Julio Cesar Aviles /Save the Children

DIGITALNA ZAŠTITA DJECE U POKRETU I RASELJENE DJECE

Save the Children

Pregled aktuelnog konteksta i trendova, potencijalnih rizika i praktičnih narednih koraka

Inicijativa za migrante i raseljene organizacije Save the Children

Farjana Sultana / Save the Children

Zahvale

Autorica zahvaljuje Steveu Morganu, Josiahu Kaplanu, Ilani Tyler-Rubinstein i Madeleine Maxwell-Hart iz Inicijative za migrante i raseljene organizacije Save the Children na savjetima i doprinosima tokom cijelog procesa istraživanja. Dodatnu zahvalnost duguje organizaciji Save the Children u Danskoj koja je naručila ovaj izvještaj i organizaciji Danida pri Ministarstvu vanjskih poslova Danske čijim je sredstvima finansiran rad na istraživanju.
Također hvala osoblju iz ureda organizacije Save the Children u Libanu, Etiopiji, El Salvadoru, na Balkanu, u Afganistanu, Ujedinjenom Kraljevstvu, Norveškoj, Danskoj, SAD-u i Švicarskoj na tome što su dijelili svoja iskustva i znanja o uticaju digitalnog programiranja na djecu u pokretu i raseljenu djecu.

Zahvalnost dugujem i vanjskim agencijama, uključujući UNHCR, OCHA, UNICEF, The Engine Room, GovLab Univerziteta u New Yorku, Univerzitet Yale, ChildFund, World Vision i InterAction, zato što su podijelile svoje uvide, kao i svima koji su davali savjete i ustupili nalaze istraživanja o upotrebi digitalnih tehnologija u izradi programa za djecu u pokretu i raseljenu djecu.

Posebno zahvaljujemo članovima upravne grupe projekta: Arij Boureslan, Menaca Calyaneratne, Albert Den Boogert, Susan Grant, Sofyen Khalfaoui, Alice Moltke Ladekarl, Hannah Newth i Dominiek Vangaever.

Istraživačica i glavna autorica: Linda Raftree
Urednice teksta: Lisa Findley i Nicola Kiess
Grafički dizajn: John McGill

MINISTRY OF FOREIGN AFFAIRS OF DENMARK
Danida

Sadržaj

Skraćenice i akronimi

CDR	Evidencija podataka o pozivima
COPPA	Zakon o privatnosti i zaštiti djece na internetu
DNA	Deoksiribonukleinska kiselina
EU	Evropska unija
FBI	Federalni biro za istrage
GDPR	Opća uredba o zaštiti podataka
GPS	Globalni pozicioni sistem
GSMA	Globalni sistem za mobilnu komunikcaiju
HHI	Harvard Humanitarian Initiative
HIF	Humanitarian Innovation Fund
HIV	Virus humane imunodeficijencije
ICE	Agencija za imigraciju i carinu
ICRC	Međunarodni komitet Crvenog krsta
IFRC	Međunarodna federacija društava Crvenog krsta i Crvenog polumjeseca
ICT	Informacijske i komunikacijske tehnologije
ID	Identifikacijska isprava
IOM	Međunarodna organizacija za migracije
IT	Informacijske tehnologije
ITU	Međunarodna telekomunikacijska unija
LGBTQI	Lezbejke, gay, biseksualne, transrodne, queer i interseksualne osobe
MDI	Inicijativa za migrante i raseljene (organizacije Save the Children)
M&E	Praćenje i evaluacija
(M)NVO	Međunarodna) nevladina organizacija
OCHA	Ured Ujedinjenih nacija za koordinaciju humanitarnih poslova
PIM	Protection Information Management
RD4C	Responsible Data for Children
RIL	Response Innovation Lab
UAVs	Bespilotne letjelice
UK	Ujedinjeno Kraljevstvo
UN	Ujedinjene nacije
UNCTAD	Konferencija Ujedinjenih nacija o trgovini i razvoju
UNDG	Grupa Ujedinjenih nacija za razvoj
UNHCR	Visoki komesar Ujedinjenih nacija za izbjeglice
UNICEF	Međunarodni fond Ujedinjenih nacija za djecu
UNODC	Ured Ujedinjenih nacija za borbu protiv droge i kriminala
US	Sjedinjene Države
WFP	Svjetski program za hranu

Definiranje digitalne tehnologije i inovacija

U ovom izvještaju termine digitalna tehnologija, inovacije, alati i pristupi koristimo u širem smislu za:

- upotrebu mobilnih uređaja kao što su telefoni ili tableti;
- prikupljanje i korištenje digitalnih podataka;
- globalne pozicione sisteme (GPS) i senzore;
- biometriju (npr. digitalne otiske prstiju, skeniranje rožnice i prepoznavanje lica);
- velike podatke i povezane pristupe (npr. analitiku podataka, vještačku inteligenciju, mašinsko učenje, duboko učenje, analizu raspoloženja i prediktivnu analitiku);
- platforme društvenih medija i s njima povezane sadržaje i
- druge alate, platforme, aplikacije i pristupe za čije funkcioniranje su potrebni mobilni podaci, internet, digitalni podaci ili napredni računarski kapacitet.

