstiču da imaju jedinstveni navigacijski interface na različitim uređajima, poput računara, tableta ili mobilnih telefona.
	Ponudite roditeljima jasne informacije o vrstama sadržaja i dostupnim uslugama, uključujući, primjerice, objašnjenje web lokacija društvenih mreža i usluga utemeljenih na lokaciji, način pristupa internetu putem mobilnih uređaja i opcije dostupne roditeljima za primjenu kontrola.
	Obavijestite roditelje o načinu prijavljivanja zlouporabe, pogrešne uporabe 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 sustav utemeljen na „povjerenju i ugledu“ kako bi se podstaknulo dobro ponašanje i omogućilo vršnjacima da primjerom prenose najbolje prakse. Promovirajte važnost društvenog izvještavanja, koje omogućuje ljudima da se obrate drugim korisnicima ili pouzdanim prijateljima kako 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, primjerice, sa pop-up obavijestima koji podsjećaju korisnike na odgovarajuće i sigurno ponašanje, poput nedavanja njihovih kontakt informacija.
	Surađujte s roditeljima kako biste bili sigurni da ih informacije objavljene na internetu o djeci ne izlažu riziku. Pribavite informirani pristanak djece kada ih prikazujete u programima, filmovima, video zapisima itd., gdje god je to moguće, i poštujte svako odbijanje sudjelovanja.
Promoviranje 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 sudjelovanje.
	Vidi opće smjernice u Tablici 1.

5.4 Značajka D: Sustavi vođeni vještačkom inteligencijom

S povećanom pažnjom koja se daje tehnologijama za učenje, pojmovi „vještačka inteligencija“, „strojno učenje“ i „duboko učenje“ široko su u uporabi u istom značenju kao odraz koncepta replikacije „inteligentnog“ ponašanja u strojevima. U ovom se dijelu fokusiramo na načine na koje procesi strojnog učenja i dubokog učenja utječu na dječji život i, konačno, na njihova ljudska prava.

„Zbog eksponencijalnog napretka tehnologija utemeljenih na vještačkoj inteligenciji u posljednjih nekoliko godina, trenutačni međunarodni okvir koji štiti dječja prava ne bavi se izričito mnogim pitanjima koja su pokrenuta razvitkom i uporabom vještačke inteligencije. Međutim, ovaj okvir identificira 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 utjecati na dječja prava, poput prava na privatnost, obrazovanje i igranje, kao i prava na nediskriminaciju."

Primjena vještačke inteligencije može izmijeniti utjecaj na djecu raznih usluga koje se koriste na društvenim mrežama, poput platformi za streaming video-zapisa. Tehnologija ekrana osjetljivog na dodir i dizajn ovih platformi omogućuju vrlo maloj djeci 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 također ima utjecaja 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 točka za Wi-Fi vezu i personaliziranim online nalogom igračke, odnosno potrošača, gdje se podatci čuvaju. Takve igračke komuniciraju sa serverima zasnovanim na oblaku koji čuvaju i obrađuju podatke koje pružaju djeca koja komuniciraju s igračkom. Ovaj model ima sigurnosne probleme ako se sigurnost ne primjenjuje na svakoj razini, što su pokazali brojni slučajevi hakiranja u kojima su procurili osobni podaci. Štoviše, neki hakirani 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, primjerice, davanjem savjeta i preporuka na temelju otkrivenog ponašanja (kao što je ranije spomenuto u aplikaciji BBC Own It), presudno je da kompanije koje dizajniraju pametne uređaje temelje ove preporuke na dokazima i razvijaju ih u dogovoru sa stručnjacima za zaštitu djece.

Iako neke kompanije unapređuju načela za etičnu uporabu vještačke inteligencije, nije jasno postoje li javne politike usmjerene na vještačku inteligenciju i djecu. Nekoliko tehnoloških i trgovinskih udruga i skupina za informatiku izradili su etična načela u vezi s 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, “Završno izvješće: Vještačka inteligencija i dječja prava”, 2018.

