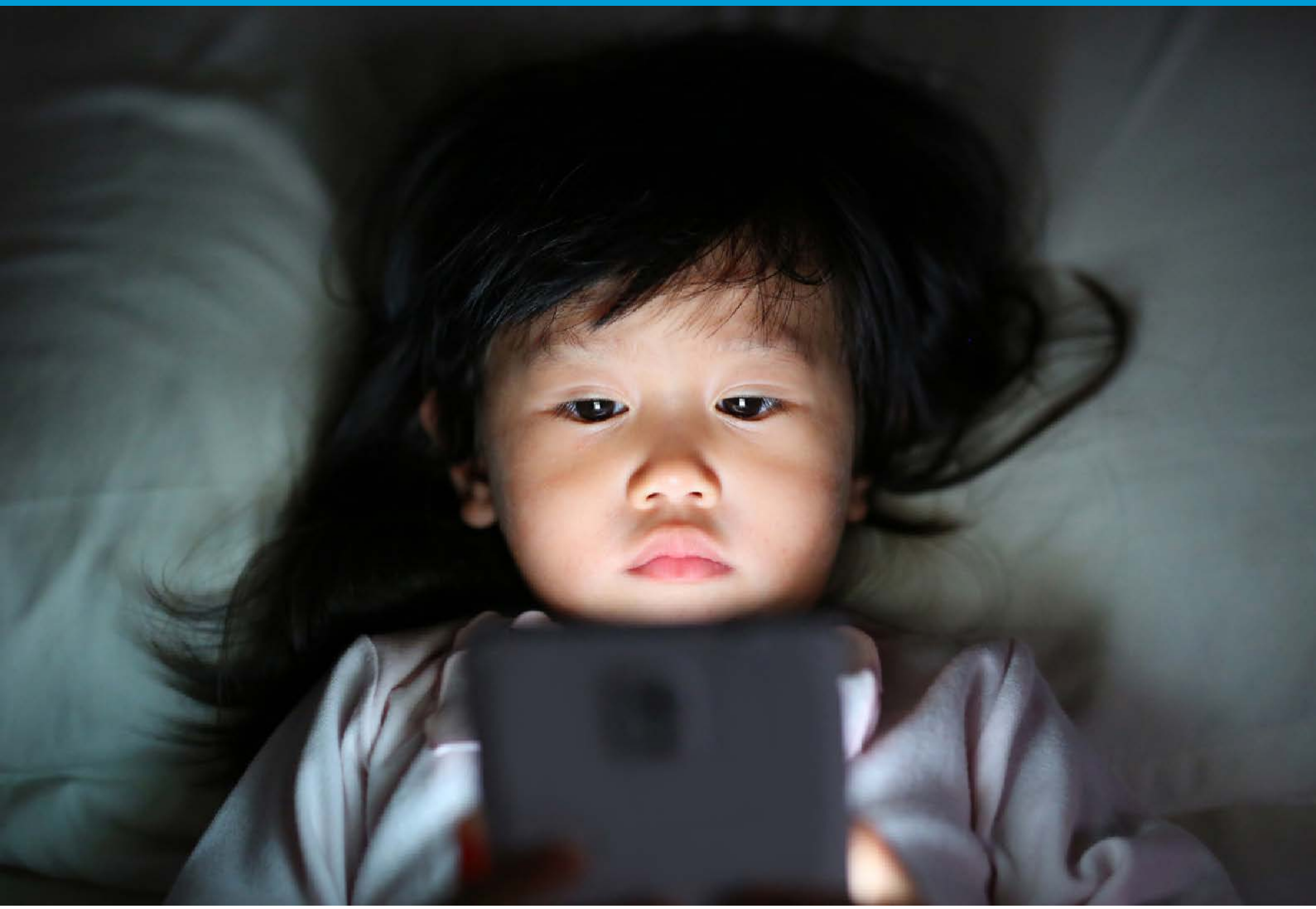
ITUPublications

Međunarodna unija za telekomunikacije
Odjeljenje za razvoj

Smjernice za kreatore politika o zaštiti djece na internetu

2020



Smjernice za kreatore politika o zaštiti djece na internetu

2020

Priznanja

Ove smjernice su razvile Međunarodna unija za telekomunikacije (ITU) i radna grupa autora koji su dali doprinos, a dolaze iz vodećih institucija aktivnih u sektoru informacionih i komunikacionih tehnologija (IKT), kao i na pitanjima dječije zaštite (na internetu), a bile su uključene i sljedeće organizacije:

ECPAT International, Global Kids Online mreža, Globalno partnerstvo za zaustavljanje nasilja nad djecom, projekat HABLATAM, Nesigurna mreža centara za sigurniji internet (Insafe), INTERPOL, Međunarodni centar za nestalu i iskorištenu djecu (ICMEC), Međunarodna alijansa za osobe sa invaliditetom (IDA), Međunarodna unija za telekomunikacije (ITU), The Internet Watch Foundation (IWF), Londonska škola ekonomije, Kancelarija specijalnog predstavnika generalnog sekretara za borbu protiv nasilja nad djecom i specijalni izvjestilac o prodaji i seksualnom iskorištavanju djece, Privately SA, RNW Media, Centri za sigurniji internet iz Velike Britanije, Globalni savez WePROTECT (WPGA) i Svjetska fondacija za djetinjstvo iz SAD-a.

Radnom grupom predsjedao je David Wright (Centri za sigurniji internet iz Velike Britanije / SWGfL), a koordinisala je Fanny Rotino (ITU).

Ove smjernice ne bi bile moguće bez vremena, entuzijazma i predanosti autora koji su dali svoj doprinos. Neprocjenjive doprinose dali su i COFACE-porodice Evrope, Savjet Evrope, australijski povjerenik eSafety, Evropska komisija, e-Worldwide Group (e-WWG), OECD, Omladina i mediji u Berkman Klein centru za internet i Društvo na univerzitetu Harvard, kao i pojedine nacionalne vlade i interesne strane u industriji koje dijele zajednički cilj da naprave internet boljim i sigurnijim mjestom za djecu i mlade.

ITU je zahvalan sljedećim partnerima koji su dali svoje dragocjeno vrijeme i uvide: (navedeno abecednim redom organizacije):

- Martin Schmalzried (COFACE-porodice Evrope)
- Livia Stoica (Savjet Evrope)
- John Carr (ECPAT International)
- Julia Fossi i Ella Serry (povjerenici eSafety)
- Manuela Marta (Evropska komisija)
- Salma Abbasi (e-WWG)
- Amy Crocker i Serena Tommasino (Globalno partnerstvo za zaustavljanje nasilja nad djecom)
- Lionel Brossi (HABLATAM)
- Sandra Marchenko (ICMEC)
- Karl Hopwood (Insafe)[1]
- Lucy Richardson (Međunarodna alijansa za osobe sa invaliditetom - IDA)
- Matthew Dompier (Interpol)
- Fanny Rotino (ITU)
- Tess Leyland (IWF)
- Sonia Livingstone (Londonska škola ekonomije i Global Kids Online)

---

1 *U okviru Instrumenta za povezivanje Evrope (CEF), European Schoolnet u ime Evropske komisije pokreće platformu Bolji internet za djecu, koja uključuje koordinaciju Insafe mreže evropskih centara za sigurniji internet. Više informacija dostupno je na* www.betterinternetforkids.eu

- Elettra Ronchi (OECD)
- Manus De Barra (Kancelarija specijalnog predstavnika generalnog sekretara za borbu protiv nasilja nad djecom)
- Deepak Tewari (Privately SA)
- Pavithra Ram (RNW Media)
- Maud De Boer-Buquicchio (specijalna izvjestiteljica Ujedinjenih nacija o prodaji i seksualnom iskorištavanju djece)
- David Wright (Centri za sigurniji internet u Velikoj Britaniji / SWGfL)
- Iain Drennan i Susannah Richmond (Globalni savez WePROTECT)
- Lina Fernandez i dr. Joanna Rubinstein (Svjetska fondacija za djetinjstvo iz SAD-a)
- Sandra Cortesi (Omladina i mediji)

ISBN

978-92-61-30121-7 (Štampana verzija)

978-92-61-30451-5 (Elektronska verzija)

978-92-61-30111-8 (EPUB verzija)

978-92-61-30461-4 (Mobi verzija)

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

Predgovor

U svijetu u kojem internet prožima gotovo sve aspekte modernog života, održavanje bezbijednosti mladih korisnika na internetu postalo je sve hitnije pitanje svake zemlje.

ITU je svoj prvi set Smjernica o zaštiti djece na internetu razvio još 2009. godine. Od tih ranih dana, internet je evoluirao do neprepoznatljivosti. Iako je djeci postao beskrajno bogatiji resurs za igru i učenje, postao je i mnogo opasnije mjesto za njih da se odvaže da ga koriste bez pratnje.

Od pitanja privatnosti do nasilnog i neprimjerenog sadržaja, do prevaranata na internetu i širokog spektra vrbovanja, seksualnog zlostavljanja i iskorištavanja na internetu, današnja djeca suočena su s mnogim rizicima. Prijetnje se umnožavaju, a počinioci sve više istovremeno djeluju u mnogim različitim pravnim jurisdikcijama, ograničavajući efikasnost reagovanja i pravnih lijekova specifičnih za pojedine zemlje.

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

Očuvanje bezbijednosti djece na internetu više nego ikad prije traži zajednički i koordinisani međunarodni odgovor, zahtijevajući aktivno uključivanje i podršku velikog broja interesnih strana - od interesnih strana u industriji, uključujući platforme privatnog sektora, pružaoca usluga i mrežnih operatera, do vlada i civilnog društva.

Prepoznavši to, 2018. godine države članice ITU-a zatražile su nešto više od pravovremenog osvježavanja Smjernica za zaštitu djece na internetu što je s vremena na vrijeme bilo rađeno u prošlosti. Umjesto toga, ove nove revidirane smjernice iznova su osmišljene, ponovo napisane i preoblikovane kako bi odražavale vrlo značajne pomake u digitalnom krajoliku u kojem se djeca nalaze.

Pored odgovora na nova dostignuća 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 učestvovanje. Obuhvaćeno je i razmatranje posebnih potreba djece migranata i drugih ranjivih grupa.

Nadamo se da će ove smjernice kreatorima politika poslužiti kao čvrst temelj na kojem će se razviti inkluzivne nacionalne strategije sa više interesnih strana, uključujući otvorene konsultacije i dijalog s djecom, kako bi se razvile bolje ciljane mjere i efikasnije djelovanje.

Razvijajući ove nove smjernice, ITU i partneri nastojali su stvoriti vrlo upotrebljiv, fleksibilan i prilagodljiv okvir čvrsto zasnovan na međunarodnim standardima i zajedničkim ciljevima - posebno na Konvenciji o pravima djeteta i ciljevima održivog razvoja Ujedinjenih nacija. U pravom duhu uloge ITU-a kao globalnog sazivača, ponosna sam na činjenicu da su ove revidirane smjernice proizvod globalnih zajedničkih napora i da su u njihovom koautorstvu međunarodni stručnjaci iz široke zajednice sa više interesnih strana.

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

U doba kada sve više mladih ljudi koristi internet, ove Smjernice za zaštitu djece na internetu su važnije nego ikad. Kreatori politika, industrija, roditelji i nastavnici - i sama djeca - svi imaju vitalnu ulogu. Zahvalna sam, kao i uvijek, na vašoj podršci i radujem se nastavku naše bliske saradnje po ovom kritičnom pitanju.

Doreen Bogdan-Martin
direktorica, Biro za razvoj telekomunikacija (BDT)

Predgovor

Prije trideset godina, gotovo sve vlade obavezale su se da će poštovati, štititi i promovisati dječija prava. UN Konvencija o pravima djeteta (CRC) najrašireniji je ratifikovani međunarodni ugovor o ljudskim pravima u istoriji. Iako je u protekle tri decenije postignut značajan napredak, ostaju značajni izazovi i pojavila su se nova područja rizika za djecu.

2015. godine sve su nacije obnovile posvećenost djeci u agendi 2030. i 17 univerzalnih ciljeva održivog razvoja (SDG). Cilj 16.2, na primjer, poziva na zaustavljanje zlostavljanja, eksploatacije i svih oblika nasilja i mučenja nad djecom do 2030. godine. Ali zaštita djece je zajednička nit unutar 11 od 17 ciljeva održivog razvoja. UNICEF stavlja djecu u središte agende 2030. godine kako je prikazano na slici 1.

Slika 1: Djeca, informacione i komunikacione tehnologije (IKT) i ciljevi održivog razvoja (SDG)

Agenda za održivi razvoj do 2030. prepoznaje da informacione i komunikacione tehnologije (IKT) mogu biti ključni faktor za postizanje ciljeva održivog razvoja. Širenje informacione i komunikacione tehnologije (IKT) i globalna međusobna povezanost potencijalno mogu ubrzati ljudski napredak, premostiti digitalnu podjelu i razviti društva znanja. Ono dalje definiše specifične ciljeve za upotrebu IKT-a za održivi razvoj u obrazovanju (Cilj 4), rodnu ravnopravnost (Cilj 5), infrastrukturu (Cilj 9 - univerzalan i povoljan pristup internetu) i Cilj 17 - partnerstva i sredstva za implementaciju[1]. IKT imaju moć duboke transformacije ekonomije u cjelini čineći pokretačku snagu u postizanju svakog od 17 ciljeva održivog razvoja. IKT su svoj potez već pokrenuli dajući mogućnosti milijardama pojedinaca širom svijeta - pružajući, između ostalog, pristup obrazovnim resursima i zdravstvenoj zaštiti, te uslugama poput e-uprave i društvenih medija.

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

Ali širi i dostupniji pristup internetu i mobilnoj tehnologiji takođe predstavljaju značajne izazove za dječiju sigurnost i dobrobit - kako na internetu tako i izvan njega.

---

1 UNDP, Ciljevi održivog razvoja | UNDP, undp.org, pristupljeno 29. januara 2020., https://www.undp.org/content/undp/en/home/sustainable-development-goals.html; Houlin Zhao, "Zašto su IKT toliko ključne za postizanje ciljeva održivog razvoja," *ITU*, ITU novinski časopis, 48, pristupljeno 29. januara 2020, https://www.itu.int/en/ itunews/Documents/2017/2017-03/2017_ITUNews03-en.pdf.

Da bi se smanjili rizici digitalnog svijeta, a istovremeno omogućilo većem broju djece i mladih da iskoriste njegove koristi, vlade, civilno društvo, lokalne zajednice, međunarodne organizacije i industrija moraju se udružiti u zajedničkoj svrsi. Posebno su potrebni kreatori politika kako bi se postigao međunarodni cilj da djeca budu sigurna na internetu.

Kako bi odgovorila na izazove koje postavlja brzi razvoj IKT i izazove zaštite djece koje on donosi, u novembru 2008. godine Inicijativa o zaštiti djece na na internetu (COP) pokrenuta je kao međunarodna inicijativa sa više interesnih strana od strane Međunarodne unije za telekomunikacije (ITU). Cilj ove inicijative je okupiti partnere iz svih sektora globalne zajednice kako bi stvorili sigurno internetsko iskustvo sa puno mogućnosti za djecu širom svijeta.

Štaviše, Konferencija opunomoćenika Međunarodne unije za telekomunikacije održana u Dubaiju 2018. godine potvrdila je važnost inicijative zaštite djece na internetu priznavši je kao platformu za podizanje svijesti, razmjenu najboljih praksi i pružanje pomoći i podrške državama članicama, posebno zemljama u razvoju, u razvoju i primjeni razvojnih puteva za zaštitu djece na internetu. Takođe je prepoznala važnost zaštite djece na internetu u okviru UN Konvencije o pravima djeteta i drugih ugovora o ljudskim pravima podstičući saradnju između svih interesnih strana uključenih u zaštitu djece na internetu.

Konferencija je prepoznala Agendu za održivi razvoj 2030, baveći se različitim aspektima zaštite djece na internetu u Ciljevima održivog razvoja (SDG), posebno Ciljeve održivog razvoja 1, 3, 4, 5, 9, 10 i 16; dalje je priznala Rezoluciju 175 (Rev. Dubai, 2018.) o pristupačnosti za osobe s invaliditetom i osobe sa posebnim potrebama telekomunikacionim / informacionim i komunikacionim tehnologijama (IKT) i Rezoluciju 67 (Rev. Buenos Aires, 2017.) Svjetske konferencije o razvoju telekomunikacija (WTDC), o ulozi ITU-ovog sektora za razvoj telekomunikacija (ITU-D) u zaštiti djece na internetu.

Krajem 2019. godine, ITU / UNESCO-ova komisija za širokopojasni pristup za održivi razvoj pokrenula je Izvještaj o sigurnosti djece na internetu s djelotvornim preporukama kako učiniti internet sigurnijim za djecu.

2009. godine ITU je objavio prvi set smjernica o zaštiti djece na internetu, u kontekstu Inicijative za zaštitu djece na internetu. Tokom posljednje decenije, smjernice za zaštitu djece na internetu prevedene su na mnoge jezike i koristile su ih mnoge zemlje svijeta kao referentnu tačku za razvojne puteve i nacionalne strategije povezane sa zaštitom djece na internetu. Služile su nacionalnim vladinim tijelima, organizacijama civilnog društva, institucijama za brigu o djeci, industriji i mnogim drugim interesnim stranama u njihovim naporima da zaštite djecu na internetu.

Preciznije, smjernice su korištene za izradu, razvoj i implementaciju nacionalnih strategija zaštite djece na internetu u mnogim državama članicama kao što su Kamerun, Gabon, Gambija, Gana, Kenija, Sijera Leone, Uganda i Zambija u afričkoj regiji; Bahrein i Oman u arapskoj regiji; Brunej, Kambodža Kiribati, Indonezija, Malezija, Mjanmar i Vanuatu u azijsko-pacifičkoj regiji; i Bosna i Hercegovina, Gruzija, Moldavija, Crna Gora, Poljska i Ukrajina u evropskom regionu.

Nadalje, smjernice su stvorile temelj za regionalne događaje poput Regionalne konferencije o zaštiti djece na internetu (ACOP): Pružanje mogućnosti budućim digitalnim građanima u Kampali u Ugandi (2014) i ASEAN-ova regionalna konferencija o zaštiti djece na internetu održana u Bangkoku na Tajlandu (2020).

Prema Rezoluciji 179 (Rev. Dubai, 2018), ITU-u je u saradnji s partnerima inicijative za zaštitu djece na internetu i interesnim stranama naloženo da ažurira četiri seta smjernica uzimajući u obzir tehnološki razvoj u telekomunikacionoj industriji, uključujući smjernice za djecu s invaliditetom i djecu sa specifičnim potrebama.

Kao rezultat ovog procesa, ove su smjernice značajno ažurirane i pregledane od strane stručnjaka i relevantnih interesnih strana, uspostavljajući širok set preporuka za zaštitu djece u digitalnom svijetu. Rezultat su zajedničkog napora više interesnih strana, i korištenja znanja, iskustva i stručnosti mnogih organizacija i pojedinaca iz cijelog svijeta na polju zaštite djece na internetu. Cilj im je uspostaviti temelje sigurnog i bezbijednog sajber svijeta za buduće generacije. One treba da djeluju kao nacrt koji se može prilagoditi i koristiti na način koji je u skladu s nacionalnim ili lokalnim običajima i zakonima. Štaviše, ove smjernice se bave pitanjima koja pogađaju svu djecu i mlade mlađe od 18 godina, prepoznajući različite potrebe svake starosne grupe. Dalje, one imaju za cilj da odgovore na potrebe djece u različitim životnim uslovima i djece sa posebnim potrebama i invaliditetom. Smjernice takođe jačaju obim zaštite djece na internetu, baveći se svim rizicima, prijetnjama i štetama s kojima se djeca mogu susresti na internetu i pažljivo ih balansirajući s prednostima koje digitalni svijet može donijeti u dječiji život.

Postoji nada da će ove smjernice dovesti ne samo do izgradnje sveobuhvatnijeg informacionog društva, već će i omogućiti državama članicama ITU-a da ispune svoje obaveze prema zaštiti i ostvarivanju prava djece kako je utvrđeno u UN Konvenciji o pravima djeteta[2], usvojenoj Rezolucijom Generalne skupštine Ujedinjenih nacija 44/25 od 20. novembra 1989. godine i Ishodnim dokumentom Svjetskog samita o informacionom društvu[3] (WSIS).

Izdavanjem ovih smjernica, inicijativa za zaštitu djece na internetu poziva sve interesne strane da sprovode politike i strategije koje će zaštititi djecu u sajber prostoru i promovisati njihov sigurniji pristup svim izvanrednim mogućnostima koje resursi na internetu mogu pružiti.

2 UNICEF, "Konvencija o pravima djeteta," unicef.org, pristupljeno 29. januara 2020, https://www.unicef.org/child-rights-convention.

3 WSIS je održan u dvije faze: u Ženevi (10-12. Decembra 2003.) i u Tunisu (16-18. Novembra 2005.). Na Svjetskom samitu o informacionom društvu je zaključeno da će se hrabrim zalaganjem „izgraditi informativno društvo usmjereno na ljude, inkluzivno i razvojno orijentisano, gdje svi mogu stvarati, pristupati, koristiti i dijeliti informacije i znanje".

Sadržaj

Spisak tabela, slika i izdvojenih tekstova

Tabele

Slike

Izdvojeni tekstovi

1. Pregled dokumenta

1.1 Svrha

Nacionalne vlade su dužne osigurati zaštitu djece u fizičkom i virtuelnom svijetu. Važno je uvidjeti da više nema smisla pokušavati održavati krute razlike između događaja iz svtarnog svijeta i internetskih događaja, jer su nove tehnologije sada potpuno integrisane u živote tolikog broja djece i mladih. Ova dva svijeta su sve više isprepletena i međusobno zavisna.

Kreatori politika[1] i sve druge relevantne interesne strane imaju vrlo važne uloge. Brzina kojom se tehnologija razvija znači da mnoge tradicionalne metode kreiranja politika više ne odgovaraju ovoj svrsi. Od kreatora politika se zahtijeva da razviju pravni okvir koji je prilagodljiv, inkluzivan i odgovara svojoj svrsi u brzo promjenjivom digitalnom dobu radi zaštite djece na internetu.

Svrha ovih smjernica je ponuditi kreatorima politika u državama članicama ITU-a jednostavan i fleksibilan okvir za razumijevanje i postupanje u skladu sa njihovom zakonskom obavezom da osiguraju zaštitu djece u stvarnom, fizičkom i virtuelnom svijetu.

Smjernice to čine bavljenjem nekolikim važnim pitanjima za kreatore politika:

1) Šta je zaštita djece na internetu?
2) Zašto ja kao kreator politika moram brinuti o zaštiti djece na internetu?
3) Koji je pravni, društveno-politički i razvojni kontekst moje zemlje?
4) Kako kreatori politika trebaju početi razmatrati i oblikovati efikasnu i održivu politiku zaštite djece na internetu u svojoj zemlji?

Pritom se smjernice oslanjaju na postojeće modele, okvire i resurse kako bi pružile kontekst i uvid u dobru praksu iz cijelog svijeta.

1.2 Obim

Obim zaštite djece na internetu proširuje se na svaku štetu kojoj su djeca izložena na internetu, pokrivajući širok spektar rizika koji ugrožavaju sigurnost i dobrobit djece. To je složen izazov kojem se mora pristupiti iz više uglova, uključujući zakonodavstvo, upravljanje, obrazovanje, politiku i društvo.

Pored toga, zaštita djece na internetu mora se zasnivati na razumijevanju opštih i specifičnih rizika, prijetnji i šteta za djecu u digitalnom okruženju. To zahtijeva jasne definicije i uspostavljanje jasnih parametara za intervenciju koji uključuju i razlikuju djela koja čine krivično djelo od onih koja, iako nisu nezakonita, ipak predstavljaju prijetnju dobrobiti djeteta.

U tu svrhu smjernice pružaju pregled trenutnih prijetnji i šteta s kojima se suočavaju djeca u digitalnom okruženju. Uprkos tome, brzina kojom se tehnologija i pridružene prijetnje i štete razvijaju znači da tradicionalna brzina i način kreiranja politika nisu u stanju da idu ukorak. Kreatori politika u digitalno doba trebaju izgraditi pravne i političke okvire koji su

1 Pojam kreatori politika ovdje se odnosi na sve interesne strane koje su odgovorne za razvoj i sprovođenje politike, posebno one unutar vlade.

dovoljno prilagodljivi i inkluzivni da mogu da se nose sa postojećim izazovima i što je više moguće predvide one koji dolaze. Da biste to učinili, potrebna je saradnja sa svim interesnim stranama, uključujući IKT industriju, istraživačku zajednicu, civilno društvo, javnost i samu djecu. Ovaj proces može biti podržan razmatranjem opštih načela zaštite djece na internetu.

1.3 Opšta načela

Jedanaest opštih načela koja su ovdje izložena, a uzeta zajedno, pomoći će u razvoju perspektivne i cjelovite nacionalne strategije zaštite djece na internetu.

Redoslijed ovih načela prije odražava logički narativ nego poredak po važnosti.

Razvoj nacionalne strategije zaštite djece na internetu trebao bi:

1. zasnivati se na cjelovitoj viziji koja uključuje vladu, industriju i društvo;
2. da bude rezultat sveobuhvatnog razumijevanja i analize cijelog digitalnog okruženja, a ipak prilagođen okolnostima i prioritetima zemlje;
3. da poštuje i da bude u skladu sa osnovnim pravima djece utvrđenim UN Konvencijom o pravima djeteta i drugim ključnim međunarodnim konvencijama i zakonima;
4. da poštuje i da bude dosljedan postojećim, sličnim i srodnim domaćim zakonima i strategijama koje su na snazi, kao što su zakoni o zlostavljanju djece ili strategije sigurnosti djece;
5. da poštuje dječija građanska prava i slobode, koje ne bi trebalo žrtvovati radi zaštite;
6. da bude razvijen uz aktivno učešće svih relevantnih interesnih strana, uključujući djecu, rješavajući njihove potrebe i odgovornosti i zadovoljavajući potrebe manjinskih i marginalizovanih grupa;
7. da bude dizajniran da se uskladi sa širim vladinim planovima za ekonomski i socijalni prosperitet i da maksimalizuje doprinos IKT održivom razvoju i socijalnoj inkluziji;
8. da koristi najprikladnije dostupne instrumente politike za ostvarenje svog cilja, uzimajući u obzir specifične okolnosti zemlje;
9. da bude postavljen na najviši nivo vlasti, koji će biti odgovoran za dodjeljivanje relevantnih uloga i odgovornosti i raspodjelu dovoljnih ljudskih i finansijskih resursa;
10. da pomogne u izgradnji digitalnog okruženja u koje djeca, roditelji / staratelji i interesne strane mogu imati povjerenje;
11. da usmjeri napore interesnih strana na pružanje mogućnosti i obrazovanje djece o digitalnoj pismenosti kako bi se zaštitili na internetu.