19 Ibid.

20 Ibid.

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

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

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

„Poput korporacija, vlade diljem svijeta usvojile su strategije za buduće lidere o razvitku i uporabi vještačke inteligencije, potičući okruženje pogodno za inovatore i korporacije.“ Međutim, nejasno je kako se takve nacionalne strategije izravno bave dječjim pravima.

Unapređenje pristupa Facebooka sadržaju povezanom sa samoubojstvom i samoozljeđivanjem

U 2019. godini, Facebook je počeo organizirati redovne konzultacije sa stručnjacima iz cijelog svijeta radi razgovora o nekim težim temama povezanim sa samoubojstvom i samoozljeđivanjem. Ove teme obuhvaćaju pitanja poput kako postupati oproštajnim pismima samoubojica, rizicima povezanim s depresivnim sadržajem na internetu i značajnim prikazima samoubojstva. Dodatni detalji ovih sastanaka dostupni su na Facebookovoj novoj stranici za prevenciju samoubojstava, u njegovom Sigurnosnom centru. Ove konzultacije za rezultat su imale nekoliko poboljšanja u načinu na koji Facebook obrađuje ovu vrstu sadržaja. Primjerice, ojačana je politika u vezi sa samoozljeđivanjem kako bi se zabranilo grafičko rezanje slika radi izbjegavanja nenamjernog promoviranja ili izazivanja samoozljeđivanja. Čak i kada netko traži potporu 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 poduzeti radnje na potencijalno štetnom sadržaju, uključujući uklanjanje istog ili dodavanjem upozorenja da se radi o osjetljivom sadržaju. Od travnja do lipnja 2019. godine, Facebook je intervenirao kod više od 1,5 milijuna sadržaja samoubojstava i samoozljeđivanja na svojoj web lokaciji i otkrio više od 95 odsto istih prije nego što ih je korisnik prijavio. U istom razdoblju, Instagram je intervenirao kod više od 800 tisuća sličnih sadržaja, od kojih je više od 77 odsto otkriveno prije nego što ih je korisnik prijavio.

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

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

24 Ibid.

Dobra praksa: Uporaba 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 sigurnost sadržaja, Facebook je također 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 pHashu, iako je od temelja kreiran kao poseban algoritam sa neovisnom softverskom implementacijom. Tehnologiju za podudaranje videozapisa, TMK + PDQF, zajednički su razvili Facebookov tim za istraživanje vještačke inteligencije i znanstvenici sa Sveučilišta u Modeni i Reggio Emilia u Italiji.

Ove tehnologije stvaraju učinkovit 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 videozapisa. Haševi se također mogu lakše dijeliti s 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 Tablici 5. su date neke od preporuka poduzećima za usklađivanje svojih načela prilikom dizajniranja i implementacije rješenja namijenjenih djeci, a utemeljenih na vještačkoj inteligenciji.

Ove se preporuke temelje 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 također oslanjaju na rad UNICEF-a i studije Sveučilišta Kalifornije u Berkeleyu o vještačkoj inteligenciji i pravima djeteta.

UNICEF i UC Berkeley, “Završno izvješće: Vještačka inteligencija i dječja prava”, 2018.

Tablica 5. Kontrolna lista zaštite djece na internetu za Značajku D: Sustavi vođeni vještačkom inteligencijom

Uvrštavanje pitanja prava djeteta u sve odgovarajuće korporativne politike i procese upravljanja	Operateri sustava vođenih vještačkom inteligencijom mogu identificirati, spriječiti i ublažiti negativne učinke IK tehnologija na prava djece i mladih i identificirati mogućnosti za potporu napretku djece i mladih.
	Sustavi vještačke inteligencije trebaju se dizajnirati, razvijati, implementirati i istraživati kako bi se poštovala, promovirala 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. Sustave vještačke inteligencije treba iskoristiti tako da ovu potporu pruže u punom potencijalu.
	Uvrstite inkluzivni pristup dizajnu pri razvitku 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 etične smjernice, zakone, standarde i regulatorna tijela radi nadzora procesa kojima se sprječava da se primjena sustava vještačke inteligencije ne krše dječja prava.
Razvitak standardnih procesa radi rješavanja problema materijala seksualnog zlostavljanja djece	U suradnji s državom, tijelima za provedbu zakona, civilnim društvom i organizacijama za potporu na vrućim linijama, operateri sustava vođenih vještačkom inteligencijom igraju ključnu ulogu u borbi protiv materijala seksualnog zlostavljanja djece poduzimanjem sljedećih radnji:
	Vidi opće smjernice u Tablici 1.

Stvaranje sigurnijeg i starosno prikladnog digitalnog okruženja	Operateri sustava vođenih vještačkom inteligencijom mogu pomoći u stvaranju sigurnijeg, ugodnijeg digitalnog okruženja za djecu svih uzrasta poduzimanjem sljedećih radnji:
	Usvojite multidisciplinarni pristup prilikom razvijanja tehnologija koje utječu na djecu i konzultirajte se s civilnim društvom, uključujući akademsku zajednicu, kako bi se identificirali potencijalni utjecaji ovih tehnologija na prava različitih vrsta potencijalnih krajnjih korisnika.
	Primijenite planiranu sigurnost i planiranu privatnost za proizvode i usluge kojima se djeca bave ili ih često koriste.
	Kako su sustavi vještačke inteligencije "gladni" podataka, kompanije koje koriste vještačku inteligenciju za svoje usluge trebale bi koristiti posebnu budnost u pogledu prikupljanja, obrade, skladištenja, prodaje i objavljivanja osobnih podataka djece. Sustavi vještačke inteligencije bi trebali biti transparentni tako da bi moglo biti moguće otkriti kako i zašto je sustav 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 sustavima vještačke inteligencije. Potrebno je uspostaviti procese za pravodobno ispravljanje svih diskriminatornih rezultata i uspostaviti nadzorna tijela za žalbe i kontinuirano praćenje dječje sigurnosti i zaštite. Odgovornost i mehanizmi za obeštećenje idu ruku pod ruku.
	Sačiniti planove za rukovanje posebno osjetljivim podatcima, uključujući otkrivanja zlouporabe ili druge štete koja se može podijeliti s kompanijom putem njezinih proizvoda. Digitalne platforme i sustavi vještačke inteligencije trebali bi smanjiti prikupljanje podataka o djeci i povećati dječju kontrolu nad podatcima koje kreiraju. Uvjeti uporabe trebaju biti razumljivi djeci kako bi osnažili svoju svijest i sposobnost.
Edukacija djece, roditelja i edukatora o dječjoj sigurnosti i njihovoj odgovornoj uporabi IK tehnologija	Pružatelji sustava vođenih vještačkom inteligencijom mogu dopuniti tehničke mjere obrazovnim aktivnostima i aktivnostima osnaživanja.
	Trebalo bi biti moguće objasniti svrhu sustava s vještačkom inteligencijom djeci korisnicima i njihovim roditeljima ili skrbnicima kako bi ih osnažili da odluče koristiti ili odbiti takve platforme.

Promoviranje digitalne tehnologije kao načina za povećanje građanskog angažmana	Kompanije koje nude sustave vođene vještačkom inteligencijom mogu ohrabriti i osnažiti djecu i mlade podržavajući njihovo pravo na sudjelovanje.
	Vidi opće smjernice u Tablici 1.
Korištenje tehnologije	Sustavi vođeni vještačkom inteligencijom trebali bi se razvijati kako bi podržali dječji napredak u zaštiti razvitka i blagostanja kao rezultat u cijelom dizajnu sustava, te educirali djecu o razvitku i implementaciji. Njihova referentna točka trebale bi biti najbolje dostupne i široko prihvaćene metrike razvitka i blagostanja. Kompanije bi trebale ulagati u istraživanje i razvitak etičnih alata utemeljenih na vještačkoj inteligenciji za otkrivanje radnji online materijala seksualnog zlostavljanja djece i online uznemiravanja i maltretiranja i to u suradnji s 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 osobnih podataka.