1.4 Korištenje ovih smjernica

Ove smjernice uzimaju u obzir relevantna istraživanja, postojeće modele i materijale i daju jasne preporuke za razvoj nacionalne strategije zaštite djece na internetu.

- Odjeljak 2 nam predstavlja zaštitu djece na internetu i daje uvid u nedavna istraživanja, uključujući aspekte novih tehnologija, ključnih prijetnji i šteta za djecu.
- Odjeljak 3 navodi kako se pripremiti za nacionalnu strategiju zaštite djece na internetu, uključujući relevantne interesne strane, postojeće primjere reagovanja na prijetnje i štete na internetu i koristi postojanja nacionalne strategije.
- Odjeljak 4 pokriva preporuke za okvire i implementaciju.
- Odjeljak 5 daje nacionalne kontrolne liste za razvoj nacionalne strategije zaštite djece na internetu.
- Odjeljak 6 daje korisne referentne materijale.

2. Uvod

U 2019. godini više od polovine svjetske populacije koristilo je internet. Najveća grupa korisnika su oni mlađi od 44 godine, sa podjednako visokom upotrebom među 16 do 24 godine i 35 do 44 godine. Na globalnom nivou, svako treće dijete koristi internet (0-18 godina)[2]. U zemljama u razvoju djeca i mladi prednjače u korištenju interneta[3], a procjenjuje se da će se ova populacija više nego udvostručiti tokom sljedećih pet godina. Nove generacije odrastaju uz internet i većina se povezuje s tehnologijom mobilne mreže, posebno na globalnom jugu[4].

Iako je pristup internetu osnovni za ostvarivanje prava djece, još uvijek postoje značajne regionalne, nacionalne, rodne i druge razlike u pristupu koje ograničavaju mogućnosti za djevojčice, djecu s invaliditetom, djecu iz manjina i druge ranjive grupe. U pogledu digitalne rodne podjele, istraživanje pokazuje da u svim regijama, osim u Sjedinjenim Američkim Državama, muški korisnici interneta uglavnom premašuju ženske korisnike. U mnogim zemljama djevojke nemaju iste mogućnosti pristupa kao dječaci, a tamo gdje ih imaju, djevojke ne samo da su u velikoj mjeri praćene i ograničene u korištenju interneta, već mogu i da ugroze svoju sigurnost u nastojanju da pristupe internetu[5]. Jasno je da djeca i mladi koji nemaju digitalne vještine ili govore manjinske jezike ne mogu lako pronaći odgovarajući sadržaj na internetu i da djeca iz ruralnih područja imaju manje digitalnih vještina, provode više vremena na internetu (posebno igrajući igrice) i dobijaju manje roditeljskog posredovanja i nadzora[6].

Međutim, nijedan razgovor o rizicima i prijetnjama ne može se odvijati bez priznavanja izuzetno obogaćujuće i osnažujuće prirode digitalne tehnologije. Internet i digitalne tehnologije transformišu način na koji živimo i otvorili su mnoge nove načine komunikacije, igranja igara, uživanja u muzici i uključivanja u široki niz kulturnih, obrazovnih aktivnosti i aktivnosti za poboljšanje vještina. Internet može pružiti presudan pristup zdravstvenim i obrazovnim uslugama, kao i informacije o temama koje su važne za mlade, ali mogu biti tabu u njihovim društvima.

Kao što su djeca i mladi često među prvima u usvajanju i prilagođavanju novim mogućnostima koje im pruža internet, tako su među prvima izloženi i nizu problema vezanih za sigurnost i dobrobit koje društvo mora prepoznati i suočiti se sa njima. Bitno je otvoreno razgovarati o rizicima koji postoje za djecu i mlade na internetu. Diskusija otvara platformu sa koje se djeca i mladi mogu naučiti kako prepoznati rizik i spriječiti ili riješiti štetu ako se ona ostvari, kao i prednosti i mogućnosti koje internet može ponuditi.

2 OECD, “Nove tehnologije i djeca 21. vijeka: Najnoviji trendovi i ishodi,” Radni dokument OECD-a o obrazovanju br. 179 (Direkcija za obrazovanje i razvoj vještina, OECD), pristupljeno 27. januara 2020, https://www .oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282018%2915&docLanguage =En.

3 Ofcom, “Djeca i roditelji: Izveštaj o upotrebi medija i stavovima za 2018. godinu “(Ofcom), pristupljeno 17. januara 2020. godine, https://www.ofcom.org.uk/_data/assets/pdf_file/0024/134907/children-and-parents-media-use-and -attitudes-2018.pdf.

4 ITU, “Izvještaj o mjerenju informacionog društva,” pristupljeno 16. januara 2020, https://www.itu.int/dms_pub/ itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-E.pdf.

5 “Mladi adolescenti i digitalni mediji: Upotrebe, rizici i mogućnosti u zemljama sa niskim i srednjim dohotkom, ”GAGE, pristupljeno 29. januara 2020,https://www.gage.odi.org/publication/digital-media-risks -opportunities/.

6 Livingstone, S., Kardefelt Winther, D., i Hussein, M. (2019). Global Kids Online uporedni izvještaj, izvještaj o istraživanju Innocenti. UNICEF-ova kancelarija za istraživanje - Innocenti, Firenca, https://www.unicef-irc .org/publications/1059-global-kids-online-comparative-report.html. Ovo može imati neočekivane rezultate, na primjer, istraživanje koje je HABLATAM obavio u pet latinoameričkih zemalja pokazalo je da djeca u ranjivim zajednicama mogu koristiti platforme za upoznavanje, videoigre i društvene mreže za obavljanje novčanih transakcija u nezakonite svrhe. Mreža Contectados al Sur, “Hablatam,” projekat Hablatam 2020, pristupljeno 6. februara 2020, https://hablatam.net/.

U mnogim dijelovima svijeta mladi dobro razumiju neke rizike s kojima se suočavaju na internetu.[7][8] Istraživanje je pokazalo, na primjer, da većina djece i mladih može razlikovati sajber maltretiranje od šale ili zadirkivanja na internetu. Oni prepoznaju da sajber maltretiranje ima javnu dimenziju i da je osmišljeno kako bi naštetilo, ali pronaći balans između djetetovih internetskih mogućnosti i rizika ostaje izazov[9].

Za države članice ITU-a zaštita djece i mladih na internetu i dalje je prioritet, mora se pažljivo izbalansirati s naporima na promociji prilika za djecu i mlade na internetu[10] i da se to mora učiniti na način koji štiti djecu i mlade bez uticaja na njihov pristup ili pristup šire javnosti informacijama ili na mogućnost uživanja slobode govora, izražavanja i udruživanja.

Očigledna je potreba za predanim investicijskim i kreativnim rješenjima za rješavanje rizika s kojima se suočavaju djeca i mladi, ne samo zbog digitalne podjele između djece i odraslih koja ograničava preporuke i savjete roditelja, učitelja i staratelja. Istovremeno, kako djeca i mladi odrastaju i postaju odrasli, roditelji i aktivni članovi društva, postoji potencijalna i neizostavna prilika da smanje digitalnu podjelu.

U svjetlu ovoga, izgradnja povjerenja u internet mora biti u vrhu i u središtu javne politike. Vlade i društvo trebaju raditi s djecom i mladima kako bi razumjeli njihova mišljenja i pokrenuli istinsku javnu raspravu o rizicima i mogućnostima. Podrška djeci i mladima u upravljanju rizicima na internetu može biti efikasna, ali vlade takođe moraju osigurati da postoje odgovarajuće usluge podrške za one koji na internetu budu oštećeni i da djeca znaju kako pristupiti tim uslugama.

Neke zemlje se muče da izdvoje dovoljno resursa da se bore za digitalnu pismenost i sigurnost djece na internetu. Međutim, djeca prijavljuju da su roditelji, nastavnici, tehnološke kompanije i vlade važni igrači u razvoju rješenja koja podržavaju njihovu sigurnost na internetu. Zemlje članice ITU-a takođe su naznačile da postoji značajna podrška za poboljšanu razmjenu znanja i koordinisani napori kako bi se obezbijedila sigurnost većeg broja djece na internetu[9].

Djeca i mladi kreću se kroz sve složeniji digitalni krajolik i usvajanje vještačke inteligencije za mašinsko učenje, analitiku velikih podataka, robotiku, virtuelnu i proširenu stvarnost, i internet stvari uređeni su za transformisanje dječjih medijskih praksi. To zahtijeva kreiranje politike i ulaganja za djecu, roditelje i zajednice u budućnosti kao i danas.

7 Od 2016. ITU provodi konsultacije u okviru zaštite djece na internetu sa djecom i odraslim interesnim stranama o važnim pitanjima kao što su sajber maltretiranje, digitalna pismenost i dječije aktivnosti na internetu.
8 ITU, Omladinske konsultacije, https://www.itu.int/en/council/cwg-cop/Pages/meetings.aspx.
9 UNICEF, “Global Kids Online uporedni izvještaj (2019).”
10 ITU, “Proslava 10 godina zaštite djece na internetu”, ITU vijesti, 6. februara 2018, https://news.itu.int/celebrating-10-years-child-online-protection/.

2.1 Šta je zaštita djece na internetu?

Internet tehnologije djeci i mladima nude brojne mogućnosti komunikacije, učenja novih vještina, da budu kreativni i daju doprinos boljem društvu. Ali one mogu donijeti i nove rizike, poput izlaganja problemima zaštite privatnosti, nezakonitom sadržaju, uznemiravanju, sajber maltretiranju, zloupotrebi ličnih podataka ili vrbovanja u seksualne svrhe, pa čak i seksualnom zlostavljanju djece.

Ove smjernice razvijaju cjelovit pristup za reagovanje na sve potencijalne prijetnje i štete s kojima se djeca i mladi mogu susresti prilikom sticanja digitalne pismenosti. One prepoznaju da sve relevantne interesne strane imaju ulogu u njihovoj digitalnoj otpornosti, blagostanju i zaštiti, dok istovremeno imaju koristi od mogućnosti koje internet može ponuditi.

Zaštita djece i mladih je zajednička odgovornost i uloga svih relevantnih interesnih strana je da osiguraju održivu budućnost za sve. Da bi se to dogodilo, kreatori politika, industrija, roditelji, staratelji, edukatori i druge interesne strane, moraju osigurati da djeca i mladi mogu ostvariti svoj potencijal - na internetu i izvan njega.

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

- reagovanje, podrška i samopomoć u slučaju suočavanja s prijetnjom;
- sprječavanje štete;
- dinamična ravnoteža između osiguranja zaštite i pružanja mogućnosti djeci da budu digitalni građani;
- podržavanje prava i odgovornosti i djece i društva.

Štaviše, zbog brzog napretka u tehnologiji i društvu i bezgranične prirode interneta, zaštita djece na internetu mora biti agilna i prilagodljiva da bi bila efikasna. Iako ove smjernice nude uvid u vodeće rizike za djecu i mlade na internetu, uključujući štetan i nezakonit sadržaj, uznemiravanje, sajber maltretiranje, zloupotrebu ličnih podataka ili vrbovanje u seksualne svrhe i seksualno zlostavljanje i iskorištavanje djece, s razvojem će se pojaviti novi izazovi tehnoloških inovacija i obično će se razlikovati od regije do regije. Međutim, s novim izazovima najbolje će se izaći na kraj u zajedničkom radu u vidu globalne zajednice, jer treba pronaći nova rješenja za te izazove.

2.2 Djeca u digitalnom svijetu

Internet je promijenio naš način života. Potpuno je integrisan u živote djece i mladih, što onemogućava zasebno razmatranje digitalnog i fizičkog svijeta. Trećina svih korisnika interneta danas su djeca i mladi, a UNICEF procjenjuje da je 71% mladih već na internetu.

Takva povezanost izuzetno osnažuje. Svijet interneta omogućava djeci i mladima da prebrode nedostatke i invaliditet, a pružio je nova mjesta za zabavu, obrazovanje, učestvovanje i izgradnju odnosa. Digitalne platforme se danas koriste za razne aktivnosti i često su multimedijska iskustva.

Pristup i učenje korištenja i navigacije ovom tehnologijom smatra se presudnim za razvoj mladih ljudi i prvi se put koristi u ranoj dobi. Kreatori politika moraju razumjeti da djeca i mladi ljudi često počinju koristiti platforme i usluge prije nego što navrše minimalnu starosnu dob, pa obrazovanje mora započeti rano.

Djeca i mladi žele biti uključeni u razgovor i imaju dragocjenu stručnost kao 'digitalni domoroci' što se može dijeliti. Kreatori politika i stručnjaci moraju se uključiti s djecom i mladima u tekuću debatu o internetskom okruženju kako bi podržali njihova prava.

Pristup internetu

U 2019. godini više od polovine svjetske populacije koristilo je internet (53,6 posto), s procijenjenih 4,1 milijardu korisnika. Na globalnom nivou, svaki treći korisnik interneta je dijete mlađe od 18 godina[1]. U nekim zemljama sa nižim dohotkom taj broj raste na otprilike svaki drugi, dok je u zemljama sa višim dohotkom otprilike svaki peti korisnik dijete mlađe od 18 godina. Prema UNICEF-u, širom svijeta 71% mladih već je na internetu[2]. Stoga su djeca i mladi sada u velikoj mjeri, trajno i dosljedno prisutni na internetu[3]. Internet služi u druge društvene, ekonomske ili političke svrhe i postao je porodični ili potrošački proizvod ili usluga koja je sastavni dio načina na koji porodice, djeca i mladi žive svoj život.

U 2017. godini pristup internetu za djecu i mlade na regionalnom nivou je u velikoj je mjeri povezan sa nivoom prihoda. Zemlje sa niskim prihodima imaju tendenciju da imaju manje djece korisnika interneta od zemalja sa visokim prihodima.

Djeca i mladi u većini zemalja vikendom provode više vremena na internetu nego radnim danom, a adolescenti (od 15 do 17 godina) provode najviše vremena na internetu, u prosjeku između 2.5 i 5.3 sata, u zavisnosti od zemlje.

Korištenje interneta

Među djecom i mladima najpopularniji uređaj za pristup internetu je mobilni telefon, a slijede ga stoni računari i laptopi. Djeca i mladi provode u prosjeku oko dva sata dnevno na internetu tokom sedmice i otprilike duplo više od toga svakog dana vikenda. Neki se osjećaju trajno povezanima. Ali mnogi drugi još uvijek nemaju pristup internetu kod kuće.

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

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

3 Livingstone, S., Carr, J., and Byrne, J. (2015) Svako treće: Upravljanje internetom i dječija prava."

U praksi, većina djece i mladih koji koriste internet, pristupaju mu preko više uređaja: Djeca i mladi koji se barem sedmično povežu ponekad koriste do tri različita uređaja da to učine. Starija djeca i djeca u bogatijim zemljama uglavnom koriste više uređaja, a dječaci koriste nešto više uređaja nego djevojčice u svim anketiranim zemljama.

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

Djeca i mladi također se bave politikom putem interneta i čine da se njihov glas čuje putem blogova.

Ukupan nivo učestvovanja u igranju na internetu razlikuje se od zemlje do zemlje približno u skladu s dostupnošću interneta djeci i mladim ljudima, dok se 10% do 30% djece i mladih koji se koriste internetom bave kreativnim aktivnostima na internetu svake sedmice.

U edukativne svrhe, mnoga djeca i mladi svih uzrasta koriste internet za izradu domaćih zadataka, ili čak da nadoknade gradivo nakon propuštenih predavanja ili potraže zdravstvene informacije na internetu svake sedmice. Čini se da starija djeca imaju veći apetit za informacijama od mlađe djece.

2.3 Uticaj tehnologije na dječije digitalno iskustvo

Internet i digitalna tehnologija mogu pružiti prilike i predstavljati rizike za djecu i mlade. Na primjer, kada djeca koriste društvene medije, imaju koristi od mnogih prilika za istraživanje, učenje, komunikaciju i razvijanje ključnih vještina. Na primjer, djeca društvene mreže vide kao platforme koje im omogućavaju da istražuju lični identitet u sigurnom okruženju. Imati odgovarajuće vještine i znati kako se baviti pitanjima vezanim za privatnost i reputaciju važno je za mlade ljude.

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

Međutim, konsultacije koje pokazuju da većina djece koja koristi društvene medije prije navršenih trinaest godina[11], a usluge provjere godišta su uglavnom slabe ili ih nema, mogu se suočiti sa povećanom mogućnošću od rizika. I dok djeca žele da nauče digitalne vještine i da postanu digitalni građani, posebno vodeći računa o svojoj privatnosti, oni imaju tendenciju da razmišljaju o privatnosti u odnosu na svoje prijatelje i poznanike - „Šta moji prijatelji mogu vidjeti?“ - a manje u odnosu na strance i treće strane. U kombinaciji s dječijom prirodnom znatiželjom i uopšteno sa nižim pragom rizika, to ih može učiniti ranjivima na vrbovanje, iskorištavanje, maltretiranje ili druge vrste štetnog sadržaja ili kontakata.

11 Mreža Contectados al Sur, „Hablatam“; UNICEF, „Global Kids Online uporedni izvještaj (2019).”

Raširena popularnost razmjene slika i video zapisa putem mobilnih aplikacija, a posebno korištenje platformi za strimovanje uživo od strane djece predstavlja daljnju zabrinutost u vezi s privatnošću i rizikom. Neka djeca stvaraju seksualne slike sebe, prijatelja, braće i sestara i dijele ih na internetu. Za neku, posebno stariju djecu, to se može smatrati prirodnim istraživanjem seksualnosti i seksualnog identiteta, dok za drugu, posebno mlađu djecu, često postoji prisila odrasle osobe ili drugog djeteta. Bez obzira na slučaj, rezultujući sadržaj je u mnogim zemljama nezakonit i može izložiti djecu riziku od krivičnog gonjenja ili se može koristiti za daljnje iskorištavanje djeteta.

Slično tome, igre na internetu omogućavaju djeci da ispune svoje osnovno pravo na igru, kao i da grade mreže, provode vrijeme i upoznaju nove prijatelje i razvijaju važne vještine. Ovo uglavnom može biti pozitivno. Međutim, sve je više dokaza koji ukazuju da ukoliko se ostave bez nadzora i podrške odgovorne odrasle osobe, platforme za igranje na internetu mogu takođe predstavljati rizik za djecu, od poremećaja uzrokovanih igrama, finansijskih rizika, prikupljanja i unovčavanja ličnih podataka djece, do sajber maltretiranja, govora mržnje, nasilja, i izlaganja neprimjerenom ponašanju ili sadržaju[12], te vrbovanja uz korištenje stvarnih, kompjuterski generisanih ili čak slika i video zapisa iz virtuelne stvarnosti koji prikazuju i normalizuju seksualno zlostavljanje i iskorištavanje djece.

Nadalje, tehnološki razvoj doveo je do pojave interneta stvari, gdje je sve veći broj i obim uređaja u 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.

2.4 Ključne prijetnje djeci na internetu

Odrasli i djeca su na internetu izloženi nizu rizika i opasnosti. Ipak, djeca su znatno ranjivija populacija. Neka djeca su takođe ranjivija od drugih grupa djece, na primer djeca sa invaliditetom[13] ili djeca koja su u pokretu. Kreatori politika moraju garantovati da se sva djeca mogu razvijati i obrazovati u sigurnom digitalnom okruženju. Ideja da su djeca ranjiva i da ih treba zaštititi od svih oblika eksploatacije izložena je u UN Konvenciji o pravima djeteta.

Nekoliko područja u digitalnom okruženju pružaju velike mogućnosti za djecu, ali istovremeno predstavljaju rizike koji mogu duboko naškoditi djeci i ugroziti njihovu dobrobit. Postoje brige, kako za odrasle, tako i za djecu, da se, na primjer, internet može koristiti za narušavanje privatnosti, širenje dezinformacija ili još gore, za omogućavanje pristupa pornografiji.

Ovdje je presudno razlikovati rizik od štete za djecu. Nije svaka aktivnost koja može nositi elemente rizika opasna i ne postaju svi rizici nužno štetni za djecu, na primjer, seksting (slanje seksi poruka) je način na koji mladi ljudi mogu istraživati seksualnost i veze, a koji nije nužno štetan.

12 UNICEF, “Global Kids Online uporedni izvještaj (2019).” (UNICEF, 2019)
13 Lundy i suradnici, „DVA KLIKA NAPRIJED I JEDAN KLIK NAZAD“, Izvještaj o djeci s invaliditetom u digitalnom okruženju (Savjet Evrope, oktobar 2019.), https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

Slika 2: Klasifikacija prijetnji za djecu na internetu[14]

	SADRŽAJ Dijete u ulozi primaoca poruka masovne proizvodnje	KONTAKT Dijete u ulozi učesnika interakcije koju je inicirala odrasla osoba	PONAŠANJE Dijete u ulozi nasilnika/žrtve
Agresivne	Nasilan sadržaj ili sadržaj sa prikazima krvi	Uznemiravanje, uhođenje	Onlajn vršnjačko nasilje, neprijateljsko ophođenje prema vršnjacima
Seksualne	Pornografski sadržaj	Vrbovanje, seksualno iskorištavanje od strane nepoznate osobe	Seksualno uznemiravanje, "seksting"
Vrijednosne	Sadržaj koji obiluje rasizmom i govorom mržnje	Ubjeđivanje na ideološkoj osnovi	Potencijalno štetan sadržaj generisan od strane korisnika
Komercijalne	Oglašavanje i plasman proizvoda	Prikupljanje i zloupotreba ličnih podataka	Kockanje, povreda autorskih prava

Izvor: EU Kids Online (Livingstone, Haddon, Görzig i Ólafsson (2011))

Dolazak digitalnog doba predstavio je nove izazove u zaštiti djece. Djeca moraju biti osposobljena za sigurnu navigaciju internetskim svijetom i ubiranje njegovih mnogih nagrada.

Kreatori politika moraju osigurati postojanje odgovarajućeg zakonodavstva, zaštitnih mjera i alata koji će omogućiti djeci da se sigurno razvijaju i uče. Ključno je da djeca budu opremljena potrebnim vještinama za prepoznavanje prijetnji i potpuno razumijevanje implikacija i suptilnosti njihovog ponašanja na internetu.

Dok su na internetu, djeca se mogu susresti s mnoštvom prijetnji od organizacija, odraslih i svojih vršnjaka.

Sadržaj i manipulacija

- Izlaganje neprikladnom ili čak kriminalnom sadržaju može dovesti djecu do ekstrema kao što su samopovređivanje, destruktivno i nasilno ponašanje. Izloženost takvom sadržaju može podjednako dovesti do radikalizacije ili pretplate na rasističke ili diskriminatorne ideje. Prepoznato je da se mnoga djeca ne pridržavaju starosnih ograničenja postavljenih na internet stranicama.
- Izloženost netačnim ili nepotpunim informacijama ograničava dječije razumijevanje svijeta oko sebe. Trend prilagođavanja sadržaja na osnovu ponašanja korisnika može dovesti do „filtera mjehura", ograničavajući djecu u razvoju i dosezanju širokog spektra sadržaja.
- Izloženost sadržaju koji se algoritamski filtrira s namjerom manipulacije može u velikoj mjeri uticati na djetetov razvoj, mišljenja, vrijednosti i navike. Izoliranje djece u „eho komore" ili „filtere mjehurove" sprečava ih da pristupe širokom spektru mišljenja i ideja.

14 Livingstone, S., Haddon, L., Görzig, A., i Ólafsson, K. (2011). *Rizici i sigurnost na internetu: Perspektiva Evropske djece.* Potpuni nalazi. LSE, London: EU Kids Online, http://eprints.lse.ac.uk/33731/.

Kontakt sa odraslima ili vršnjacima

Djeca se mogu susresti sa širokim spektrom prijetnji od vršnjaka ili odraslih.

- Maltretiranje na internetu može se širiti više i brže nego izvan interneta. Ono se može dogoditi u bilo koje doba dana i noći, napadajući na taj način ranije 'sigurne prostore', i može biti anonimno.
- Djeca koja su žrtve izvan interneta, vjerovatno će biti žrtve i na internetu. To djecu sa invaliditetom stavlja u veći rizik na internetu, jer istraživanja pokazuju da će djeca sa invaliditetom vjerovatnije doživjeti zlostavljanje bilo koje vrste, a posebno je vjerovatno da će doživjeti seksualnu viktimizaciju. Viktimizacija može uključivati maltretiranje, uznemiravanje, isključenje i diskriminaciju na osnovu stvarne ili zamišljene invalidnosti djeteta ili zbog aspekata povezanih s njegovom invalidnošću, poput načina na koji se ponaša ili govori ili opreme ili usluga koje koristi.
- Kleveta i povreda ugleda: slike i video zapisi mogu se mijenjati i dijeliti milijardama ljudi. Nepromišljeni komentari mogu biti dostupni decenijama i svi ih mogu besplatno pogledati.
- Djeca mogu biti meta napada, vrebanja i zlostavljanja od strane prestupnika putem interneta bilo lokalno ili sa drugog kraja svijeta, koji će se često predstaviti kao neko drugi. To može poprimati nekoliko oblika, uključujući radikalizaciju ili prisiljavanje na slanje seksualno eksplicitnog sadržaja.
- Mogu da budu prisiljena, prevarena ili primorana na kupovinu sa ili bez odobrenja osobe koja plaća račun.
- Neželjeno oglašavanje pokreće pitanja pristanka i prodaje podataka.

Ponašanje djeteta, koje može dovesti do posljedica

- Maltretiranje putem interneta može biti posebno uznemirujuće i štetno jer se može širiti više, s većim nivoom javnosti, a sadržaj koji se širi elektronskim putem može se ponovno pojaviti u bilo kojem trenutku, što žrtvama nasilja može otežati zatvaranje incidenta; može sadržavati štetne vizuelne slike ili uvrjedljive riječi; sadržaj je dostupan 24 sata dnevno; maltretiranje elektronskim putem može se odvijati svaki dan po cijeli dan u toku sedmice, tako da može zadirati u žrtvinu privatnost čak i na inače 'sigurnim' mjestima kao što je njihov dom; i ličnim podacima se može manipulisati, mogu se izmijeniti vizuelne slike i zatim se mogu proslijediti drugima. Štaviše, to se može uraditi anonimno. Otkrivanje ličnih podataka dovodi do rizika od fizičke štete, uključujući susrete u stvarnom životu sa poznanicima sa interneta, uz mogućnost fizičkog i / ili seksualnog zlostavljanja.
- Kršenje vlastitih ili tuđih prava plagijatom i postavljanjem sadržaja bez dozvole, uključujući snimanje i postavljanje neprikladnih fotografija bez dozvole.
- Kršenje tuđih autorskih prava, npr. preuzimanjem muzike, filmova ili TV programa za koje treba platiti, jer to može biti štetno za žrtvu krađe.
- Opsesivna i pretjerana upotreba interneta i / ili igara na internetu na štetu društvenih i / ili aktivnosti na otvorenom važnih za zdravlje, izgradnju povjerenja, socijalni razvoj i opštu dobrobit.
- Pokušaj povrede, uznemiravanja ili maltretiranja nekoga drugog, uključujući i lažno predstavljanje, često se predstavljajući kao drugo dijete.
- Sve češće ponašanje tinejdžera je 'seksting' (dijeljenje seksualizovanih slika ili teksta putem mobilnih telefona). Ove slike i tekst često dijele partneri u vezi ili potencijalni partneri, ali ponekad se dijeljenje završi sa mnogo širom publikom. Smatra se da je malo vjerovatno da mladi tinejdžeri adekvatno razumiju implikacije ovakvog ponašanja i potencijalne rizike koje sa sobom nosi.