Referencije

Tekst Opće uredbe o zaštiti podataka (Uredba (EU) 2016/679 Parlamenta i Vijeća Europe od 27. travnja 2016. O zaštiti fizičkih osoba u vezi s obradom osobnih podataka i slobodnom kretanju tih podataka, a kojom se izvan snage stavlja Direktiva 95/46/EC (Opća uredba o zaštiti podataka) i tekst iste objavljen u Službenom listu EU.

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

BBC politika:

- Politika zaštite djece i provedbe mjera zaštite djece, verzija 2017., revidirana 2018. i ažurirana verzija 2019.
- Okvir za neovisne producentske kuće koje rade na produkcijama BBC-a o pravilima eksternih operatera o zaštiti djece;
- Smjernice: Interakcija s 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 skupine za seksualno iskorištavanje djece u Terminološkim smjernicama za zaštitu djece od seksualnog iskorištavanja i seksualnog zlostavljanja, 2016. (Luksemburške smjernice), Konvencije Vijeća Europe o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja, 2007., kao i UNICEF-ovog Global Kids Online izvješća, 2019.

Adolescent

Adolescenti su osobe starosti između 10 i 19 godina. Važno je napomenuti da „adolescenti“ nisu obvezujući 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 sustave koji su čista znanstvena fantastika (tzv. "jaka“ vještačka inteligencija sa samosvjesnom formom) i sustave koji su već operativni i sposobni za obavljanje vrlo složenih zadataka (ovi su sustavi opisani kao „slaba“ ili „umjerena“ vještačka inteligencija, poput prepoznavanja lica ili glasa i upravljanja vozilima.)

Sustavi vještačke inteligencije

Sustav vještačke inteligencije je sustav utemeljen na stroju koji može, za određeni skup ciljeva koje definira čovjek, davati predviđanja, preporuke ili odluke koje utječu na stvarno ili virtualno okruženje. Sustavi vještačke inteligencije su osmišljeni za funkcioniranje na različitim razinama autonomije.

Alexa

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

UNICEF i ITU, “Smjernice za IKT kompanije u pogledu sigurnosti djece na internetu”, 2014.
Vijeće Europe, “Što je vještačka inteligencija?”.
OECD (2019), Preporuke Vijeća o vještačkoj inteligenciji, https://webcache.googleusercontent
UNICEF i ITU, “Smjernice za IKT kompanije u pogledu sigurnosti djece na internetu”, 2014.

Najbolji interes djeteta

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

Dijete

Sukladno članku 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 seksualnog iskorištavanja i zlostavljanja djece, npr. (a) poticanje ili prinuđivanje djeteta da se bavi bilo kojom nezakonitom seksualnom aktivnošću; (b) iskorištavanje djece za prostituciju ili druge nezakonite seksualne radnje; (c) izrabljivačka uporaba 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 putem interneta ili u vezi s online okruženjem.

Seksualno iskorištavanje i zlostavljanje djece

Brza evolucija IK tehnologija stvorila je nove oblike seksualnog iskorištavanja i zlostavljanja djece na internetu, koji se mogu odvijati virtualno i ne moraju uključivati fizički susret licem u lice s djetetom. Iako pravni sustavi u velikom broju država još uvijek označavaju slike i videozapise 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 sukladno Smjernicama Povjerenstva za širokopojasnu mrežu i odgovoru globalne suradnje u borbi protiv seksualnog iskorištavanja i zlostavljanja djece "WePROTECT Global Alliance Model National Response". Ovaj pojam preciznije opisuje sadržaj. Pornografija se odnosi na zakonitu, komercijaliziranu industriju, a kako Luksemburške smjernice navode da uporaba 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" 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; spolni organi djece kada se slike proizvode ili koriste prvenstveno u seksualne svrhe.

Vidi Luksemburške smjernice za izraze poput „kompjutorski ili digitalno generiran materijal seksualne zlouporabe djece".