2.5 Ključne štete za djecu na internetu

Prethodni odjeljak odnosi se na prijetnje s kojima se djeca mogu susresti na internetu. Ovaj odjeljak ističe štetu koja može nastati od tih prijetnji.

Štete

Prema UNICEF-ovim studijama o upotrebi interneta, sljedeće kategorije se smatraju rizicima i štetama:

- Samozlostavljanje i samopovređivanje:
  - samoubilački sadržaj
  - diskriminacija
- Izloženost neprikladnim materijalima:
  - izlaganje ekstremističkom / nasilnom / krvavom sadržaju
  - ugrađeni marketing
  - kockanje na internetu
- Oko 20% djece koja su anketirana po tom pitanju reklo je da je u proteklih godinu dana vidjelo internet stranice ili internetske rasprave o ljudima koji fizički nanose štetu ili povrjeđuju sebe.
- Radikalizacija:
  - ideološko ubjeđivanje
  - govor mržnje
- Djeca su bila sklonija da prijave da su uznemirena govorom mržnje ili seksualnim sadržajem na internetu, da se tretiraju na štetan način na internetu ili izvan njega ili da se susreću licem u lice s osobom s kojom su se prvo upoznala na internetu.
- Seksualno zlostavljanje i iskorištavanje:
  - samostalno generisani sadržaj
  - Seksualno vrbovanje
  - materijal seksualnog zlostavljanja djece (CSAM)
  - trgovina ljudima
  - seksualno iskorištavanje djece na putovanjima i u turizmu

Studija o djeci iz 2017. godine u Danskoj, Mađarskoj i Velikoj Britaniji otkrila je da je 6% djece imalo vlastite eksplicitne slike podijeljene bez njihovog odobrenja.

U 2019. godini Internet Watch Foundation (IWF) je identifikovala više od 132.000 internet stranica za koje je potvrđeno da sadrže slike i video zapise seksualnog zlostavljanja djece. Svaka internet stranica mogla je da sadrži bilo šta, od jedne do hiljade slika ovog zlostavljanja.

Rizici povezani sa nasiljem na internetu, poput širenja golišavih fotografija bez pristanka i seksualnog sajber maltretiranja, obilježeni su nejednakom rodnom dinamikom, a djevojke su obično više pogođene rodnim pritiscima na seksualno ponašanje, a posljedice su negativnije i uzrokuju štete.

– Kršenje i zloupotreba ličnih podataka:

  • hakovanje
  • prevara i krađa

  Mnogi ljudi su upoznati s prevarama i hakovanjem, ali narušavanje privatnosti u vezi sa djetetovim aktivnostima na internetu smatra se još jednim prekršajem. Odrasli često ugrožavaju mlade pretražujući njihove mobilne telefone i istražujući njihove aktivnosti na internetu, na primjer, izvještaji djece iz Brazila pokazuju da i dječaci i djevojčice, iz različitih starosnih grupa, roditelje doživljavaju tako da više kontrolišu djevojčice kako koriste internet. Pokušaji da se to objasni često sugerišu da su djevojke u nekim slučajevima ranjivije zbog društvenih struktura u kojima žive, posebno s obzirom na njihovu sigurnost, u kontekstu u kojem se granica između interakcije na internetu i izvan njega sve više briše.

– Sajber maltretiranje, vrebanje i uznemiravanje: Neprijateljska i nasilna aktivnost vršnjaka

  Sobe za razgovor i internet stranice društvenih mreža mogu otvoriti vrata nasilju i maltretiranju, jer se anonimni korisnici, uključujući i mlade, uključuju u agresivnu ili nasilnu komunikaciju. U sedam evropskih zemalja - Belgiji, Danskoj, Irskoj, Italiji, Portugalu, Rumuniji i Velikoj Britaniji - Livingstone, Mascheroni, Ólafsson i Haddon[1] otkrili su da je 2010. godine u prosjeku 8% djece bilo žrtva sajber maltretiranja, dok je 2014. godine 12% djece bilo žrtva sajber maltretiranja.

Neophodno je naglasiti da su ranjiva djeca često izložena većem riziku da budu žrtve sajber maltretiranja.

1 Livingstone, S., Mascheroni, G., Ólafsson, K., and Haddon, L., (2014) *Rizici i mogućnosti za djecu na internetu: uporedni nalazi EU Kids Online i Net Children Go Mobile*. London: Londonska škola ekonomije i političkih nauka, www.eukidsonline.net i hYp://www .netchildrengomobile.eu/.

U fokusu: Povećavanje nejednakosti

U 2017. godini oko 60% djece nije bilo na internetu u afričkoj regiji, u poređenju sa samo 4% u Europi. Muških korisnika interneta ima više od ženskih korisnika u svim svjetskim regijama, a korištenje interneta od strane djevojaka često se prati i ograničava. Širenjem širokopojasne mreže za nepovezane dijelove svijeta ta će se nejednakost znatno povećati[15].

Djeca koja se oslanjaju na mobilne telefone, a ne na računare, mogu dobiti samo drugorazredno iskustvo na internetu. Djeca koja govore manjinske jezike često ne mogu pronaći odgovarajući sadržaj na internetu, a djeca iz ruralnih područja vjerovatnije će doživjeti krađu lozinki ili novca.

15 Komisija za širokopojasni pristup, „Sigurnost djece na internetu: Smanjenje rizika od nasilja, zlostavljanja i iskorištavanja na internetu (2019)."

Istraživanja pokazuju da mnogi adolescenti širom svijeta moraju prolaziti kroz značajne prepreke u svom učešću na internetu. Za mnoge, izazovi pristupa - loša povezanost, preveliki troškovi podataka i uređaja i nedostatak odgovarajuće opreme - ostaju ključne prepreke.

Širenjem pristupačne širokopojasne mreže u zemlje u razvoju, pojavljuje se hitna potreba za uspostavljanjem mjera za minimalizaciju rizika i prijetnji ovoj djeci, a da im se istovremeno omogući da iskoriste sve prednosti digitalnog svijeta.

U fokusu: Materijal seksualnog zlostavljanja djece (CSAM)

Razmjere problema

Internet je transformisao obim i prirodu proizvodnje, distribucije i dostupnosti materijala seksualnog zlostavljanja djece. 2018. godine tehnološke kompanije sa sjedištem u Sjedinjenim Američkim Državama prijavile su preko 45 miliona slika i video zapisa na internetu za koje se sumnja da prikazuju djecu koja su seksualno zlostavljana iz cijelog svijeta. Ovo je globalna industrija i razmjera i težina zlostavljanja rastu uprkos naporima da se to zaustavi.

Istorijski gledano, u svijetu bez interneta pronalazak materijala seksualnog zlostavljanja djece zahtijevao je od počinitelja da poduzmu značajne rizike, uz značajane troškove, da bi dobili pristup materijalu. Zahvaljujući internetu, prestupnici sada mogu relativno lako pristupiti ovom materijalu i upustiti se u sve rizičnije ponašanje. Kamere su manje, sve više integrisane u svaki aspekt našeg života, što čini postupak izrade materijala seksualnog zlostavljanja djece i dobijanja sadržaja od nekontaktnog zlostavljanja lakšim nego što je to ikada bilo.

Nemoguće je utvrditi tačnu veličinu ili oblik ove tajne i nezakonite aktivnosti. Međutim, jasno je da se broj nezakonitih slika koje su sada u opticaju može izbrojati u milionima. Skoro svoj djeci koja imaju učešća u slikama kopirana je slika. Internet Watch Foundation je 2018. godine pratila koliko često su se pojavljivale slike djeteta za koje se znalo da je spašeno 2013. godine. Tokom tri mjeseca, analitičari iz Internet Watch Foundation upratili su slike 347 puta - 5 puta svakog radnog dana.

Trenutni pejzaž

Svaki put kad se slika djeteta koje je zlostavljano pojavi i ponovo pojavi na internetu, ili je preuzme prestupnik, to dijete se ponovno zlostavlja. Žrtve su prisiljene živjeti s dugovječnošću i cirkulacijom ovih slika do kraja svog života.

Čim se otkrije materijal koji prikazuje ili internet stranica koja sadrži seksualno zlostavljanje djece, važno je ukloniti ili blokirati sadržaj što je brže moguće. Globalna priroda interneta to otežava: prestupnici mogu proizvoditi materijal u jednoj zemlji, a prikazivati ga u drugoj za potrošače u trećoj. Gotovo je nemoguće donijeti nacionalne naloge ili obavijesti bez sofisticirane međunarodne saradnje.

Tempo inovacija u digitalnom svijetu znači da se prestupnički pejzaž neprestano mijenja. Ključne prijetnje koje su se nedavno pojavile uključuju:

- Porast šifrovanja nehotično omogućava prestupnicima da rade i dijele materijal putem skrivenih kanala, dok u isto vrijeme otkrivanje i sprovođenje zakona čine još većim izazovom.
- Forumi posvećeni vrbovanju djece rastu u zaštićenim uglovima interneta, normalizujući i podstičući ovakvo ponašanje, često zahtijevajući 'novi sadržaj' da bi se dobio pristup.
- Brzo širenje interneta omogućava korisnicima da se povežu na internet u oblastima koja tek trebaju razviti / sprovesti sveobuhvatnu zaštitnu strategiju ili odgovarajuću infrastrukturu.

- Djeca koriste uređaje bez nadzora u mlađoj dobi, a seksualno ponašanje na internetu se normalizuje. Broj slika koje djeca generišu sama, svake godine raste.

U fokusu: Samostalno generisani sadržaj

Djeca i adolescenti mogu snimati kompromitirajuće slike ili video zapise. Iako ovo ponašanje samo po sebi nije nužno nezakonito i može se odvijati kao dio normalnog, zdravog seksualnog razvoja, postoje rizici da se bilo koji takav sadržaj može širiti putem interneta ili izvan njega radi nanošenja štete djeci ili da se koristi kao osnova za iznuđivanje usluga. Iako se neka djeca mogu prisiliti ili prinuditi da dijele seksualne slike, druga (posebno adolescenti) mogu samovoljno proizvoditi seksualni sadržaj. To ne znači da oni pristaju ili da su odgovorni za eksploatacijsku ili nasilnu upotrebu i / ili distribuciju ovih slika.

Seksting je definisan kao „produkcija vlastitih seksualnih slika“[16] ili kao „razmjena seksualnih poruka ili slika“ i „stvaranje, dijeljenje i prosljeđivanje seksualno sugestivnih golih ili golišavih slika putem mobilnih telefona i / ili interneta”[17]. Seksting je oblik generisanog vlastitog seksualno eksplicitnog sadržaja[18], a praksa je „izuzetno raznolika u smislu konteksta, značenja i namjere“[19].

Iako je seksting vjerovatno najčešći oblik generisanog vlastitog seksualno eksplicitnog sadržaja koji uključuje djecu, a često ga prave adolescenti koji pristaju na to iskustvo i koji uživaju u njemu, postoje i mnogi oblici neželjenog sekstinga. To se odnosi na aspekte aktivnosti bez pristanka, poput dijeljenja ili primanja neželjenih seksualno eksplicitnih fotografija, video zapisa ili poruka, na primjer od strane poznatih ili nepoznatih osoba koje pokušavaju uspostaviti kontakt, izvršiti pritisak ili vrbovati dijete. Seksting može biti i oblik seksualnog maltretiranja, kada se na dijete vrši pritisak da pošalje sliku dječku / djevojci / vršnjaku koji je zatim distribuira vršnjačkoj mreži bez njihovog pristanka.

U fokusu: Sajber maltretiranje

Iako maltretiranje kao fenomen daleko prethodi internetu, dodane razmjere, obim i kontinuitet maltretiranja počinjenih na internetu mogu dodatno pogoršati ono što je već uznemirujuće i često štetno iskustvo za njegove žrtve. Sajber maltretiranje definiše se kao namjerna šteta koja se ponavlja nanesena upotrebom računara, mobilnih telefona i drugih elektronskih uređaja. Često se odvija paralelno sa nasiljem izvan interneta koje se odvija u školi ili negdje drugdje, može imati dodatne rasističke, vjerske ili seksističke dimenzije i može predstavljati produženje štete nanesene izvan interneta, poput hakovanja profila, širenja fotografija i video zapisa na internetu i svakodnevne prirode uvredljivih poruka i dostupnosti sadržaja. Uopšteno, to je socijalni problem, a ne problem krivične prirode, koji zahtijeva cjelovit pristup koji uključuje škole, porodice i sto je ključno samu djecu u pravljenju politika za suzbijanje sajber maltretiranja.

---

16 Karen Cooper i dr., „Adolescenti i snimanje vlastitih seksualnih slika: Pregled literature, ”Računari u ljudskom ponašanju 55 (februar 2016.): 706–16, https://doi.org/10.1016/j.chb.2015.10.003.

17 Jessica Ringrose i dr., „Kvalitativna studija o djeci, mladima i 'sekstingu': Izveštaj pripremljen za NSPCC “(London, Velika Britanija: Nacionalno društvo za prevenciju okrutnosti nad djecom, 2012.), http://doi.wiley.com/10.1046/j.1365-2206.1997.00037.x.

18 UNODC, „Studija o efektima novih informacionih tehnologija na zlostavljanje i eksploataciju dece“ (Beč: UN, 2015), https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.[3] UNODC, Studija o efektima novih informacionih tehnologija na zlostavljanje i eksploataciju djece, str.22.

19 Cooper i dr., „Adolescenti i snimanje vlastitih seksualnih slika:”

U fokusu: Vrbovanje na internetu i seksualno iznuđivanje

Sa brzim napretkom tehnologije i povećanim pristupom internetu i digitalnim komunikacijama koje smo iskusili posljednjih godina, neizbježno je uslijedio i povećani rizik od kriminalnih djela na internetu usmjerenih na djecu. Među ovim novim oblicima seksualnog iskorištavanja djece na internetu su vrbovanje putem interneta i seksualno iznuđivanje djece. Vrbovanje putem interneta široko se odnosi na proces odrasle osobe koja se sprijateljila i uticala na dijete (mlađe od 18 godina), korištenjem interneta ili drugih digitalnih tehnologija, radi kontaktne ili nekontaktne seksualne interakcije s tim djetetom. Kroz postupak vrbovanja, prestupnik pokušava postići poštovanje djeteta kako bi održao tajnost i izbjegao otkrivanje i kažnjavanje[20]. Važno je prepoznati da postoje i slučajevi vršnjačkog zlostavljanja.

INTERPOL izvještava da internet olakšava vrbovanje zahvaljujući velikom broju lako dostupnih potencijalnih meta i omogućavajući osobama koje vrbuju djecu da se predstave na način koji je privlačan za dijete. Seksualni prestupnici koriste manipulaciju, prisilu i zavođenje kako bi smanjili otpor i namamili djecu da se bave seksualnom aktivnošću. Osoba koja vrbuje djecu provodi namjerni postupak identifikovanja ranjive potencijalne žrtve, prikupljanja podataka o porodičnoj podršci koje dijete ima i koristi pritisak ili sram / strah za seksualno zlostavljanje djeteta. Osobe koje vrbuju djecu mogu koristiti pornografiju za odrasle i materijale za zlostavljanje ili eksploataciju djece kako bi smanjili otpor svojih potencijalnih meta, predstavljajući dječju seksualnu aktivnost kao prirodnu i normalnu. Internet je promijenio način na koji ljudi komuniciraju i redefinisao je pojam "prijatelja". Osoba koja vrbuje djecu može vrlo lako i brzo uspostaviti prijateljstvo s djetetom na internetu, što nas prisiljava na ponovnu procjenu tradicionalnih obrazovnih poruka o 'opasnim neznancima'.

Vrbovanje na internetu je prvi put formalno priznato u međunarodnom pravnom instrumentu 2007. godine Konvencijom Savjeta Evrope o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja (Lanzarote konvencija). Član 23. kriminalizuje „podsticanje djece u seksualne svrhe“, za šta je potrebno da postoji namjerni prijedlog za upoznavanje djeteta u svrhu počinjenja seksualnog prekršaja, a nakon toga slijede „materijalna djela koja vode takvom sastanku“. U mnogim slučajevima vrbovanja, djeca su seksualno zlostavljana i iskorištavana na internetu - „sastanak“ koji zahtijeva Lanzarote konvencija i mnogi postojeći nacionalni zakoni u potpunosti je virtuelni - ali je, bez obzira na to, jednako štetan za dijete kao i fizički sastanak. Ključno je da se kriminalizacija vrbovanja proširi „na slučajeve kada seksualno zlostavljanje nije rezultat ličnog sastanka, već je počinjeno na internetu“[21].

Seksualno iznuđivanje[22] može se dogoditi kao obilježje vrbovanja na internetu ili kao samostalan prekršaj. Iako se seksualno iznuđivanje može dogoditi i bez postupka vrbovanja na internetu, u nekim slučajevima vrbovanje putem interneta može dovesti do seksualnog iznuđivanja[23]. Seksualno iznuđivanje se može dogoditi u kontekstu vrbovanja na internetu dok osoba koja vrbuje djecu manipuliše i vrši uticaj na dijete tokom postupka vrbovanja putem

20 Međunarodni centar za nestalu i iskorištavanu djecu, „Vrbovanje djece na internetu u seksualne svrhe: Model zakonodavstva i globalna revizija, ”1. izdanje (Međunarodni centar za nestalu i iskorištavanu djecu, 2017.), https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf.

21 Lanzarote komitet, komitet stranaka Konvencije Savjeta Evrope o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja, Podsticanje djece u seksualne svrhe putem informacionih i komunikacionih tehnologija (vrbovanje), mišljenje o članu 23 Lanzarote konvencije i njegova objašnjenja, 17. juna 2015., na *https://edoc.coe.int/en/children-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html* (zadnji put posjećeno 6. novembra 2019.).

22 Nacionalni centar za nestalu i iskorištavanu djecu (NCMEC), Seksualno iznuđivanje, na http://www.missingkids.com/ theissues/onlineexploitation/sextortion (zadnji put posjećeno 6. novembra 2019.).

23 Terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i seksualnog zlostavljanja, Međuagencijska radna grupa za borbu protiv seksualnog iskorištavanja djece, Luksemburg, 28. januara 2016., D.4iii, 27-28, na http://luxembourgguidelines.org/english-version.

prijetnji, zastrašivanja i prisiljavanja na slanje svojih seksualnih slika (pravljenje vlastitog sadržaja)[24]. Ako žrtva odbije da da tražene seksualne usluge, dodatne intimne slike, novac ili druge pogodnosti, njegove ili njene slike mogu biti objavljene na internetu u svrhu prouzrokovanja poniženja ili nevolje ili prisiljavanja djeteta da generiše dodatni seksualno eksplicitni materijal[25].

Seksualno iznuđivanje se naziva „virtuelnim seksualnim napadom“ zbog sličnih emocionalnih i psiholoških učinaka na žrtve[26]. U nekim slučajevima, zlostavljanje je prouzrokovalo tolike traume da su žrtve pokušale da povrijede same sebe ili da izvrše samoubistvo kao način izbjegavanja zlostavljanja.

Europol je primijetio da je prikupljanje informacija za procjenu obima seksualnog iznuđivanja koje pogađa djecu problematično i da je možda jako podcijenjeno[27]. Pored toga, nedostatak zajedničke terminologije i definicija za vrbovanje i seksualno iznuđivanje na internetu prepreke su u prikupljanju tačnih podataka i razumijevanju stvarnog obima problema na globalnom nivou.

2.6 Djeca sa ranjivostima

Djeca i mladi mogu biti ranjivi iz različitih razloga. Istraživanje provedeno 2019. godine izjavilo je da „digitalni životi ranjive djece rijetko dobijaju istu suptilnu i osjetljivu pažnju koju privlače problemi „u stvarnom životu". Nadalje, u izvještaju se dalje kaže da „u najboljem slučaju oni (djeca i mladi) dobijaju iste generičke savjete o sigurnosti na internetu kao i sva druga djeca i mladi, dok je ovdje potrebna intervencija specijaliste“.

Tri su primjera specifičnih ranjivosti: djeca migranti, djeca s poremećajem iz autističnog spektra i djeca s invaliditetom, ali naravno postoje i mnogi drugi.

Djeca migranti

Djeca i mladi migrantskog porijekla često dolaze u jednu zemlju (ili tamo već žive) sa određenim skupom socio-kulturnih iskustava i očekivanja. Iako se obično smatra da je tehnologija posrednik za povezivanje i učestvovanje, rizici i mogućnosti na internetu mogu se uveliko razlikovati u različitim kontekstima. Nadalje, empirijski nalazi i istraživanja pokazuju vitalnu funkciju digitalnih medija uopšte:

- Važni su za orijentaciju (prilikom putovanja u novu zemlju).
- Ona je centralna funkcija za prilagođavanje i upoznavanje sa društvom / kulturom zemlje u kojoj se nalaze.
- Društveni mediji mogu igrati ključnu ulogu u održavanju kontakta s porodicom i vršnjacima i u pristupu opštim informacijama.

24 Terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i seksualnog zlostavljanja, Međuagencijska radna grupa za borbu protiv seksualnog iskorištavanja djece, Luksemburg, 28. januara 2016, D.4iii, 27-28, na http://luxembourgguidelines.org/english-version.

25 Terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i seksualnog zlostavljanja, Međuagencijska radna grupa za borbu protiv seksualnog iskorištavanja djece, Luksemburg, 28. januara 2016, D.4iii, 27-28, na http://luxembourgguidelines.org/english-version.

26 Benjamin Wittes i dr., „Seksualno iznuđivanje: Sajber bezbijednost, tinejdžeri i seksualni napad iz daljine“(Institucija Brookings, 11. maja 2016.), https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.

27 Europol, „Seksualna prisila i iznuda putem interneta kao oblik zločina koji pogađa djecu: Perspektiva organa za sprovođenje zakona “(Evropski centar za borbu protiv sajber kriminala, maj 2017.), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

Uz brojne pozitivne aspekte, digitalni mediji takođe mogu donijeti izazove migrantima, uključujući:

- Infrastrukturu - važno je razmišljati o sigurnim prostorima na internetu kako bi djeca i mladi migranti mogli imati privatnost i sigurnost.
- Resurse - migranti troše većinu novca na pre-paid telefonske kartice.
- Integraciju - pored pristupa tehnologiji, djeca migranti i mladi moraju dobiti i dobro digitalno obrazovanje.

Djeca sa poremećajem iz spektra autizma (PSA)

Spektar autizma rezimira dva osnovna domena u procesu dijagnostike ponašanja DSM-5:

- ograničeno i ponavljajuće ponašanje („potreba za istovjetnošću“);
- poteškoće sa socijalnim i komunikativnim ponašanjem;
- česta istovremena pojava s intelektualnim invaliditetom, jezičkim problemima i slično.

Tehnologija i internet nude beskrajne mogućnosti djeci i mladima kada uče, komuniciraju i igraju se. Međutim, uz ove prednosti postoje i mnogi rizici na koje bi djeca i mladi sa poremećajem iz spektra autizma mogli biti ranjiviji:

- Internet djeci i mladima s autizmom može pružiti mogućnosti za druženje i posebna interesovanja koja možda nemaju izvan interneta.
- Društveni izazovi, poput poteškoća s razumijevanjem tuđih namjera, mogu ovu grupu učiniti ranjivom na "prijatelje" s lošim namjerama.
- Izazovi na internetu često su povezani sa osnovnim karakteristikama autizma: konkretne, specifične smjernice mogle bi poboljšati iskustva pojedinaca na internetu, ali osnovni izazovi ostaju.

Djeca sa invaliditetom

Djeca sa invaliditetom se suočavaju s rizicima na internetu na mnogo istih načina kao i djeca bez invaliditeta, ali mogu se suočiti i sa specifičnim rizicima koji se odnose na njihove invalidnosti. Djeca s invaliditetom često se suočavaju s isključenošću, stigmatizacijom i preprekama (fizičkim, ekonomskim, društvenim i u stavovima) u učešću u svojim zajednicama. Ova iskustva mogu doprinijeti djetetu s invaliditetom koje traži socijalne interakcije i prijateljstva u prostorima na internetu, što može biti pozitivno, izgraditi samopoštovanje i stvoriti mreže podrške. Međutim, može ih i izložiti većem riziku za incidente vrbovanja, podsticanja na internetu i / ili seksualnog uznemiravanja - istraživanje pokazuje da djeca koja imaju poteškoće izvan interneta i ona pogođena psihosocijalnim poteškoćama imaju povećani rizik za takve incidente[28].

Djeca koja su žrtve izvan interneta, vjerovatno će biti žrtve i na internetu. To djecu sa invaliditetom stavlja u veći rizik na internetu, ali imaju i veću potrebu da budu na internetu. Istraživanja pokazuju da će djeca s invaliditetom vjerovatnije doživjeti zlostavljanje bilo koje vrste[29], a posebno je vjerovatno da će doživjeti seksualnu viktimizaciju[30]. Viktimizacija može uključivati maltretiranje, uznemiravanje, isključenje i diskriminaciju na osnovu djetetovog stvarnog ili prividnog invaliditeta ili aspekta povezanih sa njihovom invalidnošću, poput načina

28 Andrew Schrock i dr., „Podsticanje, uznemiravanje i problematičan sadržaj“, Berkmanov centar za internet i društvo, Univerzitet Harvard, decembar 2008., 87, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.‘

29 UNICEF, „Izvještaj o stanju djece u svijetu: Djeca s invaliditetom, ”2013, https://www.unicef.org/publications/files/SOWC2013_Exec_Summary_ENG_Lo_Res_24_Apr_2013.pdf.

30 Katrin Mueller-Johnson, Manuel P. Eisner i Ingrid Obsuth, „Seksualna viktimizacija mladih s fizičkim invaliditetom: Ispitivanje stopa rasprostranjenosti, rizika i zaštitnih faktora, ”Časopis za međuljudsko nasilje 29, br. 17. (novembar 2014.): 3180–3206, https://doi.org/10.1177/0886260514534529.

na koji se ponašaju ili govore, opreme ili usluga koje koriste.