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

Djeca i mladi

Opisuje osobe mlađe od 18 godina, pri čemu pojam "djeca", koja se u smjernicama također nazivaju i mlađom djecom, obuhvaća sve osobe mlađe od 15 godina i mlađe osobe između 15 i 18 godina starosti.

Igračke s internet konekcijom

Igračke s internet konekcijom se povezuju na internet pomoću tehnologija kao što su Wi-Fi i Bluetooth i obično rade zajedno s pratećim aplikacijama kako bi djeci omogućile interaktivnu igru. Prema Juniper Researchu, 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 osobne podatke od djece, uključujući imena, geolokaciju, adrese, fotografije, audio i videozapise.

Cyber maltretiranje

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

Cyber mržnja, diskriminacija i nasilni ekstremizam

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

Digitalno građanstvo

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

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

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

Luksemburške smjernice 2016 i Izvješće 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 s povrjeđivanjem na internetu. Također se odnosi na emocionalnu inteligenciju potrebnu kako 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 sve osobe koje su na položaju u upravnoj ili rukovodećoj strukturi škole.

(Online) pedofilsko zbližavanje

Pedofilsko (online) zbližavanje, kako je definirano u Luksemburškim smjernicama, odnosi se na „postupak uspostave/izgradnje odnosa s djetetom osobno ili putem interneta ili drugih digitalnih tehnologija kako bi se olakšao seksualni kontakt na internetu ili izvan njega". To je kaznena aktivnost zbližavanja s djetetom ... ,s ciljem nagovaranja djeteta na seksualni odnos.

Informacijske i komunikacijske tehnologije

Informacijske i komunikacijske tehnologije (IKT) opisuju sve informacijske 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 sustave.

Igranje online igrica

„Online igranje" se definira 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. „Ekosustav online igara" definiran je tako da uključuje gledanje drugih kako igraju videoigre putem e-sporta, streaminga ili platforme za razmjenu videozapisa, što obično pruža mogućnost gledateljima da komentiraju ili komuniciraju s igračima i ostalim članovima publike.

Western Sydney University, "Što 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 sigurnosti 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 kontroliraj 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 također 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 s uređaja. Ovi programi su obično zaštićeni lozinkom.

Osobni podaci

Ovaj pojam opisuje informacije o osobi koje se mogu pojedinačno identificirati 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 čimbenik koji omogućuje fizičko ili online kontaktiranje ili lokalizaciju osobe. U ovom kontekstu, ovo se odnosi i na sve informacije o djetetu i njegovoj pratnji koje pružatelji 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 osobnih podataka na mreži, posjedovanja javnog profila na društvenim mrežama, dijeljenja informacija s ljudima koje su djeca upoznala na mreži, korištenja postavki privatnosti, dijeljenja lozinki s prijateljima i brige o privatnosti.

Javni servisi

Riječ je o nacionalnim emiterima ili medijima koji su dozvolu za emitiranje dobili na temelju niza ugovornih obveza s državom ili parlamentom. Ove obveze u mnogim zemljama proteklih godina proširene su na suzbijanje posljedica digitalne transformacije putem medija i programa digitalne pismenosti i obveza rješavanja digitalne podjele.

Sexting

Sexting se obično definira kao slanje, primanje ili razmjena osobno proizvedenog seksualnog sadržaja, uključujući slike, poruke ili videozapise 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 trebali gledati. Dijeljenje seksualnih slika odrasle osobe s djetetom uvijek je kazneno 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 sigurnosti djece na internetu", 2014. (kako je navedeno iznad)

Povjerenstvo 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 komunikacijskim mrežama i izvještavaju o svom statusu odnosno okruženju.

URL

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

Virtualna stvarnost

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

WI-FI

Wi-Fi (engl. *Wireless Fidelity*) je skupina tehničkih standarda koji omogućuju prijenos podataka putem bežičnih mreža.

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

With the support of:

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

ISBN: 978-92-61-30411-9

Objavljeno u Švicarskoj
Geneva, 2020 Fotografije:
Shutterstock