Počinioci vrbovanja, podsticanja putem interneta i / ili seksualnog uznemiravanja djece sa invaliditetom mogu biti ne samo počinioci koji ciljaju djecu, već i oni koji ciljaju djecu sa invaliditetom. Takvi počinioci mogu biti „privrženik“ - osobe koje nemaju invaliditet a koje seksualno privlače osobe s invaliditetom (najčešće osobe sa amputacijama i osobe koje koriste pomagala u kretanju), a od kojih se neki i sami pretvaraju da imaju invaliditet[31]. Radnje takvih ljudi mogu uključivati preuzimanje fotografija i videozapisa djece s invaliditetom (koje su neškodljive prirode) i / ili njihovo dijeljenje putem namjenskih foruma ili profila na društvenim mrežama. Alati za prijavljivanje na forumima i društvenim mrežama često nemaju ciljani ili odgovarajući put za rješavanje takvih radnji.

Postoje zabrinutosti da „roditeljsko dijeljenje“ (roditelji koji dijele informacije i fotografije svoje djece na internetu) može narušiti djetetovu privatnost, dovesti do maltretiranja, izazvati sramotu ili imati negativne posljedice kasnije u životu[32]. Roditelji djece sa invaliditetom mogu dijeliti takve informacije u potrazi za podrškom ili savjetom, stavljajući djecu sa invaliditetom u veći rizik od štetnih ishoda.

Pojedina djeca 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 sa ekrana ili prilagodljivih računarskih kontrola), ili potreba za odgovarajućom podrškom (npr. podučavanje kako se koristi oprema, podrška jedan na jedan za navigaciju u društvenim interakcijama[33]).

U vezi sa rizikom od ugovora ili potpisivanja uslova i pravila, djeca s invaliditetom su u većem riziku da prihvate zakonske odredbe koje ponekad ni odrasli ne mogu razumjeti.

2.7 Dječija percepcija rizika na internetu

Izloženost nasilju širom svijeta, pristup neprikladnom sadržaju, robi i uslugama; zabrinutost zbog prekomjerne upotrebe; pitanja zaštite podataka i privatnosti su oni rizici koje su djeca istakla[34].

Adolescenti iznose niz zabrinutosti u vezi sa njihovim angažmanom u digitalnim tehnologijama. Ovdje se često uključuju pomenute brige o sigurnosti na internetu, poput straha od interakcije sa strancima na internetu, pristupa neprimjerenom sadržaju ili izloženosti zlonamjernom softveru ili virusima - dok se druge odnose na pouzdanost njihovog pristupa tehnologiji; upad roditelja u njihov 'privatni' život na internetu; i njihove vještine digitalne pismenosti[35].

31 Richard L Bruno, „Privrženici, glumci i ljudi koji to žele biti: Dva slučaja poremećaja vještačke invalidnosti, ”Seksualno i invaliditet 15, br. 4 (1997): 18, https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf.

32 UNICEF, „Privatnost djece u doba Web 2.0 i 3.0: Izazovi i mogućnosti za politiku, ”Innocenti rad o diskusiji 2017-03 (UNICEF, Kancelarija za istraživanje-Innocenti), pristupljeno 16. januara 2020, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf.

33 Za smjernice o ovim pravima, vidi član 9 Konvencije o pravima osoba s invaliditetom o pristupačnosti i član 21 o slobodi izražavanja i mišljenja i pristupu informacijama.

34 Amanda Third i drugi, „Dečija prava u digitalno doba“ (Melburn: kooperativni istraživački centar Young and Well, septembar 2014.), http://www.uws.edu.au/_data/assets/pdf_file/0003/753447/Childrens-rights-in-the-digital-age.pdf.

35 Amanda Third i dr., „Mladi i na internetu: Dječije perspektive života u digitalno doba, “Prateći izvještaj o stanju djece u svijetu 2017. (Sydney: Univerzitet u Zapadnom Sidneju, 2017). Izvještaj je sažeo stavove 490 djece uzrasta od 10 do 18 godina iz 26 različitih zemalja koja govore 24 službena jezika.

Istraživanje EU Kids Online pokazuje da se djeca na internetu u Evropi najviše brinu zbog pornografije i nasilnih sadržaja. Sve u svemu, dječacima više smeta nasilje, dok se djevojčice više brinu zbog rizika povezanih s kontaktima[36]. Zabrinutost zbog rizika veća je među djecom iz zemalja s „visokom upotrebom i visokim rizikom".

U Latinskoj Americi dječije konsultacije su pokazale da su gubitak privatnosti, nasilje i uznemiravanje glavna briga[37]. Djeca prijavljuju da ih kontaktiraju ljudi koje ne poznaju - to je posebno slučaj kada igraju igre na internetu. U takvim situacijama čini se da je glavna strategija ignorisanje i / ili blokiranje takve osobe. Djevojčice se od malih nogu na društvenim mrežama suočavaju sa uznemiravanjem. Uspijevaju se same izboriti sa ovim oblicima nasilja, blokirajući korisnike i mijenjajući podešavanja privatnosti. Uznemiravanje dolazi od korisnika koji ponekad ne govore španski, ali uspijevaju im poslati slike, zatražiti prijateljstvo i komentarisati njihove objave. Neki dječaci takođe prijavljuju da su primili takve zahtjeve.

U mnogim dijelovima svijeta djeca dobro razumiju neke od rizika s kojima se suočavaju na internetu[38]. Istraživanje je pokazalo da većina djece može razlikovati sajber maltretiranje od šale ili zadirkivanja na internetu, prepoznajući da sajber maltretiranje ima javnu dimenziju i da je stvoreno da nanese štetu[39].

36 Livingstone, S. (2014) *EU Kids Online: Otkrića, metode, preporuke.* LSE, London: EU Kids Online, https://lsedesignunit.com/EUKidsOnline/.

37 Contectados al Sur mreža, "Hablatam."

38 Od 2016. ITU provodi konsultacije sa djecom i odraslim interesnim stranama u okviru zaštite djece na internetu o važnim pitanjima kao što su sajber maltretiranje, digitalna pismenost i dječije aktivnosti na internetu.

39 UNICEF, "Global Kids Online uporedni izvještaj (2019)."

3. Priprema za nacionalnu strategiju zaštite djece na internetu

U procesu razvoja nacionalne strategije zaštite djece na internetu za promociju sigurnosti djece i mladih na internetu, nacionalne vlade i institucije koje donose politike trebaju identifikovati najbolju praksu i stupiti u kontakt s ključnim interesnim stranama.

Sljedeći odjeljci ističu tipične aktere i interesne strane, zajedno s prikazom njihove potencijalne uloge i odgovornosti u pogledu zaštite djece na internetu.

3.1 Akteri i interesne strane

Kreatori politika mogu identifikovati odgovarajuće pojedince, grupe i organizacije koji predstavljaju svakog od ovih aktera i interesnih strana u njihovoj nadležnosti. Uvažavanje svake od njihovih trenutnih, planiranih i potencijalnih aktivnosti važno je u bilo kojoj nacionalnoj koordinaciji i orkestraciji strategija zaštite djece na internetu.

Djeca i mladi

Djeca i mladi širom svijeta pokazali su da se s velikom lakoćom mogu prilagoditi i koristiti nove tehnologije. Internet postaje sve važniji u školama i kao arena u kojoj djeca mogu raditi, igrati se i komunicirati.

Prema najnovijem izvještaju ChildFund saveza, samo 18.1% intervjuisane djece misli da ljudi koji upravljaju djeluju kako bi ih zaštitili. Važno je da se kreatori politika angažuju oko djece u vezi s tim, prepoznajući njihovo pravo da budu saslušani (čl. 12. Konvencije o pravima građana).

Da bi mogli zaštititi djecu, kreatori politika trebaju standardizovati definiciju djeteta u svim pravnim dokumentima. Dijete treba biti definisano kao svaka osoba mlađa od 18 godina. To je u skladu s članom 1. UN Konvencije o pravima djeteta (UNCRC), koji kaže da „dijete podrazumijeva svako ljudsko biće mlađe od 18 godina“. Kompanijama se ne smije dopustiti da se prema osobama mlađim od 18 godina ali koje zakonski imaju dovoljno godina da pristanu na obradu podataka, ponašaju kao prema odraslima. Ova uska definicija nije opravdana nijednim dokazom o prekretnicama u razvoju tokom djetinjstva. Narušava prava i ugrožava sigurnost djece.

Iako se mnoga djeca mogu činiti sigurnom u korištenju tehnologije, mnoga se osjećaju nesigurno[40] na internetu i imaju nekoliko nedoumica[41] u vezi s internetom.

Nedostatak iskustva djece i mladih u širem svijetu može ih učiniti ranjivima na niz rizika. Ona imaju pravo očekivati pomoć i zaštitu. Takođe je važno zapamtiti da neće sva djeca i mladi doživjeti internet ili nove tehnologije na isti način. Neka od djece sa posebnim potrebama prouzrokovanim fizičkim ili drugim invaliditetom mogu biti posebno ranjiva u okruženju na internetu i trebaće im dodatna podrška.

Ankete su više puta pokazale da ono što odrasli misle da djeca i mladi rade na internetu i šta se zapravo dešava može biti vrlo različito. Polovina sve anketirane djece je rekla da odrasli u

40 ChildFund savez, “NASILJE NAD DJECOM KAKO GA DJECA OBJAŠNJAVAJU,” Mali glasovi veliki snovi, 2019, https://childfundalliance.org/zdocs/a9357061-749f-4ebf-a1e9-b1aee81cb216/SVBD-THE_REPORT-digital.pdf.

41 Savjet Evrope, “To je naš svijet: Dječji pogledi na to kako treba da zaštite svoja prava u digitalnom svijetu,” Izvještaj o dječijim konsultacijama (Savjet Evrope, Odjeljenje za prava djece, oktobar 2017.), https://rm.coe.int/it-s-our-world-children-s-views-on-how-to-protect-their-rights-in-the-/1680765dff.

njihovoj zemlji ne slušaju njihovo mišljenje o pitanjima koja su im važna[42]. Iz tog razloga, važno je osigurati, bez obzira na bilo kakve aranžmane na nacionalnom nivou za razvijanje politike u ovoj oblasti, da se pronađu odgovarajući mehanizmi koji omogućavaju da se čuju glasovi sve djece i mladih i da se njihova konkretna iskustva korištenja tehnologija uzmu u obzir.

Roditelji, staratelji i vaspitači

Roditelji, staratelji i vaspitači najviše vremena provode sa djecom. Oni bi se trebali obrazovati u digitalnoj pismenosti da razumiju okruženje na internetu i da budu u stanju da zaštite djecu i da ih nauče kako da se sami zaštite.

Obrazovne institucije imaju posebnu odgovornost da podučavaju djecu o tome kako biti sigurniji na internetu, bez obzira koriste li internet u školi, kod kuće ili bilo gdje drugdje, a kreatori politika trebaju u nacionalne planove i programe uključiti digitalnu pismenost od najranijeg uzrasta (od 3 do 18 godina). To bi djeci omogućilo da se mogu zaštititi, znati svoja prava i, prema tome, koristiti internet kao mogućnost sticanja znanja[43].

Kreatori politika bi trebalo da imaju na umu da će roditelji i staratelji skoro uvijek biti prva, posljednja i najbolja linija odbrane i podrške vlastitoj djeci. Ipak, što se tiče interneta, mogli bi se osjećati pomalo izgubljeno. Opet, škole mogu da djeluju kao važan kanal za kontaktiranje roditelja i staratelja, kako bi ih upoznali s rizicima i mnogim pozitivnim mogućnostima koje predstavljaju nove tehnologije. Međutim, škole ne bi trebale biti jedini način na koji se kontaktiraju roditelji i staratelji. Važno je koristiti mnogo različitih kanala kako bi se povećala mogućnost kontaktiranja što većeg broja roditelja i staratelja. Ovdje industrija ima značajnu ulogu u pružanju podrške svojim korisnicima ili kupcima. Roditelji i staratelji mogu odlučiti da upravljaju djetetovim aktivnostima i pristupom internetu, da razgovaraju s djetetom o pravilnom ponašanju i korištenju tehnologija, da razumiju šta dijete radi na internetu, tako da porodični razgovor objedinjuje iskustva na internetu i izvan interneta kao jedno.

Roditelji i staratelji takođe trebaju biti dobar primjer svojoj djeci kako da koriste svoje uređaje i ponašaju se na odgovarajući način na internetu.

Kreatori politika trebaju imati na umu da se roditelji i staratelji trebaju konsultovati kako bi dobili njihova mišljenja, iskustva i razumijevanje o zaštiti njihove djece na internetu.

Na kraju, kreatori politika zajedno sa drugim javnim institucijama mogu razviti kampanje za podizanje svijesti javnosti, uključujući roditelje, staratelje i nastavnike. Javne biblioteke, domovi zdravlja, čak i tržni centri i drugi veći maloprodajni centri mogu pružiti pristupačna mjesta za prezentaciju informacija o sigurnosti na internetu i digitalnim vještinama. Prilikom implementacije ovog zadatka, vlade bi trebale osigurati neutralnost u datim savjetima, bez ikakvih privatnih interesa, i pokrivati širok spektar pitanja u digitalnom prostoru.

Industrija

Industrija je jedna od ključnih interesnih strana u ekosistemu jer taj sektor posjeduje tehnološko znanje koje kreatori politika trebaju za rješavanje i razumijevanje problema kako bi razvili pravni okvir. Stoga je od suštinske važnosti da donosioci politika uključe industriju u proces razrade zakona o zaštiti djece na internetu.

42 ChildFund savez, “Nasilje nad djecom kako ga djeca objašnjavaju.”

43 UNICEF, “Vodič kroz politike o djeci i digitalnoj povezanosti” (laboratorija za politike, podaci, istraživanje i politika, Dječiji fond Ujedinjenih nacija, juni 2018.), https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf.

Takođe, važno je podstaći industriju da u svoje poslovanje ugradi sigurnosni pristup već u samom dizajnu prilikom razvoja nove tehnologije. Jasno je da bi kompanije koje razvijaju ili pružaju nove tehnološke proizvode i usluge trebale pomoći svojim korisnicima da shvate kako oni rade i kako ih sigurno i na odgovarajući način koristiti.

Industrija takođe ima veliku odgovornost da pomogne u promovisanju svijesti o internetu i sigurnosti, posebno djeci i njihovim roditeljima ili starateljima, ali i široj zajednici. Uključujući se na ovaj način, interesne strane u industriji saznaće više o brigama ostalih interesnih strana te rizicima i štetama kojima su krajnji korisnici izloženi. Sa tim znanjem, industrija bi mogla popraviti postojeće proizvode i usluge i prepoznati opasnosti u toku razvoja.

Nedavni napredak u vještačkoj inteligenciji otvara put industriji da izgradi mnogo jače kontrole i ravnoteže kako bi identifikovala korisnika i djeci pružila podsticajnu sredinu za pozitivno ponašanje na internetu. Ova dostignuća takođe mogu predstavljati nove rizike za djecu.

U nekim zemljama internetom se upravlja u okviru samoregulacije ili koregulacije. Međutim, neke zemlje razmatraju ili su implementirale zakonske i regulatorne okvire, uključujući obaveze za kompanije da otkriju, blokiraju i / ili uklone štetne sadržaje za djecu sa platformi ili usluga, kao i da pruže jasne puteve prijavljivanja i pristup podršci.

Istraživačka zajednica i nevladine organizacije

Unutar univerziteta i istraživačke zajednice vrlo je vjerovatno da će biti niz akademika i naučnika koji imaju profesionalni interes i vrlo detaljno znanje o socijalnim i tehničkim uticajima interneta. Oni su vrlo vrijedan resurs u smislu pomoći nacionalnim vladama i kreatorima politika da razviju strategije koje se zasnivaju na čvrstim činjenicama i dobrim dokazima. Oni takođe mogu djelovati kao intelektualna protivteža poslovnim interesima koji ponekad mogu biti previše kratkoročni i komercijalni.

Isto tako, unutar zajednice nevladinih organizacija (NVO) postoji čitav niz stručnjaka i informacija koji mogu biti neprocjenjiv resurs u pružanju usluga djeci, roditeljima, njegovateljima i edukatorima koji pomažu u promociji sigurnosti na internetu i uopšteno, u branjenju javnog interesa.

Organi za sprovođenje zakona

Žalosna je činjenica da je, koliko god tehnologija bila divna, privukla i pažnju kriminalnih i antisocijalnih elemenata. Internet je znatno povećao cirkulaciju materijala seksualnog zlostavljanja djece i drugih šteta na internetu. Seksualni predatori koristili su internet kako bi uspostavili početni kontakt s djecom, uvlačeći ih u vrlo štetne oblike kontakata, na internetu i izvan njega. Maltretiranje i drugi oblici uznemiravanja mogu mnogo naštetiti dječijim životima, a internet je pružio novi način da se to dogodi.

Iz ovih razloga, neophodno je da se zajednica za sprovođenje zakona potpuno angažuje sa bilo kakvom sveobuhvatnom strategijom koja će pomoći da internet bude sigurniji za djecu i mlade. Službenici za sprovođenje zakona trebaju proći odgovarajuću obuku za vođenje istraga o zločinima nad djecom i mladima povezanih s internetom. Potreban im je odgovarajući nivo tehničkog znanja i pristup forenzičkim ustanovama kako bi im se omogućilo da u najkraćem mogućem roku izvuku i protumače podatke dobijene sa računara ili interneta.

Uz to, vrlo je važno da organi za sprovođenje zakona uspostave jasne mehanizme koji će omogućiti djeci i mladima ili bilo kojem članu javnosti da prijave bilo kakve incidente ili nedoumice koje bi mogle biti u vezi sa sigurnošću djeteta ili mlade osobe na internetu. Mnoge zemlje su, na primjer, uspostavile dežurne telefonske linije da bi olakšale prijavljivanje materijala seksualnog zlostavljanja djece, a slični namjenski mehanizmi postoje da bi olakšali prijavljivanje drugih vrsta problema, na primjer, maltretiranje. Kreatori politika bi trebali sarađivati s Međunarodnim udruženjem internetskih dežurnih linija (INHOPE), pružajući im podršku u procjeni i obradi prijava materijala seksualnog zlostavljanja djece i da imaju koristi od toga što INHOPE pomaže organizacijama širom svijeta u uspostavljanju dežurnih telefonskih linija gdje ih nema. Kreatori politika trebaju osigurati da postoje otvoreni kanali komunikacije između organa za sprovođenje zakona i drugih interesnih strana. Organi za sprovođenje zakona su primarni izvor zaplijenjenog materijala seksualnog zlostavljanja djece unutar nacionalnih granica. Treba uspostaviti postupak ispitivanja ovog materijala kako bi se utvrdilo mogu li se identifikovati lokalne žrtve. Tamo gdje to nije moguće, materijal treba proslijediti INTERPOL-u radi uvrštavanja u ICSE bazu podataka. Pošto je to globalna prijetnja, kreatori politika moraju da obezbijede međunarodnu saradnju između agencija za sprovođenje zakona širom svijeta. To bi smanjilo vrijeme formalnih procesa i omogućilo bi agentima da brže reaguju.

Socijalne usluge

Tamo gdje su djeca ili mladi oštećeni ili zlostavljani na internetu, na primjer, postavljanjem njihove neprimjerene ili nezakonite slike, vjerovatno će im trebati specijalizovana i dugoročna podrška ili savjetovanje. Takođe može postojati potreba za premoštavanjem usluga i restorativnih postupaka za prestupnike, posebno za mlade prestupnike koji su takođe možda bili žrtve zlostavljanja na internetu ili izvan njega. Profesionalci koji rade u socijalnim službama moraće proći odgovarajuću obuku da bi mogli pružiti ovu vrstu podrške. Podršku treba pružiti putem kanala na internetu i izvan interneta.

Zdravstvene usluge

Zdravstvena usluga potrebna nakon svakog slučaja nasilja nad djetetom trebala bi biti obuhvaćena osnovnim planom zdravstvene zaštite na nacionalnom nivou. Zdravstvene ustanove trebale bi obavezno da prijave zlostavljanja. Zdravstveni radnici trebaju biti odgovarajuće opremljeni i obrazovani kako bi mogli pružiti podršku djeci u tom pogledu. Usluge zdravstvene zaštite trebale bi se proširiti tako da uključuju podršku za mentalno zdravlje i dobrobit djece.

Vladina ministarstva

Politika zaštite djece na internetu će spadati u nadležnost niza vladinih ministarstava i važno ih je uključiti u bilo koju uspješnu nacionalnu strategiju i akcioni plan. Ona mogu uključivati:

- Unutrašnje poslove
- Zdravstvo
- Obrazovanje
- Pravdu
- Digitalne / informacije
- Regulatorna tijela

Regulatorna tijela su u najboljem položaju da doprinesu ulozi kontrolora i računovođe u saradnji sa vladinim institucijama. Ovo može da uključuje regulatorna tijela za zaštitu medija i podataka

Širokopojasni, mobilni i bežični mrežni operateri

Operateri mogu otkriti, blokirati i prijaviti nezakonit sadržaj u svojoj mreži i pružiti porodične alate, usluge i konfiguracije koje roditelji mogu koristiti u izboru načina upravljanja pristupom njihove djece. Važno je da provajderi jednako osiguraju poštovanje građanskih sloboda i privatnosti.

Dečija prava

Nezavisne institucije za ljudska prava za djecu mogu igrati presudnu ulogu u osiguravanju zaštite djece na internetu. Iako se njihovi mandati razlikuju, takve institucije često imaju funkcije da:

- nadgledaju uticaj zakona, politike i prakse na zaštitu dječijih prava;
- promovišu primjenu međunarodnih standarda ljudskih prava na nacionalnom nivou;
- istražuju kršenja prava djece;
- pružaju sudovima ekspertizu o pravima djece;
- osiguravaju da se stavovi djece o pitanjima koja se tiču njihovih ljudskih prava čuju, uključujući razvoj relevantnog zakona i politike;
- promovišu razumijevanje i svijest javnosti o dječjim pravima; i
- preduzimaju inicijative za obrazovanje i obuku o ljudskim pravima.

Važno je uključiti direktno savjetovanje sa djecom, kao što je i njihovo pravo prema članu 12. UNCRC-a. Savjetodavne, istražne, funkcije za podizanje svijesti i obrazovne funkcije nezavisnih institucija za ljudska prava za djecu bitne su za sprečavanje i reagovanje na štetu koju djeca mogu doživjeti na internetu. Zato bi takve institucije trebale biti u srcu razvoja sveobuhvatnog pristupa zasnovanog na pravima za jačanje pravnih, regulatornih i političkih okvira koji regulišu zaštitu djece na internetu, uključujući direktne konsultacije s djecom, kao što je i njihovo pravo iz čl. 12 UNCRC.

U novije vrijeme bilo je i primjera da jurisdikcije uvode ili razmatraju uvođenje državnih agencija sa određenim mandatom da podržavaju prava djeteta na internetu, uključujući njihovu zaštitu od nasilja ili štete. Tamo gdje takve agencije postoje, one bi takođe trebale biti usko povezane s naporima da se ojača odgovor na zaštitu djece na internetu na nacionalnom nivou.

3.2 Postojeći odgovori za zaštitu djece na internetu

Razvijeno je nekoliko inicijativa kako bi se djelovalo na nacionalnom i međunarodnom nivou suočavajući se sa sve većim značajem IKT-a u životima djece širom svijeta i inherentnim rizicima za najmlađe u našim društvima.

Nacionalni modeli

Na nacionalnom nivou, treba naglasiti nekoliko zakona koji pokrivaju važne aspekte sveobuhvatnog okvira za zaštitu djece na internetu. Oni uključuju, ali se ne ograničavaju na:

- Direktivu o audiovizuelnim medijskim uslugama (AVMSD) (revidirano 2018., EU)
- Opšta uredba o zaštiti podataka (GDPR) (2018, EU)

Došlo je do inovativnog razvoja u regulatornom i institucionalnom odgovoru država članica na prijetnje sigurnosti i dobrobiti djece na internetu. Ne postoji jedinstveni način da se odgovori na materijal seksualnog zlostavljanja djece, sajber maltretiranje i druge štete na koje djeca nailaze na internetu, ali primjetno je da je u posljednjih nekoliko godina bilo novih pristupa:

Kodeks dizajna prilagođen uzrastu (2019, Velika Britanija)

Početkom 2019. godine Kancelarija povjerenika za informacije objavila je prijedloge za svoj „Kodeks za dizajniranje prilagođeno uzrastu“ radi unaprjeđenja zaštite djece na internetu. Predloženi Kodeks se fokusirao na najbolje interese za djecu, kako je izloženo u UNCRC, i u njemu je iznijeto nekoliko očekivanja za industriju. Ona uključuju jake mjere provjere starosti, usluge određivanja lokacije za djecu isključene u početnim podešavanjima, industrija da prikuplja i zadržava samo minimalnu količinu ličnih podataka djece, da proizvodi budu sigurni po samom dizajnu i da objašnjenja odgovaraju uzrastu i da su dostupna.

Zakon o štetnim digitalnim komunikacijama (revidiran 2017., Novi Zeland)

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

Povjerenik eSafety (2015, Australija)

Povjerenik eSafety je prva vladina agencija na svijetu koja se posebno bavi sigurnošću na internetu. Osnovana 2015. godine, eSafety ima zakonsku ulogu da vodi, koordiniše, obrazuje i savjetuje o pitanjima sigurnosti na internetu kako bi osigurala da svi Australci imaju sigurna i pozitivna iskustva na internetu, puna mogućnosti. eSafety upravlja istražnim programima koji se fokusiraju na čitav niz šteta, uključujući ozbiljno sajber maltretiranje djece, zlostavljanje zasnovano na slikama i zabranjeni sadržaj. Ovlaštena je da istražuje i poduzima mjere radi rješavanja žalbi ili prijava koje uključuju ovakve vrste šteta - uključujući, u nekim slučajevima, ovlaštenje za izdavanje upozorenja pojedincima i pružaocima usluga na internetu za uklanjanje materijala. Uz svoja istražna ovlaštenja, eSafety usvaja čitav pristup zajednice koji se oslanja na socijalne, kulturne i tehnološke inicijative i intervencije. Njeni preventivni, zaštitni i proaktivni napori pružaju sveobuhvatan pristup sigurnosti na internetu.

Međunarodni modeli

Na međunarodnom i transnacionalnom nivou različite interesne strane su izdale preporuke i standarde. Ove smjernice se nadovezuju na rad na osnovu sljedećeg:

Smjernice u vezi sa primjenom Fakultativnog protokola uz Konvenciju o pravima djeteta koji se odnosi na prodaju djece, dječiju prostituciju i dječiju pornografiju.

Smjernice Savjeta Evrope za poštovanje, zaštitu i ispunjavanje prava djeteta u digitalnom okruženju[44].

44 Savjet Evrope (2020), Digitalno okruženje,https://www.coe.int/en/web/children/the-digital-environment. Smjernice Savjeta Evrope za poštovanje, zaštitu i ispunjavanje prava djeteta u digitalnom okruženju prvi su takav set standarda koje je usvojilo međuvladino tijelo (CM / Rec, 2018).

Smjernice su upućene svim državama članicama Savjeta Evrope, u svrhu pomoći državama članicama i drugim relevantnim interesnim stranama u njihovim naporima da usvoje sveobuhvatan, strateški pristup maksimalno poštujući u cijelom obimu čitav spektar dječijih prava u digitalnom okruženju. Među mogim pokrivenim temama su zaštita ličnih podataka, pružanje sadržaja za djecu prilagođenog njihovim razvojnim kapacitetima, linije za pomoć i dežurne telefonske linije, ranjivost i otpornost, kao i uloga i odgovornosti poslovnih preduzeća. Pored toga, smjernice pozivaju države da uključe mišljenja djece u svoj rad, uključujući i u procese donošenja odluka, kako bi osigurale da se nacionalne politike na odgovarajući način bave razvojem u digitalnom okruženju. Smjernice su trenutno dostupne na 19 jezika. Pratit će ih verzija dokumenta prilagođena djeci, kao i Priručnik za kreatore politika, koji će pružiti konkretne mjere o načinu primjene smjernica.

Savjet Evrope - Lanzarote konvencija

Konvencija Savjeta Evrope o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja (Lanzarote konvencija), koja zahtijeva od država da pruže cjelovit odgovor na seksualno nasilje nad djecom, putem „pristupa 4P“: prevencija (Prevention), zaštita (Protection), krivično gonjenje (Prosecution) i promocija (Promotion) nacionalne i međunarodne saradnje. Funkcionisanje Konvencije u vezi sa digitalnim okruženjem pojasnio je Komitet strana potpisnica Konvencije o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja ("Lanzarote komitet"), usvajanjem niza dokumenata. To su: Mišljenje o dječijim seksualno sugestivnim ili eksplicitnim slikama i / ili video zapisima koje generišu, dijele i primaju djeca (6. juna 2019.); Interpretativno mišljenje o primjenjivosti Lanzarote konvencije na seksualna kaznena djela nad djecom potpomognuta korištenjem IKT-a (12. maj 2017.); Deklaracija o internet adresama koje oglašavaju materijale ili slike seksualnog zlostavljanja djece ili bilo koja druga krivična djela utvrđena u skladu sa Lanzarote konvencijom (16. juna 2016.); i Mišljenje o članu 23. Lanzarote konvencije - Podsticanje djece u seksualne svrhe putem informacionih i komunikacionih tehnologija (Vrbovanje). Lanzarote komitet sprovodi nadzor nad sprovođenjem Konvencije: njegov drugi tematski nadzorni krug komiteta usredsređen je na zaštitu djece od seksualnog iskorištavanja i seksualnog zlostavljanja korištenjem IKT-a: izvještaj će biti objavljen u nadzornom krugu 2020. godine. Od 2019. godine postoji 46 država potpisnica Konvencije, uključujući Tunis - prvu državu koja nije članica, a koja se pridružila.

Dalje smjernice Savjeta Evrope

Dalji standardi i alati Savjeta Evrope doprinose kolektivnoj pravnoj tekovini za sveobuhvatan okvir usmjeren na sve interesne strane. Konvencija o sajber kriminalu Savjeta Europe sadrži obaveze država potpisnica da kriminalizuju niz krivičnih djela povezanih sa materijalom seksualnog zlostavljanja djece: trenutno je ratifikovana od strane 64 države. Savjet Evrope fokusira se, između ostalog, na pružanju mogućnosti djeci i onima u njihovoj blizini da se sigurno kreću digitalnom sferom. Ovo se promoviše putem obrazovnih alata, uključujući potpuno revidirani Priručnik za pismenost na internetu (2017), Priručnik za obrazovanje o digitalnom građanstvu (2019) i priručnike namijenjene roditeljima (Roditeljstvo u digitalnom dobu - Smjernice za roditelje za zaštitu djece od seksualnog iskorištavanja i seksualnog zlostavljanja na internetu (2017); Digitalno državljanstvo ... i vaše dijete - Šta svaki roditelj treba da zna i da radi (2019). Najzad, Savjet Evrope je preduzeo konsultativno istraživanje sa decom u vezi sa njihovim pravima u digitalnom okruženju - To je naš svijet: Dječiji pogledi na to kako da zaštite svoja prava u digitalnom okruženju (2017.) i sproveo neka od prvih konsultativnih istraživanja usredsređenih na iskustva djece s invaliditetom u digitalnom okruženju - Dva klika naprijed i jedan natrag: Izvještaj o djeci sa invaliditetom u digitalnom okruženju (2019).

Izvještaj o sigurnosti djece na internetu

Sigurnost djece na internetu: Smanjenje rizika od nasilja, zlostavljanja i eksploatacije na internetu + Univerzalna deklaracija[45] o sigurnosti djece na internetu.

Preporuke OECD-a o zaštiti djece na internetu (2012 / Pregled 2019-2020) Ostale nacionalne i transnacionalne inicijative treba dalje istaći kao podršku međunarodnoj saradnji, kao i nacionalnim naporima da se uspostave strategije zaštite djece na internetu. To su na primjer:

Međunarodna baza podataka o seksualnom iskorištavanju djece

Pod upravom INTERPOL-a, međunarodna baza podataka o seksualnom iskorištavanju djece (ICSE DB) moćno je obavještajno i istražno sredstvo koje omogućava specijalizovanim istražiteljima da dijele podatke sa kolegama širom svijeta. Dostupna putem INTERPOL-ovog sigurnog globalnog policijskog komunikacionog sistema (poznatog kao I-247), ICSE DB koristi sofisticirani softver za upoređivanje slika da bi uspostavila veze između žrtava, nasilnika i mjesta. ICSE DB omogućava sertifikovanim korisnicima u zemljama članicama pristup bazi podataka u stvarnom vremenu - istraživanje postojećeg fonda, učitavanje novih podataka, trijažu i sortiranje materijala, uklanjanje konfliktnog materijala, analiziranje i komunikaciju s drugim stručnjacima širom svijeta kao odgovor na upite u vezi sa istragama o seksualnom iskorištavanju djece.

Globalni savez WeProtect

Globalni savez WePROTECT (WPGA) je globalni pokret koji okuplja uticaj, stručnost i resurse potrebne za transformaciju načina na koji se seksualno iskorištavanje djece na internetu (OSCE) rješava širom svijeta. To je partnerstvo vlada, globalnih tehnoloških kompanija i organizacija civilnog društva. Njegova priroda od više interesnih strana jedinstvena je u ovom polju. Vizija Globalnog saveza WePROTECT je da identifikuje i zaštiti više žrtava, da se uhvati više počinilaca i zaustavi seksualno iskorištavanje djece na internetu.

Globalni savez WeProtect sastoji se od niza komponenata, konkretno Modela nacionalnog odgovora i Globalnog strateškog odgovora. Dodatni detalji mogu se naći u Dodatku 3.

Indeks sigurnosti djece na internetu 2020

Indeks sigurnosti djece na internetu DQ Institute 2020 (COSI) prva je svjetska analitička platforma u stvarnom vremenu koja pomaže zemljama da bolje prate status sigurnosti svoje djece na internetu.

COSI se zasniva na šest stubova koji čine COSI okvir. Prvi i drugi stub, sajber rizici i disciplinovana digitalna upotreba, odnose se na mudru upotrebu digitalne tehnologije. Treći i četvrti stub, digitalna kompetencija i usmjeravanje i obrazovanje, povezani su sa pružanjem mogućnosti. Posljednja dva stuba odnose se na infrastrukturu, to su stubovi socijalne infrastrukture i povezanosti.

45 Komisija za širokopojasni pristup za održivi razvoj (2019.), Stanje širokopojasne mreže 2019.: Širokopojasna mreža kao osnova za održivi razvoj, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

3.3 Primjeri odgovora na štete na internetu

Postoji niz primjera odgovora na štete na internetu u Dodatku 4. Ovi primjeri obuhvaćaju obrazovne odgovore, zakonodavstvo i utvrđivanje štete na internetu.

3.4 Prednosti nacionalne strategije zaštite djece na internetu

Usklađivanje zakona

Usvajanje odgovarajućih zakona od strane svih zemalja protiv zloupotrebe IKT-a u kriminalne ili druge svrhe ključno je za postizanje globalne sajber sigurnosti. Budući da prijetnje mogu poticati od bilo kuda širom svijeta, izazovi su sami po sebi međunarodnog obima i zahtijevaju međunarodnu saradnju, istražnu pomoć i zajedničke materijalne i proceduralne odredbe. Stoga je važno da države usklade svoje pravne okvire za borbu protiv sajber kriminala, zaštite djecu na internetu i olakšaju međunarodnu saradnju[46].

Razvoj odgovarajućeg nacionalnog zakonodavstva, srodnog pravnog okvira za sajber kriminal, i unutar ovog pristupa, usklađivanje na međunarodnom nivou, ključni je korak ka uspjehu bilo koje nacionalne strategije za zaštitu djece na internetu. To prije svega zahtijeva potrebne materijalno-pravne odredbe za kriminalizaciju djela poput računarske prevare, nezakonitog pristupa, uplitanja u podatke, kršenja autorskih prava i materijala seksualnog zlostavljanja djece, istovremeno vodeći računa da djeca ne budu neprimjereno kriminalizovana. Činjenica da u krivičnom zakonu postoje odredbe koje se primjenjuju na slična djela počinjena u stvarnom svijetu ne znači da se one mogu primijeniti i na djela počinjena putem interneta. Stoga je temeljna analiza važećih nacionalnih zakona vitalna kako bi se identifikovali svi mogući nedostaci. Sljedeći korak bio bi utvrđivanje i definisanje zakonodavnog jezika i referentnog materijala koji mogu pomoći zemljama u uspostavljanju usklađenih zakona o sajber kriminalu i proceduralnih pravila. Takve praktične instrumente države mogu koristiti za razradu pravnog okvira za sajber sigurnost i srodnih zakona. ITU sarađuje s državama članicama i relevantnim interesnim stranama u ovom smjeru i uvelike doprinosi napretku globalnog usklađivanja zakona o sajber kriminalu.

S obzirom na brz tempo tehnoloških inovacija, samoregulacija i koregulacija su predloženi kao potencijalna rješenja za zastarjelost postojećih propisa i dugotrajan zakonodavni postupak. Međutim, da bi bili efikasni, regulatorna tijela / kreatori politika moraju jasno definisati određene ciljeve i izazove na polju zaštite djece na internetu, uspostaviti jasan postupak pregleda i metodologiju za procjenu efikasnosti samoregulacije i koregulacije, a u slučaju da samoregulacija i koregulacija ne uspijevaju odgovoriti na identifikovane izazove, pokrenuti formalni zakonodavni postupak za rješavanje tih izazova. Takođe, uspješne mjere samoregulacije mogu se postepeno usvajati u formalni zakon u okviru zakonodavnog procesa kako bi postale pravna zabrana i spriječile povlačenje ili prestanak pridržavanja određenih inicijativa samoregulacije.

46 Komisija za širokopojasni pristup za održivi razvoj (2019.)

Koordinacija

Vjerovatno je da kod niza aktera i interesnih strana postoji čitav niz postojećih aktivnosti i radnji koje za cilj imaju zaštitu djece na internetu, ali koje su se odvijale izolovano. Njihovo razumijevanje je važno za uvažavanje postojećih napora u razvoju nacionalne strategije zaštite djece na internetu. Strategija će koordinisati i usmjeravati napore kroz orkestraciju postojećih i novih aktivnosti.

4. Preporuke za okvire i implementaciju

Vlade se moraju baviti svim vrstama manifestacija nasilja nad djecom u digitalnom okruženju. Međutim, poduzete mjere radi zaštite djece u digitalnom okruženju ne bi trebale neopravdano ograničavati ostvarivanje drugih prava, kao što su pravo na slobodu izražavanja, pravo na pristup informacijama ili pravo na slobodu udruživanja. Umjesto sputavanja dječije prirodne znatiželje i osjećaja za inovativnost iz straha od susreta s rizicima na internetu, ključno bi bilo iskoristiti dječiju snalažljivost i poboljšati njihovu otpornost dok istražuju potencijal digitalnog okruženja.

U mnogim slučajevima nasilje nad djecom čine druga djeca. U takvim situacijama vlade bi trebale što je više moguće slijediti restorativne pristupe koji popravljaju nanesenu štetu, istovremeno sprečavajući kriminalizaciju djece. Vlade bi trebale promovisati upotrebu IKT-a u prevenciji i rješavanju nasilja, poput razvoja tehnologija i resursa za djecu da pristupe informacijama, blokiraju štetni materijal i prijave slučajeve nasilja kada se pojave[47].

Da bi se suočile sa globalnom situacijom sigurnosti djece na internetu, vlade moraju olakšati komunikaciju između svojih odgovarajućih tijela i otvoreno sarađivati na uklanjanju štete za djecu na internetu.

4.1 Okvirne preporuke

4.1.1 Pravni okvir

Vlade bi trebale pregledati i, gdje je potrebno, ažurirati njihove pravne okvire kako bi podržale potpuno ostvarivanje prava djeteta u digitalnom okruženju. Sveobuhvatan pravni okvir trebao bi se baviti preventivnim mjerama; zabranom svih oblika nasilja nad djecom u digitalnom okruženju; pružanjem efikasnih lijekova, oporavkom i reintegracijom radi rješavanja problema kršenja dječijih prava; uspostavljanjm mehanizama savjetovanja, prijavljivanja i pritužbi osjetljivih na djecu; i uspostavljanjem mehanizama odgovornosti u borbi protiv nekažnjivosti[48].

Kad god je to moguće, zakonodavstvo treba biti tehnološki neutralno, tako da njegova primjenjivost neće biti narušena budućim tehnološkim razvojem[49].

Efikasna primjena zakona zahtijeva od vlada da uspostave dopunske mjere, uključujući inicijative za podizanje svijesti i socijalnu mobilizaciju, obrazovne napore i kampanje, te jačanje kapaciteta profesionalaca koji rade sa djecom i za djecu.

U razvoju odgovarajućeg zakona, takođe je važno imati na umu da djeca nisu homogena grupa. Možda će biti potrebni različiti odgovori za djecu različitih starosnih grupa, kao i djecu koja imaju specifične potrebe ili koja su pod povećanim rizikom da budu oštećena u digitalnom okruženju ili putem njega.

47 Specijalni predstavnik generalnog sekretara za borbu protiv nasilja nad djecom, *Godišnji izvještaj specijalnog predstavnika generalnog sekretara za borbu protiv nasilja nad djecom Savjetu za ljudska prava,* A/ HRC/31/20 (januar 2016), para. 103 i 104.

48 Specijalni predstavnik generalnog sekretara za borbu protiv nasilja nad djecom, *Oslobađanje dječijeg potencijala i smanjenje rizika: IKT, internet i nasilje nad djecom, 2014. (Njujork:* Ujedinjene nacije), str. 55.

49 Specijalni predstavnik generalnog sekretara za borbu protiv nasilja nad djecom, *Oslobađanje dječijeg potencijala i smanjenje rizika: IKT, internet i nasilje nad djecom, 2014. (Njujork:* Ujedinjene nacije), str. 64.

Vlade bi trebale stvoriti jasno i predvidljivo pravno i regulatorno okruženje koje podržava preduzeća i ostale treće strane da ispune svoje odgovornosti u zaštiti dječijih prava tokom svog poslovanja, u svojoj državi i u inostranstvu[50].

Sljedeći aspekti biće korisni za kreatore politika u pregledu obima bilo kojeg pravnog okvira i pružanju sljedećeg:

- vrbovanje ili drugi oblici navođenja na daljinu, iznude ili prisile djece na neprimjeren seksualni kontakt ili seksualnu aktivnost;
- osiguravanje posjedovanja, proizvodnje i distribucije materijala seksualnog zlostavljanja djece, bez obzira na namjeru distribucije;
- uznemiravanje, maltretiranje, zlostavljanje ili govor mržnje na internetu;
- teroristički materijal na internetu;
- sajber sigurnost;
- razmišljanje da je ono što je nezakonito izvan interneta jednako nezakonito i na internetu.

4.1.2 Politički i institucionalni okviri

Garantovanje ostvarivanja prava djece u digitalnom okruženju zahtijeva od vlada da uspostave ravnotežu između maksimalne koristi od dječije upotrebe IKT uz minimum rizika povezanih sa njima. To se može postići uključivanjem mjera za zaštitu djece na internetu u nacionalne planove za širokopojasnu mrežu[51] i razvijanjem posebne višestrane strategije zaštite djece na internetu. Takav dnevni red trebao bi biti u potpunosti integrisan sa svim postojećim političkim okvirima koji su važni za dječija prava ili dječiju zaštitu, a pored toga trebalo bi dopuniti nacionalne politike dječije zaštite nudeći poseban okvir za sve rizike i potencijalne štete za djecu sa ciljem stvaranja sigurne digitalne okoline[52] uključivog i osnažujućeg karaktera.

Vlade bi trebale da uspostave nacionalni koordinacioni okvir sa jasnim mandatom i dovoljnim ovlašćenjima za koordinaciju svih aktivnosti vezanih za dječija prava i digitalne medije i IKT na međusektorskim, nacionalnim, regionalnim i lokalnim nivoima. Vlade bi trebale da uključe vremenski ograničene ciljeve i transparentan proces za procjenu i praćenje napretka i moraju osigurati da se na raspolaganje stave neophodni ljudski, tehnički i finansijski resursi za efikasno djelovanje ovog okvira[53].

Vlade bi trebale uspostaviti platformu sa više interesnih strana za usmjeravanje razvoja, primjene i praćenja nacionalnog digitalnog programa rada za djecu. Takva platforma trebala bi okupiti predstavnike najvažnijih korisnika, uključujući: djecu i mlade; udruženja roditelja / staratelja; odgovarajuće vladine sektore; sektor obrazovanja, pravosuđa, zdravstva i socijalne zaštite; nacionalne institucije za zaštitu ljudskih prava i odgovarajuća regulatorna tijela; civilno društvo; industriju; akademiju; i odgovarajuća profesionalna udruženja.

50 UN Komitet za prava djeteta, *Opšti komentar br. 16, par.* 53.
51 Stanje širokopojasne mreže 2019, Preporuka 5.6, stranica 78. https://www.itu.int/dms_pub/itu-s/opb/ pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.
52 Za primjere odredbi o zaštiti djece u nacionalnim planovima za širokopojasnu mrežu pogledajte poglavlje 10 Izvještaja o sigurnosti djece na internetu.
53 Specijalni predstavnik generalnog sekretara za borbu protiv nasilja nad djecom, *Godišnji izvještaj specijalnog predstavnika generalnog sekretara za borbu protiv nasilja nad djecom* (december 2014.) A/HRC/28/55 i *Oslobađanje dječijeg potencijala i smanjenje rizika*: *IKT, internet i nasilje nad djecom, 2014. (Njujork:* Ujedinjene nacije), par. 88.

4.1.3 Regulatorni okvir

Vlade su odgovorne za kršenja dječijih prava koja su u cjelini ili djelimično prouzrokovana od strane poslovnih preduzeća, ako nisu poduzela potrebne, odgovarajuće i razumne mjere za sprječavanje i otklanjanje takvih povreda ili su na drugi način učestvovale ili tolerisale kršenja[54].

Vodeći principi o poslovanju i ljudskim pravima predviđaju da bi korporacije trebale osigurati mehanizme pravnih lijekova i žalbi koji su legitimni, dostupni, predvidljivi, nepristrasni, kompatibilni sa pravima, transparentni, zasnovani na dijalogu i angažovanju i koji su izvor kontinuiranog učenja. Mehanizmi za žalbe koje uspostavljaju poslovna preduzeća mogu pružiti fleksibilna i pravovremena alternativna rješenja i ponekad bi moglo biti u najboljem interesu djeteta da se putem njih riješe brige zbog ponašanja kompanije. U svim slučajevima pristup sudovima ili sudskoj reviziji upravnih lijekova i drugih postupaka[55] bi trebao biti dostupan. Treba razmotriti mehanizme koji stvaraju sigurne usluge prilagođene uzrastu za djecu kako bi korisnici mogli prijaviti svoju zabrinutost.

Bez obzira na postojanje internih mehanizama za žalbe, vlade bi trebale uspostaviti mehanizme praćenja za istrage i ispravke kršenja dječijih prava, s ciljem povećanja odgovornosti IKT i drugih relevantnih kompanija, kao i da povećaju odgovornosti regulatornih agencija za razvoj standarda relevantnih za dječija prava i IKT[56]. Ovo je posebno važno jer su drugi pravni lijekovi koji su dostupni onima na koje korporativno djelovanje nepovoljno utiče - poput parnica i drugih pravnih sredstava - često komplikovani i skupi[57].

UN Komitet za prava djeteta naglasio je potencijalnu ulogu nacionalnih institucija za ljudska prava u ovom području, ističući kako bi mogle imati ulogu primanja, istrage i posredovanja u žalbama na kršenja prava od strane industrijskih subjekata; sprovođenja javnih istraga o zloupotrebama velikih razmjera; i preduzimanja zakonodavnih revizija kako bi se osiguralo poštovanje Konvencije o pravima djeteta. Komitet je naznačio da bi, po potrebi, „države trebale proširiti zakonodavni mandat nacionalnih institucija za ljudska prava kako bi se prilagodile dječijim pravima i poslovanju“. Posebno je važno da bilo koji mehanizam za žalbe bude osjetljiv na djecu, osigura privatnost i zaštitu žrtava te da poduzme aktivnosti nadgledanja, praćenja i provjere za djecu koja su žrtve.

Primjer područja u kojem bi nacionalna institucija za ljudska prava ili drugo regulatorno tijelo mogli djeci pružiti djelotvoran pravni lijek su slučajevi sajber maltretiranja. Interni pravni lijekovi i mehanizmi za žalbe ponekad se pokažu nedjelotvornima u takvim slučajevima, iako je sadržaj uznemiravajući i štetan, nacionalno zakonodavstvo često ga ne rješava i nema jasne osnove za zahtjev za njegovo uklanjanje od strane vlasnika sadržaja. Davanjem ovlašćenja javnim vlastima da primaju žalbe u vezi sa slučajevima sajber maltretiranja i da intervenišu kod vlasnika sadržaja kako bi se uklonio odgovarajući materijal bio bi važan vid zaštite za djecu[58]. To bi imalo prednosti brzog reagovanja - što je od presudne važnosti u kontekstu sajber maltretiranja - i takođe jasan pravni osnov za rješavanje problema uklanjanja materijala sajber maltretiranja.

54 UN Komitet za prava djeteta, *Opšti komentar br. 16, par.* 28.
55 Izvještaj specijalnog predstavnika generalnog sekretara za pitanje ljudskih prava i transnacionalnih korporacija i ostalih poslova, A/HRC/17/31 (2011), par. 71.
56 UN Komitet za prava djeteta, *Izvještaj o danu opšte rasprave 2014., par.* 96.
57 Izvještaj specijalnog izvjestioca o promociji i zaštiti prava na slobodu mišljenja i izražavanja, A/HRC/32/38 (2016), par. 71.
58 Bertrand de Crombrugghe, “Izvještaj Savjeta za ljudska prava o njegovom trideset prvom zasjedanju” (UN Savjet za ljudska prava, 2016).

Prilikom oblikovanja svog pristupa regulaciji digitalnog okruženja, vlade takođe moraju biti svjesne uticaja takvih propisa na uživanje svih ljudskih prava, uključujući slobodu izražavanja[59].

Vlade bi trebalo da obavežu preduzeća da izvrše detaljnu analizu prava djeteta. Ovo bi osiguralo da poslovna preduzeća identifikuju, spriječe i ublaže njihov uticaj na dječija prava, uključujući i u njihovim poslovnim odnosima i u globalnim operacijama[60].

Pored toga, vlade bi trebale razmotriti dopunske mjere kao što je osiguravanje da industrijski subjekti čije aktivnosti mogu imati uticaja na dječija prava u digitalnom okruženju moraju biti u skladu s najvišim standardima u pogledu sprečavanja i reagovanja na potencijalna kršenja prava kako bi se kvalifikovali za finansiranje ili sklapanje ugovora.

4.2 Preporuke za implementaciju

Vlade bi trebale osigurati pristup efikasnim pravnim lijekovima za djecu koja su žrtve kršenja prava, uključujući i pomoć u traženju brze i odgovarajuće nadoknade za pretrpljenu štetu, kompenzacijom po potrebi. Vlade bi takođe trebale pružiti adekvatnu podršku i pomoć djeci koja su žrtve kršenja prava koja se odnose na digitalne medije i IKT, uključujući sveobuhvatne usluge kako bi se djetetu osigurao puni oporavak i reintegracija i spriječila ponovna viktimizacija djece žrtava[61].

Sigurni i lako dostupni mehanizmi savjetovanja, izvještavanja i podnošenja žalbi za djecu, poput telefonskih linija za pomoć, trebali bi biti uspostavljeni zakonom i trebali bi biti dio nacionalnog sistema dječije zaštite. Važno je osigurati da su ove usluge povezane s bilo kojim regulatornim službama kako bi se što više pojednostavila interakcija djeteta sa institucionalnim tijelima u vremenu u kojem možda proživljava nevolju. Telefonske linije za pomoć su posebno dragocjene u pogledu visoko osjetljivih pitanja, poput seksualnog zlostavljanja, o kojim je možda djeci teško da pričaju sa vršnjacima, roditeljima, starateljima ili nastavnicima. Telefonske linije za pomoć takođe igraju ključnu ulogu u usmjeravanju djece na usluge kao što su pravne usluge, sigurne kuće, organi za sprovođenje zakona ili rehabilitacija[62].

Takođe, vlade moraju razumjeti i pratiti ponašanje prestupnika kako bi povećale stope otkrivanja nasilnika i smanjile rizik od ponovljenih prestupa osuđenih nasilnika. Uspostavljanje telefonskih linija za pomoć koje nude besplatno i anonimno savjetovanje i podršku putem telefona ili poruka za ljude koji doživljavaju osjećanja ili misli seksualnog interesovanja za djecu - potencijalne prestupnike. Pomaganje prestupnicima da promijene svoje ponašanje smanjuje rizik od ponovnog prestupa.

Zakonski mehanizmi za rješavanje žalbi takođe čine ključni dio okvira za efikasne pravne lijekove.

Regulatorna tijela bi trebala sprovesti nezavisna mjerenja i studije kako bi procijenila kako platforme izvještavaju i bave se pitanjima koja se tiču zaštite djece. Postoji tehnologija za regulatorna tijela da samostalno nadgledaju platforme. Treba podržati pružaoce usluga u objavljivanju izvještaja o transparentnosti.

59 Izvještaj specijalnog izvjestioca o promociji i zaštiti prava na slobodu mišljenja i izražavanja, A/HRC/32/38 (2016), par. 45.
60 UN Komitet za prava djeteta, *Opšti komentar br. 16, paa.* 62.
61 UN Komitet za prava djeteta, *Izvještaj o danu opšte rasprave 2014., par.* 106.
62 Specijalni predstavnik generalnog sekretara za borbu protiv nasilja nad djecom, *Oslobađanje dječijeg potencijala i smanjenje rizika, str. 51 i str. 65.*

Zajedno s međunarodnom zajednicom i industrijom, vlade bi trebale razviti univerzalni set za metriku koji interesne strane mogu koristiti za mjerenje svih važnih aspekata sigurnosti djece na internetu.

4.2.1 Seksualno iskorištavanje

Prilikom razmatranja prijetnji za djecu od šteta, posebno materijala seksualnog zlostavljanja djece, generisanih vlastitih sadržaja, vrbovanja i seksualnog iznuđivanja i drugih rizika na internetu, kreatori politika mogli bi u obzir uzeti sljedeće:

- Korake za ometanje ili smanjenje prometa materijala seksualnog zlostavljanja djece, na primjer uspostavljanjem nacionalne dežurne telefonske linije ili IWF portala za prijave, te primjenom mjera koje će blokirati pristup sadržaju na internetu za koji je poznato da sadrži ili oglašava dostupnost materijala seksualnog zlostavljanja djece.
- Osigurati postojanje nacionalnih procesa kako bi se osiguralo da se svi materijali seksualnog zlostavljanja djece pronađeni u nekoj zemlji usmjere prema centralizovanom nacionalnom resursu koji ima zakonodavna ovlaštenja da naredi kompanijama da uklone sadržaj.
- Strategije za rješavanje potražnje za materijalom seksualnog zlostavljanja djece, posebno među onima koji su osuđivani za takva djela. Važno je izgraditi svijest o činjenici da ovo nije zločin bez žrtve: djeca se zlostavljaju kako bi proizvela materijal koji se gleda, a namjernim pregledom ili preuzimanjem materijala seksualnog zlostavljanja djece osoba direktno doprinosi zlostavljanju prikazanog djeteta, a također ohrabruje zlostavljanje većeg broja djece radi stvaranja više slika.
- Jačati svijesti o činjenici da djeca nikada ne mogu pristati na seksualno zlostavljanje, bilo radi proizvodnje materijala seksualnog zlostavljanja djece ili iz bilo kojeg drugog razloga. Ohrabriti ljude koji koriste materijal seksualnog zlostavljanja djece da potraže pomoć, istovremeno ih obavještavajući da će biti krivično odgovorni za nezakonitu aktivnost kojom su se bavili / bave.
- Ostale strategije za rješavanje potražnje za materijalom seksualnog zlostavljanja djece. Na primjer, neke zemlje vode registar osuđenih seksualnih prestupnika. Sudovi su izdali sudske naloge kojima zabranjuju takvim počiniocima da koriste internet u potpunosti ili im zabranjuju da koriste dijelove interneta koje posjećuju djeca i mladi. Problem ovih naredbi do sada je bio izvršenje. Međutim, u nekim se zemljama razmatra integracija liste poznatih seksualnih prestupnika u listu za blokiranje koja će spriječiti one koji su na njoj da posjete ili se pridruže određenim internet stranicama, na primjer internet stranicama za koje je poznato da ih posjećuje veliki broj djece i mladih ljudi. Naravno, ako se prestupnik pridruži internet stranici dok koristi drugo ime ili lažnu prijavu, efikasnost takvih mjera može se znatno smanjiti, ali kriminalizacijom ovog ponašanja može se uspostaviti daljnje odvraćanje.
- Pružiti odgovarajuće dugoročne podrške žrtvama. U slučajevima gdje su djeca ili mladi ljudi bili žrtve na internetu, gdje se, na primjer, njihova nezakonita slika pojavila na internetu, oni će se prirodno osjećati vrlo zabrinuto zbog toga ko ih je mogao vidjeti i kakav će to uticaj imati na njih. To bi moglo dovesti do toga da se dijete ili mlada osoba osjeća ranjivo na maltretiranje ili dalje seksualno iskorištavanje i zlostavljanje. U tom kontekstu biće važno da postoje usluge profesionalne podrške za podršku djeci i mladima koji se nađu u tim okolnostima. Takva podrška će možda trebati biti pružena dugoročno.
- Osigurati uspostavljanje i široku promociju mehanizma koji pruža lako razumljiva i brza sredstva za prijavljivanje nezakonitog sadržaja ili nezakonitog ili zabrinjavajućeg ponašanja na internetu, npr. sistem sličan onome koji su uspostavili Virtual Global Taskforce and INHOPE. Treba podsticati upotrebu INTERPOL i24 / 7 sistema.
- Obezbijediti da je dovoljan broj službenika za sprovođenje zakona prošao adekvatnu obuku za istragu kriminala zasnovanog na internetu i računarima i da imaju pristup odgovarajućim forenzičkim ustanovama koje će im omogućiti izvlačenje i tumačenje relevantnih digitalnih podataka.

- Ulagati u obuku za organe za sprovođenje zakona, tužilaštvo i pravosuđe o metodama koje kriminalci na internetu koriste za izvršenje ovih zločina. Takođe će biti potrebno ulaganje u nabavku i održavanje objekata neophodnih za prikupljanje i tumačenje forenzičkih dokaza dobijenih sa digitalnih uređaja. Pored toga, biće važno uspostaviti bilateralnu i multilateralnu saradnju i razmjenu informacija sa odgovarajućim organima za sprovođenje zakona i istražnim tijelima u drugim zemljama.

4.2.2 Obrazovanje

Edukovati djecu o digitalnoj pismenosti kao dio strategije kojom se osigurava da mogu imati koristi od tehnologije, bez štete. To će djeci omogućiti da razviju vještine kritičkog razmišljanja koje će im pomoći da prepoznaju i razumiju dobre i loše strane svog ponašanja u digitalnom prostoru. Iako je djeci važno ilustrovati štete koje se mogu dogoditi na internetu, ovo će biti efikasno samo ako je uključeno u dio šireg programa digitalne pismenosti koji treba da odgovara uzrastu i usredsredi se na vještine i sposobnosti. Važno je uključiti koncepte socijalnog i emocionalnog učenja u obrazovanje o sigurnosti na internetu, jer će oni dati podršku u razumijevanju i upravljanju osjećajima učenika kako bi imali zdrave odnose i odnose pune poštovanja, kako na internetu tako i izvan njega.

Djeca bi trebala da imaju odgovarajuće alate i znanje za korištenje interneta i to je jedan od najboljih načina da ih se zaštiti. Jedan od načina je uvođenje digitalne pismenosti u školske programe. Druga mogućnost je stvaranje obrazovnih resursa izvan školskog plana i programa.

Oni koji rade s djecom trebali bi imati odgovarajuće znanje i vještine da pruže pouzdanu podršku djeci u odgovaranju na i rješavanju problema vezanih za zaštitu djece na internetu, kao i da obuče djecu potrebnim digitalnim vještinama da imaju koristi od korištenja tehnologije.

4.2.3 Industrija

Nacionalni i međunarodni predstavnici industrije trebali bi raditi na podizanju svijesti o problemima dječije sigurnosti na internetu i pomoći svim odraslim osobama odgovornim za dobrobit djeteta - uključujući roditelje i staratelje, škole, organizacije koje pružaju usluge mladima i zajednice - da razviju znanje i vještine koje su im potrebne da čuvaju djecu sigurnom. Industrija bi trebala usvojiti pristup sigurnosti prilikom samog dizajna svojih proizvoda, usluga i platformi, prepoznajući sigurnost kao glavni cilj.

- Da pruže prikladne alate prilagođene porodici kako bi svojim korisnicima pomogli da bolje upravljaju zaštitom svojih porodica na internetu.
- Da obezbijede odgovarajuće mehanizme prijavljivanja za svoje korisnike da prijavljuju probleme i nedoumice. Korisnici bi trebali da očekuju pravovremene odgovore na ove izvještaje koji sadrže informacije o poduzetim radnjama i, ako je primjenjivo, uputstva gdje korisnici mogu dobiti daljnju podršku.
- Pored toga, pružiti proaktivno prijavljivanje zlostavljanja djece kako bi se otkrila i riješila bilo koja vrsta zlostavljanja (klasifikovanog kao kriminalna aktivnost) djece. Ova praksa je pokazala da ako sve interesne strane doprinesu otkrivanju, blokiranju i prijavljivanju, možemo razmišljati o tome da imamo čistiji i sigurniji internet za sve. Industrija bi trebala razmotriti mogućnost uzimanja svih relevantnih alata kako bi spriječila eksploataciju svojih platformi, poput IWF usluga.

Od vitalne je važnosti da se uključe svi relevantni akteri u ekosistem, koji bi trebali biti svjesni rizika i šteta na internetu kako bi mogli spriječiti da djeca budu izložena nepotrebnim rizicima.

Razviti zajedničku metriku za sigurnost djece na internetu kako bi se izmjerili svi relevantni aspekti ove materije. Zajednički standardi i metrički podaci jedini su način za praćenje napretka u zemljama i za utvrđivanje uspjeha projekata i aktivnosti koji se sprovode radi uklanjanja svakog nasilja nad djecom i prepoznavanja snage ekosistema sigurnosti djece na internetu.

5. Razvoj nacionalne strategije zaštite djece na internetu

5.1 Nacionalna kontrolna lista

Da bi formulisali nacionalnu strategiju koja se fokusira na sigurnost djece na internetu, kreatori politika moraju razmotriti niz strategija. Tabela 1 daje ključne oblasti za razmatranje.

Tabela 1: Ključne oblasti za razmatranje

	#	Ključne oblasti za razmatranje	Više detalja
Pravni okvir	1	Pregledati postojeći pravni okvir kako bi utvrdili da postoje sva sva nadležna državna tijelakoja omogućavaju sprovođenje zakona i druge relevantne agencije za zaštitu osoba mlađih od 18 godina na internetu na svim platformama s internetom.	Generalno će biti neophodno da postoji skup zakona koji jasno pokazuje da svaki zločin koji se može počiniti nad djetetom u stvarnom svijetu može, *mutatis mutandis*, biti počinjen i na internetu ili na bilo kojoj drugoj elektronskoj mreži. Možda će biti potrebno razviti nove zakone ili prilagoditi postojeće kako bi se zabranili određeni oblici ponašanja koji se mogu odvijati samo na internetu, na primjer, navođenje djece na daljinu da izvršavaju ili gledaju seksualne činove, ili vrbovanje djece radi sastanka u stvarnom svijetu u seksualne svrhe. Dodatno za ove potrebe, biće potrebno uopšteno da postoji zakonski okvir koji zabranjuje zloupotrebu računara u kriminalne svrhe, hakovanje ili drugu zlonamjernu upotrebu ili upotrebu računarskog koda bez pristanka i koji utvrđuje da je internet mjesto na kojem se mogu počiniti krivična djela.
	2	Odrediti, mutatis mutandis, da je svaki postupak protiv djeteta koji je nezakonit u stvarnom svijetu nezakonit i na internetu i da su internetska pravila o zaštiti podataka i privatnosti za djecu takođe primjerena.	

	#	Ključne oblasti za razmatranje	Više detalja
Regulatorni okvir	3	Razmotriti razvoj regulatorne politike. To može uključivati politiku razvoja samoregulacije ili koregulacije kao i puni regulatorni okvir. Model samoregulacije ili koregulacije može uključivati formulisanje i objavljivanje kodeksa dobre prakse ili osnovnih sigurnosnih očekivanja na internetu, u smislu pružanja pomoći u uključivanju, koordinaciji ili organizaciji i održavanju učešća svih relevantnih interesnih strana i u smislu povećanja brzine kojom se mogu formulisati i primijeniti odgovarajući odgovori na tehnološke promjene. Regulatorni model može definisati očekivanja i obaveze između interesnih strana i uključiti se u pravni kontekst. Mogu se razmotriti i kazne za kršenje politike.	Neke zemlje su uspostavile model samoregulacije ili koregulacije u vezi sa razvojem politike u ovoj oblasti i putem takvih modela su, na primjer, objavile kodekse dobre prakse za vođenje internet industrije u pogledu mjera koje bi mogle najbolje raditi kada pričamo o tome da djeca i mladi ljudi treba da budu sigurniji na internetu. Na primjer, unutar Evropske unije gdje su Evropski kodeksi objavljeni i za sajtove društvenih medija i za mobilne mreže u vezi s pružanjem sadržaja i usluga djeci i mladima putem njihovih mreža. Samoregulacija i koregulacija mogu biti agilnije u smislu povećanja brzine kojom se mogu formulisati i primijeniti odgovarajući odgovori na tehnološke promjene. U novije vrijeme nekoliko zemalja je razvilo i / ili primijenilo regulatorni okvir. U ovim primjerima regulatorni okvir je nastao iz modela samoregulacije ili koregulacije i definiše zahtjeve i očekivanja interesnih strana, posebno dobavljača u industriji, kako bi bolje zaštitili svoje korisnike.

	#	Ključne oblasti za razmatranje	Više detalja
Prijavljivanje - nezakonit sadržaj	4	Osigurati da se uspostavi i široko promoviše mehanizam koji pruža lako razumljiva sredstva za prijavljivanje raznih nezakonitih sadržaja pronađenih na internetu. Na primjer, nacionalna dežurna linija koja ima sposobnost brzog reagovanja i da nezakoniti materijal brzo ukloni ili ga učini nedostupnim. Industrija bi trebala imati mehanizme za identifikovanje, blokiranje i uklanjanje zlostavljanja djece na internetu, u svim uslugama koje se odnose na njihove organizacije.	Mehanizme za prijavljivanje zloupotrebe usluge na internetu ili za prijavljivanje nepoželjnog ili nezakonitog ponašanja na internetu, na primjer, preko nacionalne dežurne telefonske linije, trebalo bi široko oglašavati i promovisati kako na internetu tako i u drugim medijima. Ako nacionalna dežurna telefonska linija nije dostupna, IWF nudi Portale za prijavljivanje kao rješenje. Linkovi za mehanizme prijavljivanja zloupotrebe trebali bi biti istaknuti na odgovarajućim dijelovima bilo koje internet stranice koja omogućava prikazivanje sadržaja koji generišu korisnici. Takođe bi trebalo da bude omogućeno da ljudi koji se na bilo koji način osjećaju ugroženima ili da ljudi koji su bili svjedoci bilo kakve zabrinjavajuće aktivnosti na internetu, imaju mogućnost da to što prije prijave odgovarajućim agencijama za sprovođenje zakona koje trebaju biti obučene i spremne odgovoriti. Virtual Global Taskforce je tijelo za sprovođenje zakona koje pruža svakodnevni mehanizam za primanje prijava o nezakonitom ponašanju ili sadržaju od osoba iz SAD-a, Kanade, Australije i Italije, a uskoro se očekuju i druge zemlje. Pogledajte www .virtualglobaltaskforce.com. Takođe pogledajte INHOPE.
Izvještavanje - zabrinutost korisnika	5	Industrija bi trebala pružiti korisnicima mogućnost da prijave brige i probleme i reaguju u skladu s tim.	Pružaoci usluga bi trebalo da budu obavezni da obezbijede i jasno naznače svojim korisnicima mogućnost prijavljivanja problema i nedoumica u okviru njihovih usluga. One bi trebale biti prilagođene za djecu i lako dostupne.

	#	Ključne oblasti za razmatranje	Više detalja
Akteri i interesne strane	6	Angažovati sve relevantne interesne strane kojima je u interesu da zaštite djecu na internetu, posebno: • Državne agencije • Organe za sprovođenje zakona • Organizacije socijalnih usluga • Provajderi internetskih usluga (ISP) i drugi provajderi elektronskih usluga (ESP) • Provajderi usluga mobilne telefonije • Javni provajderi Wi-Fi mreže • Ostale važne kompanije visoke tehnologije • Organizacije nastavnika • Organizacije roditelja • Djeca i mladi • Dječija zaštita i druge relevantne NVO • Akademska i istraživačka zajednica • Vlasnici kafića sa internetom i drugi pružaoci usluga javnog pristupa internetu npr. biblioteke, telecentri, PC Bang-ovi (PC igraonice)[63] i centri za igre na sreću na internetu itd.	Nekoliko nacionalnih vlada smatra korisnim okupljanje svih ključnih aktera i učesnika da se fokusiraju na razvoj i sprovođenje nacionalne inicijative oko pravljenja interneta sigurnijim mjestom za djecu i mlade, i podizanje svijesti o problemima i načinu rješavanja problema na vrlo praktičan način. U okviru ove strategije biće važno shvatiti da se mnogi korisnici uopšteno i stalno povezuju na internet putem različitih uređaja. Potrebno je uključiti širokopojasne, mobilne i Wi-Fi operatere. Pored toga, u mnogim zemljama mreža javnih biblioteka, telecentara i kafića sa internetom može biti važan izvor pristupa internetu, posebno za djecu i mlade.
Istraživanje	7	Obaviti istraživanje spektra nacionalnih aktera i interesnih strana kako bi utvrdili njihova mišljenja, iskustva, zabrinutosti i mogućnosti u vezi sa zaštitom djece na internetu. Ovo bi takođe trebalo uključiti nivo određene odgovornosti zajedno sa postojećim ili planiranim aktivnostima za zaštitu dece na internetu.	

63 „PC Bang“ je pojam koji se često koristi u Republici Koreji i u nekim drugim zemljama za opisivanje velike prostorije u kojoj LAN mreža omogućava igranje igara u velikim razmjerama, bilo na internetu ili između igrača u sobi.

	#	Ključne oblasti za razmatranje	Više detalja
Obrazovanje o digitalnoj pismenosti i sposobnosti ma	8	Razviti digitalnu pismenost kao dio bilo kojeg nacionalnog školskog programa koji je primjeren uzrastu i primjenjiv na svu djecu.	Škole i obrazovni sistem uopšte će predstavljati temelj obrazovanja i digitalne pismenosti nacionalne strategije zaštite djece na internetu. Svaki nacionalni školski plan i program trebao bi uključivati aspekte zaštite djece na internetu i težiti da se razviju kod djece svih uzrasta vještine primjerene uzrastu kako bi uspješno koristili i imali koristi od tehnologije i kako bi mogli da prepoznaju prijetnje i štete da bi ih uspješno izbjegavali. Oni bi trebali prepoznavati i nagrađivati pozitivno i konstruktivno ponašanje na internetu. U bilo kojoj kampanji edukacije i podizanja svijesti biće važno izabrati pravi ton. Treba izbjegavati razmjenu poruka zasnovanih na strahu, a mnogim pozitivnim i zabavnim osobinama nove tehnologije treba posvetiti dužnu pažnju. Internet ima veliki potencijal kao sredstvo koje daje mogućnosti djeci i mladima za otkrivanje novih svjetova. Podučavanje pozitivnih i odgovornih oblika ponašanja na internetu je ključni cilj programa obrazovanja i podizanja svijesti. Oni koji rade sa djecom, posebno učitelji, trebaju proći odgovarajuću obuku i biti opremljeni da bi uspješno obrazovali i razvijali ove vještine kod djece. Trebali bi da mogu da razumiju prijetnje i štete na internetu, i da imaju sposobnost da pouzdano prepoznaju znakove zlostavljanja i štete i da reaguju i prijave te probleme kako bi zaštitili svoju djecu

	#	Ključne oblasti za razmatranje	Više detalja
Obrazovni resursi	9	Osloniti se na znanje i iskustvo svih interesnih strana i razviti sigurnosne poruke i materijale za internet koji odražavaju lokalne kulturne norme i zakone i osigurati da se one efikasno distribuiraju i na odgovarajući način prezentuju cijelom ključnom ciljanom auditorijumu. Razmisliti o tome da potražite pomoć masovnih medija u promociji poruka o podizanju svijesti. Razviti materijale koji ističu pozitivne i osnažujuće aspekte interneta za djecu i mlade i izbjegavajte razmjenu poruka zasnovanih na strahu. Promovisati pozitivne i odgovorne oblike ponašanja na internetu. Razmisliti o razvoju resursa koji bi pomogli roditeljima da procijene sigurnost svoje djece na internetu i nauče o tome kako smanjiti rizike i povećati do maksimuma potencijal za vlastitu porodicu kroz ciljano obrazovanje.	Kod proizvodnje obrazovnog materijala, važno je imati na umu da se mnogi ljudi koji su novi u korištenju tehnologije neće osjećati ugodno kada je koriste. Iz tog razloga je važno osigurati da sigurnosni materijali budu dostupni u pisanom obliku ili proizvedeni na drugim medijima koji će početnicima biti poznatiji, na primjer video prezentacija Mnoge velike internetske kompanije prave internet stranice koje sadrže mnogo informacija o problemima za djecu i mlade na internetu. Međutim, vrlo često će ovaj materijal biti dostupan samo na engleskom ili na vrlo malom broju jezika. Stoga je vrlo važno da se materijali proizvode lokalno i da oslikavaju lokalne zakone, kao i lokalne kulturne norme. Ovo će biti neophodno za bilo koju kampanju o sigurnosti na internetu ili za bilo koji materijal za obuku koji se razvija.
Zaštita djece	10	Osigurati da postoje univerzalni i sistematski mehanizmi zaštite djece koji obavezuju sve one koji rade s djecom (socijalna zaštita, zdravstvo, škole itd.) da identifikuju, reaguju i prijave slučajeve zlostavljanja i štete koji se dešavaju na internetu.	Trebalo bi uspostaviti univerzalni sistem zaštite djece koji bi se primjenjivao na sve one koji rade s djecom, obavezujući ih da prijave zlostavljanje ili nanošenje štete djeci kako bi omogućili istragu i rješavanje takvih situacija.

	#	Ključne oblasti za razmatranje	Više detalja
Nacionaln a svijest	11	Organizovati kampanje podizanja nacionalne svijesti kako bi stvorili priliku za opšte isticanje problema zaštite djece na internetu. Moglo bi biti korisno iskoristiti globalne kampanje poput Dana sigurnijeg interneta za izgradnju kampanje.	Roditelji, staratelji i profesionalci, poput nastavnika, imaju presudnu ulogu u očuvanju sigurnosti djece i mladih na internetu. Trebalo bi razviti programe podrške koji pomažu u jačanju svijesti o problemima i pružaju strategije za rješavanje tih problema. Takođe bi trebalo razmotriti traženje pomoći masovnih medija u promociji poruka i kampanja o podizanju svesti. Prilike poput Dana sigurnijeg interneta biće korisne u podsticanju i ohrabrivanju nacionalnog dijaloga o zaštiti djece na internetu. Mnoge zemlje su uspješno izgradile kampanje podizanja nacionalne svijesti organizovane oko Dana sigurnijeg interneta i uključuju čitav niz aktera i interesnih strana u širenje univerzalnih poruka putem medija i društvenih medija.

	#	Ključne oblasti za razmatranje	Više detalja
Alati, usluge i podešavanja	12	Razmotriti ulogu postavki uređaja, tehničkih alata (poput programa za filtriranje) i aplikacija i postavki za zaštitu djece koje mogu pomoći. Podstaknuti korisnike da preuzmu odgovornost za svoje uređaje podstičući ažuriranja operativnog sistema i upotrebu odgovarajućeg sigurnosnog softvera i aplikacija.	Dostupno je nekoliko usluga koje mogu pomoći u uklanjanju neželjenog materijala ili blokiranju neželjenih kontakata. Neki od ovih programa za zaštitu djece i filtriranje mogu biti u osnovi besplatni jer su dio računarskog operativnog sistema ili se nude kao dio paketa dostupnog od provajdera internetskih usluga ili provajdera elektronskih usluga. Proizvođači nekih konzola za igranje takođe nude slične alate ako uređaj ima omogućen pristup internetu. Ovi programi nisu potpuno sigurni, ali mogu pružiti poželjan nivo podrške, posebno u porodicama sa mlađom djecom. Većina uređaja imaju postavke koje pomažu u zaštiti djece i promovišu zdravu i uravnoteženu upotrebu. To se odnosi na mehanizme koji omogućavaju roditeljima da upravljaju uređajima svoje djece, određujući vrijeme, aplikacije i usluge koje oni mogu koristiti i da upravljaju kupovinama. U novije vrijeme razvijeni su izvještaji i postavke koje omogućavaju korisnicima i roditeljima da bolje razumiju i upravljaju vremenom i mogućnostima pristupa ekranu. Ovi tehnički alati bi se trebali koristiti kao dio šireg arsenala. Uključivanje roditelja i / ili staratelja je presudno. Kako djeca postaju malo starija, želiće više privatnosti, a takođe će osjećati snažnu želju da počnu samostalno istraživati. Pored toga, tamo gdje postoji odnos naplate između dobavljača i kupca, procesi provjere starosne dobi mogu imati vrlo važnu ulogu u pružanju pomoći dobavljačima roba i usluga sa starosnim ograničenjem ili izdavačima materijala koji je namijenjen samo publici određene starosne dobi ili starijoj, da dopru do te određene publike. Tamo gdje ne postoji odnos naplate, upotreba tehnologije provjere starosne dobi može biti problematična ili u mnogim zemljama ovo može biti nemoguće zbog nedostatka pouzdanih izvora informacija.

5.2 Primjeri pitanja

Nakon identifikacije nacionalnih interesnih strana i aktera, sljedeća pitanja mogu se dostaviti interesnim stranama i akterima i mogu se zamoliti da ih dovrše i odgovore. Njihovi odgovori pomoći će odrediti obim pokrivenosti politikom, snage kao i područja na koja treba usmjeriti pažnju na nacionalnoj kontrolnoj listi.

- U kojoj su mjeri sigurnost na internetu i dječija prava vaša odgovornost?
- Kako su sigurnost na internetu i dječija prava integrisani u vaše postojeće politike i procese?
- U kojoj mjeri je sigurnost na internetu obuhvaćena postojećim zakonodavstvom?
- Koji su vaši sigurnosni prioriteti na internetu?
- Koje aktivnosti treba da podržite na internetu?
- Kako sarađujete sa drugim agencijama i organizacijama na poboljšanju / napretku sigurnosti na internetu?
- Mogu li vam djeca / roditelji prijaviti sigurnosne brige ili probleme na internetu?
- Koja su vaša tri ključna izazova u svijetu na internetu?
- Koje su vaše tri ključne prednosti u svijetu na internetu?

Takođe bi bilo korisno istražiti i razumjeti percepciju i iskustva djece kao i njihovih roditelja u vezi sa zaštitom djece na internetu.

6. Referentni materijal

Sigurnost djece na internetu: Ključni dokumenti i publikacije

2020.

- ECPAT International, Seksualno iskorištavanje djece na Srednjem istoku i Sjevernoj Africi, 2020.
- DQ Institute, 2020 Izvještaj o sigurnosti djece na internetu, 2020.
- EU Kids Online, EU Kids Online 2020: Rezultati istraživanja u 19 zemalja, 2020.

2019.

- Internet Watch Foundation (IWF), Godišnji izvještaj, 2019.
- Globalni savez WeProtect, Globalna procjena prijetnje, 2019.
- Komisija za širokopojasni pristup / ITU Sigurnost djece na internetu. Opšta deklaracija, 2019.
- Komisija za širokopojasni pristup / ITU Sigurnost djece na internetu: Smanjenje rizika od nasilja, zlostavljanja i iskorištavanja na internetu, 2019.
- Global Kids Online, Odrastanje u povezanom svijetu, 2019.
- Preispitivanje otkrivanja slika seksualnog zlostavljanja djece na internetu, u zborniku radova sa World Wide Web konferencije iz 2019, od 13. do 17. maja 2019, San Francisko, SAD, 2019.
- UK Home Office, Online Harms White Paper (samo u Velikoj Britaniji), 2019.
- PA Consulting, Zamršena mreža: preispitivanje pristupa seksualnom iskorištavanju i zlostavljanju djece na internetu, 2019.
- Kancelarija povjerenika za informacije Velike Britanije, Savjetovanje o Kodeksu prakse za zaštitu djece na internetu (samo u Velikoj Britaniji), 2019.
- Globalni fond za zaustavljanje nasilja nad djecom, Narušavanje štete: dokazi za razumijevanje seksualnog iskorištavanja i zlostavljanja djece na internetu, 2019.
- Globalno partnerstvo za zaustavljanje nasilja nad djecom, poziv za akciju Sigurno za učenje, Manifest mladih, 2019.
- UNESCO, Iza brojeva: završetak nasilja i maltretiranja u školama, 2019. (uključuje podatke o štetnom ponašanju na internetu i sajber maltretiranju)
- Ljudska prava Ujedinjenih nacija, dječija prava u odnosu na digitalno okruženje, 2019.
- Australijski povjerenik eSafety, Pregled sigurnosti po dizajnu, 2019.
- UNICEF, Zašto bi preduzeća trebala ulagati u digitalnu sigurnost za djecu - sažetak, 2019.
- Ministarstvo spoljnih poslova SAD-a, Izvještaj o trgovini ljudima, 2019.

2018.

- Globalni savez WeProtect, Globalna procjena prijetnje, 2018.
- Dostojanstvo djece u digitalnom svijetu, izvještaj tehničke radne grupe, 2018. Savjet Evrope, Preporuka CM / Rec (2018) 7 Komiteta ministara državama članicama o smjernicama za poštovanje, zaštitu i ispunjavanje prava djeteta u digitalnom okruženju, 2018.
- Globalni fond za zaustavljanje nasilja nad djecom, Dvogodišnja rješenja za podršku: rezultati ulaganja fonda, 2018.
- Globalni savez WeProtect, Primjeri zemalja koje imaju mogućnosti i koje primjenjuju Model nacionalnog odgovora, 2018.
- INTERPOL and ECPAT International, U susret globalnom pokazatelju o neidentifikovanim žrtvama u materijalu seksualnog iskorištavanja djece, 2018.
- EUROPOL, Procjena prijetnje organizovanim kriminalom putem interneta (IOCTA), 2018.
- NetClean, Izvještaj o sajber kriminalu seksualnog zlostavljanja djece, 2018.

- Međunarodni centar za nestalu i iskorištenu djecu (ICMEC), Materijal seksualnog zlostavljanja djece: Model zakonodavstva i globalni pregled, 9. izdanje, 2018.
- Međunarodni centar za nestalu i iskorištenu djecu (ICMEC), Studije zaštite djece: Seksualno iznuđivanje i pornografija bez pristanka, 2018.
- Međunarodno udruženje internetskih dežurnih linija, Izvještaj INHOPE, 2018.
- Internet Watch Foundation (IWF), Godišnji izvještaj, 2018.
- Thorn, Proizvodnja i aktivno trgovanje slikama seksualnog iskorištavanja djece, 2018.
- ITU, Indeks globalne sajber bezbijednosti, 2018.
- CSA Centar za ekspertize, Intervencije za počinioce seksualnog iskorištavanja djece na Internetu - pregled obima i analiza propusta, 2018.
- NatCen, Ponašanje i karakteristike počinilaca seksualnog iskorištavanja i zlostavljanja djece putem interneta - brza procjena dokaza, 2018.
- UNICEF, Vodič kroz politike o djeci i digitalnoj povezanosti, 2018.

2017

- Nacionalni centar za nestalu i iskorišćenu djecu (NCMEC), Navođenje djece na internetu: dubinska analiza izvještaja CyberTipline, 2017.
- 5Rights Foundation, Digitalno djetinjstvo, razvojne prekretnice u digitalnom okruženju, 2017.
- Childnet, DeShame izvještaj, 2017.
- Kanadski centar za zaštitu djece, Razgovor s preživjelima, 2017.
- Internet Watch Foundation (IWF), Godišnji izvještaj, 2017.
- Međunarodni centar za nestalu i iskorištenu djecu (ICMEC), Godišnji izvještaj, 2017.
- Međunarodni centar za nestalu i iskorištavanu djecu (ICMEC), Vrbovanje djece na internetu u seksualne svrhe: Model zakonodavstva i globalni pregled, 2017.
- Thorn, Internetsko istraživanje seksualnog iznuđivanja sa 2.097 žrtava seksualnog iznuđivanja starosti od 13 do 25 godina, 2017.
- UNICEF, Djeca u digitalnom svijetu, 2017.
- Univerzitet u Zapadnom Sidneju, Mladi i na internetu: Dječiji pogled na život u digitalnom dobu, 2017.
- ECPAT International, Seksualno iskorištavanje djece u jugoistočnoj Aziji, 2017.

2016

- UNICEF, Opasnosti i mogućnosti: odrastanje na internetu, 2016
- UNICEF, Zaštita djece u digitalno doba: Nacionalni odgovori na seksualno iskorištavanje i zlostavljanje djece na internetu u ASEAN-u, 2016.
- Centar za pravdu i prevenciju kriminala, Zaštita djece na internetu u regiji MENA, 2016.
- ECPAT International, Međuagencijska radna grupa za prevenciju seksualnog iskorištavanja djece, Terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i seksualnog zlostavljanja (Luksemburške smjernice), 2016.

2015.

- Globalni savez WePROTECT, Sprečavanje i suzbijanje seksualnog iskorištavanja i zlostavljanja djece (CSEA): Model nacionalnog odgovora, 2015.
- NCMEC, Globalni pejzaž dežurnih linija u borbi protiv materijala seksualnog zlostavljanja djece, 2015
- ITU i UNICEF, *Smjernice za industriju o zaštiti djece na internetu*, 2015.

U vezi sa ljudskim pravima u digitalnom svijetu

- Savjet Evrope, Smjernice za poštovanje, zaštitu i ispunjavanje prava djeteta u digitalnom okruženju, 2018.
- UNESCO, Indikatori univerzalnosti na internetu, 2019.
- Rangiranje digitalnih prava (RDR), 2019 RDR Indeks korporativne odgovornosti, 2019.
- Komisija za širokopojasni pristup za održivi razvoj Stanje širokopojasne mreže, 2019.
- ITU, Mjerenje digitalnog razvoja, 2019.
- ITU, Izvještaj o mjerenju informacijskog društva, 2018.
- UNICEF, Djeca i alati digitalnog marketinga industrije, 2018.
- Komisija za širokopojasni pristup za održivi razvoj, Digitalno zdravlje, 2017.
- Komisija za širokopojasni pristup za održivi razvoj, Digitalne vještine za život i rad, 2017.
- Komisija za širokopojasni pristup za održivi razvoj, Digitalna rodna podjela, 2017.
- UNICEF, Privatnost, zaštita ličnih podataka i ugleda, 2017.
- UNICEF, Sloboda izražavanja, udruživanja, pristupa informacijama i učešća, 2017.
- UNICEF, Pristup internetu i digitalna pismenost, 2017.
- UN CRC, Smjernice o efikasnoj zaštiti djece od seksualnog iskorištavanja, 2019.

Dodatne izvore potražite na dodatnoj listi izvora na www.itu-cop-guidelines.com

Dodatak 1: Terminologija

Definicije u nastavku se uglavnom oslanjaju na postojeće terminologije razrađene u Konvenciji o pravima djeteta, 1989. godine, kao i terminologiju Međuagencijske radne grupe za seksualno iskorištavanje djece u smjernicama o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja, 2016.[64] (Luksemburške smjernice), Konvencije Savjeta Evrope: Zaštita djece od seksualnog iskorištavanja i seksualnog zlostavljanja, 2012.[65], kao i Izvještaj Global Kids Online, 2019.[66]

Adolescenti

Adolescenti su osobe starosti od 10 do 19 godina. Važno je napomenuti da adolescenti nisu obavezujući pojam prema međunarodnom pravu, a oni mlađi od 18 godina smatraju se djecom, dok se 19-godišnjaci smatraju odraslima, osim ako punoljetstvo nije ranije dostignuto prema nacionalnom zakonu[67].

Vještačka inteligencija (AI - artificial ingelligence)

U najširem smislu, izraz se nejasno odnosi na sisteme koji su čista naučna fantastika (tzv. "jaka" vještačka inteligencija u samosvjesnom obliku) i sisteme koji su već operativni i sposobni za izvršavanje vrlo složenih zadataka (prepoznavanje lica ili glasa, vožnja vozila - ovi sistemi su opisani kao „slaba“ ili „umjerena“ vještačka inteligencija)[68].

Sistemi vještačke inteligencije

Sistem vještačke inteligencije je sistem zasnovan na mašini koji može, za dati skup ciljeva koje definiše čovek, davati predviđanja, preporuke ili odluke koje utiču na stvarno ili virtuelno okruženje, a dizajniran je za rad sa različitim nivoima autonomije[69].

Najbolji interes djeteta

Opisuje sve elemente potrebne za donošenje odluke u određenoj situaciji za određeno pojedinačno dijete ili grupu djece[70].

64 “Terminologija Luksemburških smjernica za zaštitu djece od seksualnog iskorištavanja i seksualnog zlostavljanja,” 2016, 114, http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines -396922-EN.pdf.

65 Savjet Evrope, Conseil de l’Europe i Savjet Evrope, Zaštita djece od seksualnog iskorištavanja i seksualnog zlostavljanja: Konvencija Savjeta Evrope (Strazbur: Izdavaštvo Savjeta Evrope, 2012), https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf.

66 Globalkidsonline.net, “Pravilnim korištenjem, upotreba interneta može da poboljša učenje i vještine,” novembar 2019, http:// globalkidsonline.net/synthesis-report-2019/.

67 UNICEF i ITU, Smjernice za industriju o zaštiti djece na internetu (itu.int/cop, 2015.), https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

68 Savjet Evrope, „Šta je vještačka inteligencija?“, Coe.int, Vještačka inteligencija, pristupljeno 16. januara 2020., https://www.coe.int/en/web/artificial-intelligence/what-is-ai.

69 OECD, “Preporuka Savjeta za vještačku inteligenciju” (OECD, 2019), https://webcache .googleusercontent.com/search?q=cache:hTtMv9k1ak8J:https://legalinstruments.oecd.org/api/print %3Fids%3D648%26lang%3Den+&cd=3&hl=en&ct=clnk&gl=ch&client=safari.

70 OHCHR, “Konvencija o pravima djeteta,” pristupljeno 16. januara 2020, https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

Dijete

U skladu sa članom 1. Konvencije o pravima djeteta, dijete je svaka osoba mlađa od 18 godina, osim ako punoljetstvo nije ranije dostignuto prema nacionalnom zakonu[71].

Seksualno iskorištavanje i zlostavljanje djece (CSEA)

Opisuje sve oblike seksualnog iskorištavanja i seksualnog zlostavljanja (CRC, 1989, čl. 34), npr. „(a) podsticanje ili prisiljavanje djeteta da se bavi bilo kojom nezakonitom seksualnom aktivnošću; (b) iskorištavanje djece u prostituciji ili drugim nezakonitim seksualnim postupcima; (c) iskorištavanje djece u pornografskim izvedbama i materijalima“, kao i „seksualni kontakt koji obično uključuje silu nad osobom bez pristanka“. Seksualno iskorištavanje i zlostavljanje djece sve se češće odvija putem interneta ili uz određenu vezu sa internetskim okruženjem[72].

Materijal seksualnog (iskorištavanja i) zlostavljanja djece (CSAM)

Brza evolucija IKT stvorila je nove oblike seksualnog iskorištavanja i zlostavljanja djece na internetu, koji se mogu odvijati virtuelno i ne moraju uključivati fizički sastanak licem u lice sa djetetom[73]. Iako mnoge jurisdikcije slike i videozapise seksualnog zlostavljanja djece još uvijek označavaju kao „dječiju pornografiju“ ili „nepristojne slike djece“, ove će se smjernice na subjekte kolektivno pozivati kao na materijal seksualnog zlostavljanja djece (u daljem tekstu CSAM - child sexual abuse material). To je u skladu sa Smjernicama Komisije za širokopojasni pristup i Modelom nacionalnog odgovora[74] Globalnog saveza WePROTECT. Ovaj termin preciznije opisuje sadržaj. Pornografija se odnosi na legitimnu, komercijalizovanu industriju, a kako Luksemburške smjernice navode upotrebu izraza:

”može (nenamjerno ili ne) doprinijeti smanjenju težine, banalizaciji ili čak legitimizaciji onoga što je zapravo seksualno zlostavljanje i / ili seksualno iskorištavanje djece [...] izraz „dječija pornografija“ rizikuje insinuiranje da se djela izvršavaju uz pristanak djeteta i predstavljaju legitimni seksualni materijal”[75].

Termin CSAM odnosi se na materijal koji predstavlja djela koja su seksualno nasilna i / ili eksploatatorska prema djetetu. To uključuje, ali se ne ograničava na, materijale koji bilježe seksualno zlostavljanje djece od strane odraslih; slike djece uključene u seksualno eksplicitno ponašanje; polne organe djece kada se slike proizvode ili koriste prvenstveno u seksualne svrhe.

71 OHCHR; UNICEF i ITU, *Smjernice za industriju o zaštiti djece na* internetu.
72 “Luksemburške terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i zlostavljanja,”
73 “Luksemburške terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i zlostavljanja”; UNICEF, “Uporedni izvještaj Global Kids Online (2019).”
74 Globalni savez WePROTECT, “Sprječavanje i suzbijanje seksualnog iskorištavanja i zlostavljanja djece (CSEA): Model nacionalnog odgovora.,” 2016, https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/ 582ba50bc534a51764e8a4ec/ 1479255310190/ WePROTECT+G lobal+Alliance+Model+National+Response+Guidance.pdf;
Komisija za širokopojasni pristup, “Child Online Safety: Smanjenje rizika od nasilja, zlostavljanja i iskorištavanja na internetu (2019)."
75 “Luksemburške Terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i zlostavljanja,”

Djeca i mladi

Opisuje sve osobe mlađe od 18 godina, pri čemu djeca, koja se u smjernicama takođe nazivaju i mlađom djecom, obuhvaćaju sve osobe mlađe od 15 godina i mlade ljude od 15 do 18 godina.

Igračke povezane s internetom

Igračke povezane s internetom se povezuju s internetom koristeći tehnologije kao što su Wi-Fi i Bluetooth i obično rade zajedno sa pratećim aplikacijama kako bi djeci omogućile interaktivnu igru. Prema Juniper Research-u, tržište igračaka povezanih s internetom u 2015. dostiglo je 2,8 milijardi američkih dolara , a predviđa se da će se do 2020. povećati na 11 milijardi američkih dolara. Ove igračke prikupljaju i čuvaju lične podatke od dece, uključujući imena, geolokaciju, adrese, fotografije, audio i video zapise[76].

Sajber maltretiranje, koje se naziva i maltretiranje preko interneta

Međunarodno pravo ne definiše sajber maltretiranje. U svrhu ovog dokumenta, sajber maltretiranje opisuje se kao namjeran agresivni čin koji su više puta izvršili ili grupa ili pojedinac koristeći digitalnu tehnologiju i koji je usmjeren na žrtvu koja se ne može lako odbraniti[77]. Obično uključuje „upotrebu digitalne tehnologije i interneta za objavljivanje štetnih informacija o nekome, namjerno dijeljenje privatnih podataka, fotografija ili videozapisa na štetan način, slanje prijetećih ili uvredljivih poruka (putem e-pošte, instant poruka, chata, tekstualnih poruka), širenje glasina i lažnih informacija o žrtvi ili za namjerno isključivanje iz mrežne komunikacije“[78]. Može uključivati direktne (poput chata ili razmjene tekstualnih poruka), polujavne (poput objavljivanja uznemiravajuće poruke na listi e-pošte) ili javne komunikacije (poput stvaranja internet stranice posvećene ismijavanju žrtve).

Sajber mržnja, diskriminacija i nasilni ekstremizam

„Sajber mržnja, diskriminacija i nasilni ekstremizam su posebni oblici sajber nasilja jer ciljaju kolektivni identitet, a ne pojedince […] koji se često odnose na rasu, seksualnu orijentaciju, religiju, nacionalnost ili imigracijski status, pol i politiku“[79].

Digitalno građanstvo

Digitalno građanstvo odnosi se na sposobnost pozitivnog, kritičkog i kompetentnog uključivanja u digitalno okruženje, oslanjajući se na vještine efikasne komunikacije i stvaranja, za vježbanje oblika društvenog učešća koji poštuju ljudska prava i dostojanstvo odgovornom upotrebom tehnologije[80].

76 Jeremy Greenberg, “Opasne igre: igračke povezane sa internetom, COPPA, i loše osiguranje,” Georgetown Law Technology pregled, decembar 4, 2017., https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/.

77 Anna Costanza Baldry, Anna Sorrentino, i David P. Farrington, “Sajber maltretiranje i sajber viktimizacija nasuprot roditeljskog nadzora, praćenja i kontrole aktivnosti adolescenata na internetu,” Pregled usluga za djecu i mlade 96 (januar 2019): 302–7, https://doi.org/10.1016/j.childyouth.2018.11.058.

78) UNICEF, “Global Kids Online uporedni izvještaj (2019)”; ;“Luksemburške terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i zlostavljanja,”

79 UNICEF, “Global Kids Online uporedni izvještaj (2019).”

80 Savjet Evrope, “Digitalno građanstvo i obrazovanje o digitalnom građanstvu,” Obrazovanje o digitalnom građanstvu, pristupljeno 16. januara 2020, https://www.coe.int/en/web/digital-citizenship-education/home.

Digitalna pismenost

Digitalna pismenost znači imati vještine potrebne za život, učenje i rad u društvu u kojem se komunikacija i pristup informacijama sve više odvijaju putem digitalnih tehnologija poput internet platformi, društvenih medija i mobilnih uređaja[81]. Uključuje jasnu komunikaciju, tehničke vještine i kritičko razmišljanje.

Digitalna otpornost

Ovaj pojam opisuje sposobnost djeteta da se emocionalno nosi sa štetama na internetu. Digitalna otpornost je podrazumijevala posjedovanje emocionalnih resursa potrebnih da bi, u trenutku kada shvatimo da je dijete u opasnosti na internetu, znali šta treba da radimo da bi zatražili pomoć, naučili iz iskustva i mogli da se oporavimo kada stvari krenu po zlu[82].

Edukatori

Edukator je osoba koja sistemski radi na poboljšanju razumijevanja druge osobe o datoj temi. Uloga edukatora uključuje i one koji predaju u učionicama i neformalnije edukatore koji, na primjer, koriste platforme i usluge društvenih mreža za pružanje informacija o sigurnosti na internetu ili vode kurseve u zajednici ili školama kako bi djeci i mladima pomogli da budu sigurni na internetu.

Rad edukatora variraće u zavisnosti od konteksta u kojem rade i starosne dobi grupe djece i mladih (ili odraslih) koje žele obrazovati.

Vrbovanje / vrbovanje na internetu

Vrbovanje / vrbovanje na internetu kako je definisano Luksemburškim smjernicama, odnosi se na postupak uspostavljanja / izgradnje odnosa s djetetom bilo lično ili korištenjem interneta ili drugih digitalnih tehnologija radi poticanja na internetu ili seksualnog kontakta na internetu s tom osobom koja nagovara dijete da ima seksualni odnos[83]. Postupak koji za cilj ima da namami djecu na seksualno ponašanje ili razgovore sa ili bez njihovog znanja, ili postupak koji uključuje komunikaciju i socijalizaciju između prestupnika i djeteta s namjerom da ga učini ranjivijim na seksualno zlostavljanje. Pojam vrbovanje nije definisan u međunarodnom pravu; jurisdikcije u nekim državama, uključujući Kanadu, koriste izraz „mamljenje“.

Informacione i komunikacione tehnologije (IKT)

Informacione i komunikacione tehnologije opisuju sve informacione tehnologije koje ističu aspekt komunikacije. Tu uključujemo sve usluge i uređaje koji mogu da se povežu sa internetom, poput računara, laptopa, tableta, pametnih telefona, konzola za igranje, televizora i satova[84]. Dalje se uključuju usluge kao što su radio, kao i između ostalog, širokopojasni internet, mrežni hardver i satelitski sistemi.

---

81 Univerzitet u Zapadnom Sidneju-Claire Urbach, “Šta je digitalna pismenost?,” pristupljeno 16. januara 2020, https:// www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy.

82 Dr. Andrew K. Przybylski, i dr., „Podijeljena odgovornost. Izvještaj o izgradnji dječije otpornosti na internetu” (ParentZone, Univerzitet u Oksfordu i Virgin Media, 2014), https://parentzone.org.uk/sites/default/files/ Building%20Online%20Resilience%20Report.pdf.

83 “Luksemburške terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i zlostavljanja,”

84 UNICEF i ITU, *Smjernice za industriju o zaštiti djece na internetu*.

Internet i povezane tehnologije

Sada je moguće povezati se s internetom pomoću različitih uređaja, npr. pametnih telefona, tableta, konzola za igranje, televizora i laptopa, kao i tradicionalnijih računara. Stoga, osim ako kontekst ne sugeriše drugačije, svako pozivanje na internet treba shvatiti tako da obuhvata sve ove različite metode. Da bi se obuhvatila bogato i složeno tkanje interneta, „internet i povezane tehnologije“, „IKT i internetske industrije“ i „usluge zasnovane na internetu“ koriste se naizmjenično.

Obavještenje i uklanjanje

Korisnici, pripadnici javnosti, organi za sprovođenje zakona ili organizacije sa dežurnim telefonskim linijama ponekad obavijeste operatere i pružaoce usluga o sumnjivom sadržaju na internetu. Obavještenja i postupci uklanjanja odnose se na postupke kompanije za brzo brisanje ('uklanjanje') nezakonitog sadržaja (nezakonit sadržaj definiše se prema nadležnosti) čim su upoznati ('obavijest') sa njegovim prisustvom na njihovim uslugama.

Online igranje

"Online igranje" definiše se kao igranje bilo koje vrste komercijalne digitalne igre u modu za jednog ili više igrača, putem bilo kojeg uređaja povezanog na internet, uključujući namjenske konzole, stone računare, laptope, tablete i mobilne telefone.

„Ekosistem online igranja“ definisan je tako da uključuje gledanje drugih kako igraju video igre putem e-sporta, streaminga ili platformi za razmjenu video zapisa, koje obično pružaju mogućnost gledaocima da komentarišu ili komuniciraju s igračima i ostalim članovima publike[85].

Alati za roditeljsku kontrolu

Softver koji omogućava korisnicima, obično roditelju, da kontrolišu neke ili sve funkcije računara ili drugog uređaja koji se mogu povezati na internet. Takvi programi obično mogu ograničiti pristup određenim vrstama ili klasama internet stranica ili internetskih usluga. Neki takođe pružaju mogućnost upravljanja vremenom, tj. uređaj se može postaviti tako da ima pristup internetu samo između određenih sati. Naprednije verzije mogu snimati sve tekstualne poruke poslane ili primljene sa uređaja. Programi će obično biti zaštićeni lozinkom[86].

Roditelji, njegovatelji, staratelji

Nekoliko internet stranica upućuje na roditelje na generički način (na primjer na „roditeljskoj stranici“ i odnosi se na „roditeljsku kontrolu“). Stoga bi moglo biti korisno definisati ljude koji bi u idealnom slučaju trebali podsticati djecu da maksimalno koriste mogućnosti na internetu, da se staraju da djeca i mladi koriste internet stranice sigurno i odgovorno i daju svoju saglasnost za pristup određenim internet stranicama. U ovom dokumentu pojam „roditelji“ odnosi se na svakoga (isključujući edukatore) ko ima zakonsku odgovornost za dijete. Roditeljska odgovornost će se razlikovati od zemlje do zemlje kao i zakonska roditeljska prava.

85 UNICEF, “Prava djeteta i online igranje: Prilike i izazovi za djecu i industriju,” SERIJA RADOVA ZA DISKUSIJU: Dječja prava i poslovanje u digitalnom svijetu, 2019, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

86 UNICEF i ITU, *Smjernice za industriju o zaštiti djece na internetu*.

Lične informacije

Pojam opisuje informacije o osobi koje se mogu pojedinačno identifikovati i koje se prikupljaju na internetu. One uključuju puno ime i prezime, kontakt podatke poput kućne adrese i adrese e-pošte, brojeve telefona, materijale poput otisaka prstiju ili prepoznavanja lica, brojeve osiguranja ili bilo koji drugi faktor koji omogućava fizičko ili internetsko kontaktiranje ili lokalizaciju osobe. U tom kontekstu se dalje odnose na sve informacije o djetetu i njegovoj okolini koje pružaoci usluga prikupljaju na internetu, uključujući tu i igračke povezane s internetom i internet stvari i bilo koju drugu tehnologiju povezanu s internetom.

Privatnost

Privatnost se često mjeri u smislu dijeljenja ličnih podataka na internetu, posjedovanja javnog profila na društvenim mrežama, dijeljenja informacija s ljudima koje su upoznali na internetu, korištenja podešavanja privatnosti, dijeljenja lozinki s prijateljima, zabrinutosti zbog privatnosti[87].

Seksting

Seksting se obično definiše kao slanje, primanje ili razmjena sopstvenog seksualnog sadržaja, uključujući slike, poruke ili video zapise putem mobilnih telefona i / ili interneta[88]. Stvaranje, distribucija i posjedovanje seksualnih slika djece u većini zemalja je nezakonito. Ako se otkriju seksualne slike djece, odrasli ih ne bi trebali gledati. Dijeljenje seksualnih slika odrasle osobe s djetetom uvijek je krivično djelo i može doći do štete između djece, a možda će biti potrebno prijavljivanje i uklanjanje podijeljenih slika.

Iznuđivanje ili seksualno iznuđivanje djece

Iznuđivanje ili seksualno iznuđivanje (koje se naziva i „seksualna prisila i iznuđivanje na internetu“)[89] opisuje „ucjenjivanje osobe uz pomoć vlastitih slika te osobe kako bi se iznudile seksualne usluge, novac ili druge koristi od nje / njega pod prijetnjom dijeljenja materijala bez pristanka prikazane osobe (npr. objavljivanje slika na društvenim medijima)“[90].

Internet stvari (IoT)

Internet stvari predstavlja sljedeći korak prema digitalizaciji društva i ekonomije, gdje su predmeti i ljudi međusobno povezani komunikacionim mrežama i izvještavaju o svom statusu i / ili okolnom okruženju[91].

URL

Skraćenica za „jedinstveni lokator resursa (uniform resource locator)“, adresa internet stranice[92].

---

87 “Zakon o zaštiti privatnosti djece na internetu,” Pub. L. No. 15 U.S.C. 6501-6505 (1998), https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

88 “Luksemburške terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i zlostavljanja,”

89 Europol, „Seksualna prisila i iznuda putem interneta kao oblik zločina koji pogađa djecu: Perspektiva organa za sprovođenje zakona“ (Evropski centar za borbu protiv sajber kriminala, maj 2017), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

90 “Luksemburške terminološke smjernice za zaštitu djece od seksualnog iskorištavanja i zlostavljanja,”

91 Ntantko, Internet stvari, 1. oktobar 2013, Jedinstveno digitalno tržište - Evropska komisija, https://ec.europa.eu/digital-single-market/en/internet-of-things.

92 UNICEF i ITU, *Smjernice za industriju o zaštiti djece na internetu*.

Virtuelna realnost

Virtuelna realnost je upotreba računarske tehnologije za stvaranje efekta interaktivnog trodimenzionalnog svijeta u kojem objekti stvaraju osjećaj prostorne prisutnosti[93].

Wi-Fi

Wi-Fi (Wireless Fidelity) je grupa tehničkih standarda koji omogućavaju prenos podataka putem bežičnih mreža[94].

93 NASA, "Virtuelna realnost," nas.nasa.gov, pristupljeno 16. januara 2020, https://www.nas.nasa.gov/Software/VWT/ vr.html.
94 Zakon o zaštiti privatnosti djece na internetu.

Dodatak 2: Prekršajni kontakti sa djecom i mladima

Djeca i mladi mogu biti izloženi nizu neželjenih ili neprimjerenih kontakata na internetu koji mogu imati strašne posljedice za njih. Neki od ovih kontakata mogu biti seksualne prirode.

Studije su pokazale da je 22% djece maltretirano[95], uznemiravano ili proganjano na internetu; 24% je dobilo neželjene seksualne komentare;[96] 8% je u stvarnom životu upoznalo ljude koje su prije poznavali samo putem interneta[97]. Iako se procenti razlikuju u zavisnosti od zemlje i regije, ove brojke pokazuju da su rizici stvarni[98]. Jedno istraživanje o internetu u Sjedinjenim Američkim Državama[99] pokazalo je da je 32% tinejdžera na internetu kontaktirao potpuno nepoznati čovjek, od kojih je 23% reklo da su se osjećali uplašeno i nelagodno tokom kontakta; a 4% je dobilo agresivno seksualno podsticanje.

Seksualni predatori koriste internet za kontaktiranje djece i mladih u seksualne svrhe, često koristeći tehniku poznatu kao vrbovanje kojom djetetovo povjerenje stiču pozivajući se na njegove interese. Često uvode seksualne teme, fotografije i eksplicitne izraze kako bi desenzibilizovali, podigli seksualnu svijest i ublažili volju svojih mladih žrtava. Pokloni, novac, pa čak i karte za prevoz se koriste za nagovaranje i namamljivanje djeteta ili mlade osobe na mjesto gdje ga predator može seksualno iskorištavati. Ovi susreti se mogu čak fotografisati ili snimiti kao video snimak. Djeci i mladima često nedostaje emocionalna zrelost i samopoštovanje, što ih čini podložnim manipulacijama i zastrašivanju. Oni se takođe ustručavaju reći odraslima o svojim susretima iz straha od srama ili gubitka pristupa internetu. U nekim slučajevima im prijete predatori i kažu da vezu drže u tajnosti. Seksualni predatori takođe uče jedni od drugih putem internetskih foruma i chat soba.

95 U-report (2019), http://www.ureport.in/v2/.
96 Projekat deSHAME (2017), https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf.
97 Lenhardt, A., Anderson, M., Smith, A. (2015), Tinejdžeri, tehnologija i romantične veze, https://www.pewresearch.org/internet/2015/10/01/teens-technology-and-romantic-relationships/
98 Livingstone, S., Haddon, L., Görzig, A., i Ólafsson, K. (2011). *Rizici i sigurnost na internetu: Perspektiva evropske djece*. Potpuni nalazi. LSE, London: EU Kids Online, http://eprints.lse.ac.uk/33731/.
99 Amanda Lenhart i dr., „Korištenje društvenih medija stiče veće uporište u tinejdžerskom životu dok prihvataju konverzacionu prirodu interaktivnih internetskih medija.“, Pew internet i američki životni projekt, 2007,44,https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf.

Dodatak 3: Globalni savez WeProtect

WePROTECT Model nacionalnog odgovora

Strategija WePROTECT Globalnog saveza podržava zemlje da razviju koordinisane odgovore više interesnih strana za borbu protiv seksualnog iskorištavanja djece na internetu, vođene svojim Modelima nacionalnog odgovora (MNR). Model nacionalnog odgovora Globalnog saveza WePROTECT djeluje kao nacrt za nacionalnu akciju. Pruža okvir za zemlje na koji bi se trebale osloniti da se pozabave seksualnim iskorištavanjem djece na internetu (OCSE). Model je namijenjen da pomogne zemlji da:

- procijeni trenutni odgovor na seksualno iskorištavanje djece na internetu i identifikuje nedostatke;
- da prioritet nacionalnim naporima pri popunjavanju praznina;
- poboljša međunarodno razumijevanje i saradnju.

Model ne teži propisivanju aktivnosti ili postavljanju jedinstvenog pristupa. Njegova svrha je opisati sposobnosti potrebne za efikasnu zaštitu djece i pružiti podršku zemljama da razviju ili poboljšaju svoje postojeće sposobnosti. Takođe navodi niz mogućnosti koje će, ako postoje i budu efikasne, ubrzati i poboljšati ishode. Model nacionalnog odgovora uključuje dvadeset i jednu sposobnost, podijeljenu u šest odjeljaka: politika i upravljanje, krivično pravosuđe, žrtve, društvo, industrija i mediji i komunikacije. Globalni savez WePROTECT vjeruje da će djelovanje u svih šest područja pružiti potpun nacionalni odgovor na ovaj zločin.

Model će omogućiti zemlji - bez obzira na polaznu tačku - da identifikuje sve propuste u mogućnostima i započne planiranje da popravi te propuste. Iako će države razvijati vlastite individualne pristupe, čineći to u kontekstu zajednički dogovorenog okvira i razumijevanja sposobnosti, postoji nada da se komunikacija i saradnja među interesnim stranama na nacionalnom i međunarodnom nivou mogu dalje poboljšati.

WePROTECT globalni strateški odgovor

Globalni strateški odgovor (GSR) WePROTECT Globalnog saveza koordinisani je pristup borbi protiv seksualnog iskorištavanja djece na internetu koji uključuje veći globalni uvid, međunarodno usklađivanje nacionalnih pristupa i globalna rješenja koja prelaze nacionalni odgovor. Globalni strateški odgovor je u osnovi prateći dio Modela nacionalnog odgovora (MNR); dok je Model nacionalnog odgovora usredotočen na sposobnosti potrebne za rješavanje seksualnog iskorištavanja djece na internetu na nacionalnom nivou, globalni strateški odgovor je usredotočen na prioritetna područja za međunarodnu saradnju i izgradnju kapaciteta.

Globalni strateški odgovor uključuje šest tematskih područja, sa povezanim potrebnim mogućnostima i očekivanim ishodima za svako područje, kao i partnere koji bi trebali raditi zajedno preko granice kako bi ih ostvarili.

Politika i zakonodavstvo

Razvijanje političke volje za djelovanjem i zakonodavstva za efikasno usklađivanje pristupa krivičnim djelima kao rezultat će imati obnovu posvećenosti na visokom nivou na nacionalnom i međunarodnom nivou za borbu protiv seksualnog iskorištavanja djece na internetu.

Krivična pravda

Razmjena informacija, uključujući zajednički pristup međunarodnim bazama podataka putem formalnih okvira za razmjenu podataka, u kombinaciji sa posvećenim, obučenim službenicima i tužiocima sa iskustvom u seksualnom iskorištavanju djece na internetu najbolji su način za otkrivanje, progon i privođenje prestupnika, uključujući i uspješne zajedničke istrage i osuđujuće presude.

Uticaj na žrtve i usluge

Efikasna i pravovremena podrška žrtvama, uključujući zaštitu njihovog identiteta i davanje mogućnosti da pričaju, pomaže u tome da se osigura da žrtve imaju pristup podršci koja im je potrebna u trenutku kada im je potrebna.

Tehnologija

Korištenje tehničkih rješenja, uključujući vještačku inteligenciju, za otkrivanje, blokiranje i sprečavanje štetnih materijala, striminga uživo i vrbovanja na internetu, što mora uključiti širok i dosljedan rad tehnološkog sektora, omogućit će tim platformama da izbjegnu da se koriste kao alat za seksualno iskorištavanje djece na internetu.

Društvo

Postoje brojne mogućnosti koje zajednički djeluju u širem društvu kako bi osnažile djecu da se zaštite od seksualnog iskorištavanja djece na internetu, bez obzira gdje žive. Osiguravanjem da je razvoj digitalne kulture sigurniji po dizajnu (tj. ima ugrađene sigurnosne funkcije) i da postoji etičan i dosljedan pristup prijavljivanja medija, izloženost nezakonitim sadržajima na internetu biće ograničena. U međuvremenu, obrazovanje i informisanje djece i roditelja, staratelja i stručnjaka i ciljane intervencije za prestupnike, sve rade na sprječavanju ili smanjivanju pojave seksualnog iskorištavanja djece na internetu.

Istraživanje i uvid

Konačno, procjene prijetnji (poput Globalne procjene prijetnje 2019), istraživanja prestupnika i rad na razumijevanju dugotrajnih trauma žrtava pružit će vladi, organima za sprovođenje zakona, civilnom društvu, akademskoj zajednici i industriji jasno razumijevanje najnovijih prijetnji.

Dodatak 4: Primjeri odgovora na štete na internetu

Ovdje uključene primjere sastavili su autori smjernica ITU-a za donošenje politika i njihovi saradnici.

Obrazovanje djece o štetama na internetu

BBC-jeva Own IT aplikacija – aplikacija za očuvanje sigurnosti namijenjena djeci od 8 do 13 godina koja dobijaju prvi pametni telefon. Kombinujući najsavremeniju tehnologiju mašinskog učenja za praćenje dječijih aktivnosti na pametnom telefonu sa mogućnošću da djeca samostalno prijavljuju svoje emocionalno stanje, koristi ove informacije za pružanje prilagođenih sadržaja i intervencija koji djeci pomažu da ostanu sretna i sigurna na internetu.

Aplikacija sadrži posebno dopušten sadržaj sa BBC-a, 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, pomažući mladim ljudima i roditeljima da konstruktivnije razgovaraju o svojim iskustvima na internetu. Aplikacija ne prikuplja nikakve lične podatke ili sadržaj generisan od korisnika dok se cijelo mašinsko učenje odvija u aplikaciji / na uređaju korisnika.

Project Evolve - Obrazovni okvir za razvijanje digitalnih sposobnosti s potpunim resursima, koji identifikuje digitalne vještine za svako pojedinačno dijete različitog uzrasta kako bi pomogao roditeljima i nastavnicima da shvate sposobnosti koje bi njihova djeca trebala imati, zajedno sa resursima i aktivnostima koje će im razviti određene vještine.

360 degree safe – alat na internetu za samostalni pregled za škole u razmatranju i ocjenjivanju njihovih cjelokupnih internetskih sigurnosnih odredbi koji pruža smjernice i podršku za dobijanje definisanih standarda.

DQ Institute - Podaci su prikupljeni od 145 426 djece i adolescenata u 30 zemalja od 2017. do 2019. godine kao dio #DQEveryChild, globalnog pokreta za digitalno građanstvo zagovaranog od strane DQ Instituta, koji je pokrenut u Singapuru uz podršku Singtela i brzo se proširio u saradnji sa Svjetskim ekonomskim forumom da bi uključio preko 100 partnerskih organizacija. Cilj ovog pokreta bio je osnažiti djecu sa sveobuhvatnim sposobnostima za digitalno građanstvo od početka njihovog digitalnog života, koristeći online program obrazovanja i ocjenjivanja DQ World. Podaci iz ovog pokreta korišteni su za izradu indeksa sigurnosti djece na internetu 2020 (COSI). Okvir za COSI procjenjuje i rangira sigurnost djece na internetu u 30 zemalja na osnovu 24 područja koja su grupisana u šest stubova koji utiču na sigurnost djece na internetu.

DQ Pro paket za porodičnu spremnost i DQ World pružaju mogućnosti roditeljima da procijene digitalnu spremnost svog djeteta i kroz obrazovne materijale poboljšaju digitalne sposobnosti kao što su digitalno državljanstvo, upravljanje vremenom ekrana, upravljanje sajber zlostavljanjem, upravljanje sistemom sajber sigurnosti, digitalna empatija, upravljanje digitalnim otiskom, kritičko razmišljanje i upravljanje privatnošću.

Australijski eSafety Toolkit za škole skup je resursa dizajniranih da podrže škole u stvaranju sigurnijeg internetskog okruženja. Ovaj alat odražava višestrani pristup obrazovanju o sigurnosti na internetu i podijeljen je u četiri elementa s resursima koji:

- pripremaju škole za procjenu njihove spremnosti za rješavanje problema sigurnosti na internetu i daje prijedloge za poboljšanje njihovih trenutnih praksi;
- uključuju cijelu školsku zajednicu da bude posvećena i uključena u stvaranje sigurnog internetskog okruženja;
- edukuju ističući najbolju praksu u obrazovanju o sigurnosti na internetu i podržavaju škole u razvoju internetskih sigurnosnih sposobnosti školske zajednice;
- efikasno odgovaraju na incidente, istovremeno podržavajući sigurnost i blagostanje.

Edukativna kampanja Kancelarije za elektronske komunikacije Poljske-UKE I Click Sensible edukuje djecu i roditelje o tome kako biti sigurniji na internetu i kako prepoznati i upravljati rizikom.

ChildFund iz Vijetnama osnovao je inicijativu Swipe Safe. Ovaj program edukuje djecu o potencijalnim rizicima na internetu, poput sajber prevara, maltretiranja ili seksualnog zlostavljanja, i daje savjete o načinima kako da budu sigurna.

Izvještaj Komisije za širokopojasni pristup o Tehnologiji, širokopojasnom pristupu i obrazovanju: program unapređenja obrazovanja za sve , 2013.

Iskustva djece na internetu: Izgradnja globalnog razumijevanja i djelovanja, UNICEF, 2019.

Istraživanje Global Kids Online uključuje mnoštvo informacija o odgovorima dobre prakse na štete na internetu.

Primjeri angažovane industrije

Australijski povjerenik eSafety gradi snažna partnerstva i sarađuje s industrijom kako bi omogućio svim Australcima da imaju sigurnija, pozitivnija iskustva na internetu. Primjer je rad eSafety na sigurnosti po dizajnu. Kao dio inicijative, eSafety je proveo detaljan proces savjetovanja s industrijom, trgovinskim tijelima i organizacijama odgovornim za zaštitu korisnika, kao i roditeljima, starateljima i mladima. Inicijativa Sigurnost po dizajnu dizajnirana je da podstakne i pomogne industriji da osigura da je sigurnost korisnika ugrađena u samom dizajnu, razvoju i primjeni internetskih usluga i platformi. eSafety takođe propisuje tri postavke prijavljivanja i prigovora: postavke prijavljivanja sajber nasilja, postavke prijavljivanja zloupotrebe zasnovane na slikama i postavke prijavljivanja internetskog sadržaja. eSafety može formalno narediti određenim provajderima internetskih usluga da uklone sadržaj sa njihovih usluga. Iako ove postavke u velikoj mjeri djeluju kao model saradnje između vlade i industrije, ovlaštenja koja eSafety ima na raspolaganju da prisili na uklanjanje materijala pružaju kritičnu sigurnosnu mrežu i tjeraju industriju da bude proaktivna u rješavanju štete na internetu.

Kompanija Telia preuzima odgovornost da razumije i upravlja negativnim uticajima povezivanja i da bude potpuno transparentna i odgovorna na nivou odbora. Takođe im je stalo do djece i mladih jer priznaju da su oni aktivni korisnici njihovih usluga.

Kancelarija za elektronske komunikacije Poljske-UKE uključuje civilno društvo i djecu u njihove kampanje propagiranja kako bi shvatili šta potpisuju na internetu.

The Internet Watch Foundation je partnerska organizacija koja okuplja industriju, vladu, organe za sprovođenje zakona i nevladine organizacije kako bi eliminisala seksualno zlostavljanje djece. U 2020. IWF je imala 152 člana na različitim platformama i infrastrukturnim

usluagma i nudi članovima čitav niz usluga kako bi se spriječilo širenje kriminalnih slika na njihovim platformama.

Pokrivenost zakonodavstvom

Izraziti političku volju za davanje prioriteta zaštiti djece na internetu potpisivanjem Univerzalne deklaracije o sigurnosti djece na internetu (Komisija za širokopojasni pristup).

Regulativa

Out of the Shadows: objašnjavanje odgovora na indeks seksualnog zlostavljanja i iskorištavanja djece (2019) od strane The Economist Intelligence Unit jedini je alat za ocjenjivanje koji analizira odgovor zemalja na seksualno zlostavljanje i iskorištavanje djece, uključujući digitalni prostor i odgovor IKT industrije na ovaj problem.

Identifikacija zlostavljanja djece putem interneta

Slijede primjeri dobre prakse u identifikovanju zlostavljanja djece na internetu.

INHOPE: Mreža INHOPE osnovana je 1999. godine za borbu protiv materijala seksualnog zlostavljanja djece na internetu kao odgovor na zajedničku viziju interneta bez materijala seksualnog zlostavljanja djece. U proteklih 20 godina, INHOPE je narastao kako bi se uspješno borio protiv rasta, geografskog širenja i surovosti materijala seksualnog zlostavljanja djece na internetu. Danas dežurne telefonske linije INHOPE-a rade na terenu na svim kontinentima, primaju izvještaje i brzo uklanjaju materijal seksualnog zlostavljanja djece s interneta i dijele podatke sa organima za sprovođenje zakona.

Microsoft PhotoDNA kreira heševe slika i upoređuje ih sa bazom podataka hešova koji su već identifikovani i za koje je potvrđeno da su materijal seksualnog zlostavljanja djece. Ako pronađe podudaranje, slika se blokira. Međutim, ovaj alat ne koristi tehnologiju prepoznavanja lica niti može identifikovati osobu ili predmet na slici. Ali, sa pojavom PhotoDNA for Video stvari su poprimile novi zaokret.

PhotoDNA for Video rastavlja video u ključne kadrove i u osnovi stvara hešove za te snimke ekrana. Na isti način na koji PhotoDNA može pronaći podudaranje sa slikom koja je izmijenjena kako bi se izbjeglo otkrivanje, PhotoDNA for Video može pronaći sadržaj seksualnog iskorištavanja djece koji je uređen ili spojen u videozapis koji bi u protivnom mogao izgledati bezazlen.

Microsoft je objavio novi alat za prepoznavanje dječijih predatora koji u chatovima na internetu vrbuju djecu zbog zlostavljanja. Projekat Artemis, razvijen u saradnji s The Meet Group, Robloxom, Kik i Thornom, nadovezuje se na Microsoftovu patentiranu tehnologiju i putem Thorna će biti dostupan besplatno internetskim kompanijama koje nude funkciju chata. Projekat Artemis je tehnički alat koji daje upozorenja administratorima kada je potrebno bilo kakvo poduzimanje mjera u chat sobama. Ova tehnika otkrivanja vrbovanja moći će otkriti, locirati i prijaviti predatore koji pokušavaju namamiti djecu u seksualne svrhe.

Thorn je razvio oglase za odvraćanje namijenjene onima koji traže materijal seksualnog zlostavljanja djece, a koji su u periodu od tri godine poslani milionima puta preko četiri pretraživača. Pored toga, oglasi su zabilježili stopu učestanosti klikova 3% od strane ljudi koji traže pomoć nakon pretraživanja eksploatatorskog materijala.

Safer od kompanije Thorn, je alat koji se može upotrijebiti direktno na platformi privatne kompanije za identifikovanje, uklanjanje i prijavljivanje materijala seksualnog zlostavljanja djece.

Thorn Spotlight, softver koji daje organima za sprovođenje zakona u svih 50 država Sjedinjenih Američkih Država i Kanade mogućnost da ubrzaju identifikaciju žrtava i skrate vrijeme istrage za više od 60%.

Geebo, povjerljivi sajt posvećen tome da seksualno iskorištavanje drži van svoje platforme, nikada nije imao slučajeve seksualnog iskorištavanja djece. Uspijevaju u tome djelomično zbog svog postupka prethodnog pregleda.

Google AI klasifikator može se koristiti za otkrivanje materijala seksualnog zlostavljanja djece na mrežama, uslugama i platformama. Ovaj alat je dostupan besplatno putem Google API-ja za sigurnost sadržaja, koji je skup alata koji povećava kapacitet za pregled sadržaja na takav način da zahtijeva da mu bude izloženo manje ljudi. Ovaj alat bi pomogao ljudskim stručnjacima da pregledaju materijal u još većem obimu i idu u korak sa prestupnicima, ciljajući slike koje prethodno nisu bile označene kao nezakoniti materijali. Dijeljenje ove tehnologije ubrzalo bi identifikaciju slika.

Google je 2015. proširio svoj rad na hešovima uvođenjem jedinstvene tehnologije prepoznavanja otisaka prstiju i podudaranja za videozapise na YouTubeu, koji skeniraju i prepoznaju učitane videozapise koji sadrže poznati materijal seksualnog zlostavljanja djece.

Tokom Hackathona za zaštitu djece 2019. Facebook je najavio dvije tehnologije otvorenog koda koje otkrivaju identične i gotovo identične fotografije i video zapise. Ova dva algoritma su dostupna u GitHub-u koji omogućava sistemima za razmjenu heša da međusobno razgovaraju, čineći sisteme mnogo snažnijim.

Dežurna telefonska linija IWF-a ostaje neprestano aktivna, ne samo prateći hiljade izvještaja pripadnika javnosti, koji su možda nabasali na slike seksualnog zlostavljanja djece na internetu, već i obavljajući jedinstvenu proaktivnu ulogu u traženju ovog nezakonitog sadržaja na internetu. Omogućavanjem dežurnih telefonskih telefonskih linija da koriste svoje informacije i fokusiraju resurse, može se identifikovati i ukloniti više sadržaja. Štaviše, IWF neprekidno sarađuje s Googleom, Microsoftom, Facebookom i drugim kompanijama unutar svog članstva kako bi neprestano pomjerao tehničke granice. IWF nudi rješenje Portal za prijavljivanje koji omogućava korisnicima interneta u zemljama i nacijama bez dežurnih telefonskih linija da prijave slike i video zapise za sumnju na seksualno zlostavljanje djece direktno IWF-u putem posebne internetske stranice na portalu.

IWF u suradnji sa dobrotvornom organizacijom za podršku žrtvama Marie Collins Foundation želi stvoriti novu kampanju u kojoj poziva mladiće da prijave sve seksualne slike ili video zapise djece mlađe od 18 godina koje su napravili sami na koje mogu naletjeti tokom pretraživanja na internetu.

Interpol je stvorio bazu slika i video zapisa o međunarodnom seksualnom iskorištavanju djece (ICSE), koja je obavještajno i istražno sredstvo, omogućavajući specijalizovanim istražiteljima iz više od 50 zemalja da dijele podatke o slučajevima seksualnog zlostavljanja djece. Analizirajući digitalni, vizuelni i audio sadržaj fotografija i video zapisa, stručnjaci za identifikaciju žrtava mogu pronaći tragove, prepoznati svako preklapanje slučajeva i udružiti napore u pronalaženju žrtava seksualnog zlostavljanja djece. Trenutno Interpolova baza podataka o seksualnom iskorištavanju djece sadrži više od 1,5 miliona slika i video zapisa i pomogla je u identifikovanju 19 400 žrtava širom svijeta.

NetClean ProActive je softver zasnovan na podudaranju obilježja i drugim algoritmima za otkrivanje koji automatski otkriva slike i video zapise seksualnog zlostavljanja djece u poslovnim okruženjima.

Griffeye Brain koristi vještačku inteligenciju za skeniranje ranije neklasifikovanog sadržaja, upoređivanje sa osobinama poznatog sadržaja materijala seksualnog zlostavljanja djece i označavanje sumnjivih stavki radi pregleda od strane agenta.

RAINN je stvorio i upravlja Nacionalnom dežurnom telefonskom linijom za seksualno nasilje u partnerstvu s više od 1 000 lokalnih pružalaca usluga prijavljivanja seksualnog zlostavljanja širom zemlje i vodi sigurnosnu liniju za pomoć Ministarstva odbrane za Ministarstvo odbrane. RAINN također vodi programe za sprečavanje seksualnog nasilja, pomoć preživjelima i osiguravanje da počinioci budu izvedeni pred lice pravde.

Safehorizon je neprofitna organizacija za pomoć žrtvama koja stoji uz žrtve nasilja i zlostavljanja u Njujorku od 1978. Safehorizon nudi usluge dežurnih telefonskih linija za žrtve nasilja.

Projekat Arachnid je inovativni alat kojim upravlja Kanadski centar, projekat Arachnid koristi se za borbu protiv rastuće proliferacije materijala seksualnog zlostavljanja djece (CSAM) na internetu.

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

With the support of:

Međunarodna telekomunikaciona unija

Place des Nations
CH-1211 Geneva
20
Switzerland

ISBN: 978-92-61-30451-5

Objavljeno u Švajcarskoj
Ženeva,
2020 Fotografije:
Shutterstock