PREDGOVOR

Marieke van der Velden / Save the Children

Procjenjuje se da je 34 miliona djece i mladih prisilno raseljeno1 , a još toliko ih je u pokretu u potrazi za ekonomskim i obrazovnim mogućnostima. Digitalna povezanost, digitalni podaci i nove tehnologije mijenjaju načine na koje se raseljene osobe informiraju, kako pristupaju informacijama i kako komuniciraju, kao i kako agencije provode i upravljaju svojim programima i kako mjere njihov učinak.

Humanitarne organizacije sve više se oslanjaju na podatke i nove tehnologije kako bi unaprijedile svoj doseg i pomogle ugroženim populacijama do kojih je teško doći, uključujući i djecu u pokretu. Aktuelna pandemija bolesti COVID-19 ubrzala je potrebu humanitarnog sektora za izradom digitalnih rješenja koja će pružiti podršku ugroženim populacijama, uključujući djecu migrante i raseljenu djecu. Međutim, povećana povezanost među ovim populacijama nosi sa sobom i potencijalno povećanje rizika. Rapidno uvođenje tehnoloških inovacija, s kojim nacionalna zakonodavstva muku muče da održe korak, donosi nove etičke dileme i prijetnje po sigurnost i dobrobit raseljene djece.

Inicijativa za migrante i raseljene (MDI) organizacije Save the Children također je inovativna i između ostalog radi na alatima koji se oslanjaju na nove tehnologije, a koji će omogućiti bezbjedniji i učinkovitiji odgovor u svrhu pružanja podrške najugroženijoj djeci u pokretu. Primjer jednog takvog alata je prediktivna raseljenost – prototip za predviđanje budućeg opsega i trajanja kriza raseljenosti prouzrokovanih sukobima. Kako bi nadopunio takve napore, MDI je istovremeno naručio ovaj izvještaj za potrebe unapređenja rada organizacije Save the Children na zaštiti djece u situacijama kada se digitalne tehnologije 'ukrštaju' s kontekstima migracije i raseljenosti.

Izvještaj o digitalnoj zaštiti za djecu prati preporuke iz studije MDI i organizacije Save the Children Danska o "Raseljenoj djeci i novim tehnologijama"2, a također se osvrće i na relevantne preporuke iz Globalnog izvještaja o reviziji organizacije Save the Children iz 2016. godine. Pouke iz ovog izvještaja poduprijet će izgradnju kapaciteta unutar organizacije Save the Children za potrebe odgovorne primjene tehnologije u svrhu izrade programa za djecu i mlade u kontekstu migracija i raseljenosti, a istovremeno će pružiti značajan i blagovremen doprinos razvoju dobre prakse o digitalnoj zaštiti za djecu u cijelom sektoru. Očekujemo da će sekundarna faza ovog istraživanja 2021. godine podržati izradu smjernica i alata za podršku donošenju odluka koji će organizaciji i cijelom sektoru ponuditi neophodne instrumente digitalne zaštite za djecu i doprinijeti široj agendi digitalne transformacije.

Podaci i tehnološke inovacije nisu "neprijatelji" – oni nude izvrsne i prijeko potrebne kapacitete za pozitivne i transformativne promjene u našem sektoru. Ipak, kako se obim i uticaj tehnologije bude povećavao, tako će akteri u humanitarnom sektoru morati biti opremljeni odgovarajućim mehanizmima digitalne zaštite kako ne bi nanijeli štetu upravo onoj djeci kojoj nastoje pružiti sigurnost i kako bi smanjili sve eventualne pravne rizike i rizike za svoj ugled. Također, u sve većem oslanjanju na digitalne tehnologije ne trebamo zapostaviti one koji nemaju pristupa. Sve češće vidimo primjere gdje dolazimo u opasnost da ćemo doprinijeti "digitalnom jazu" tako što će programi zasnovani na velikim podacima i tehnologiji previdjeti one koji nemaju pristup povezivanju. Humanitarni sektor mora se čim prije suočiti sa izazovom pronalaženja načina na koji ćemo kolektivno i učinkovito prebroditi ovo mnoštvo izazova, a da pritom ne odbacimo mogućnosti koje nam nude tehnološke inovacije. Stoga se nadam da će ovaj izvještaj i praktičarima i donositeljima politika pomoći u sagledavanju tog izazova i ohrabriti ih da bez odlaganja "digitalnoj zaštiti" daju prioritet.

Steve Morgan
Direktor
Inicijativa za migrante i raseljene
Save the Children International

CJ Clarke / Save the Children

Sierra Leone Country Office

IZVRŠNI SAŽETAK

Potencijal za digitalnu transformaciju izrade programa

Procjenjuje se da je 34 miliona djece širom svijeta prisilno raseljeno iz svojih domova3, a ovaj broj je iz godine u godinu sve veći. Digitalne tehnologije imaju potencijal za transformaciju izrade programa sa djecom migrantima i raseljenom djecom tako što će umnogome olakšati dopiranje do populacija u pokretu i pružanje pomoći i tako što će povećati učinkovitost i potaknuti unapređenje kvaliteta programa, a zahvaljujući tome će Save the Children i druge agencije moći ostvariti bolji učinak za najugroženije kategorije djece na svijetu.

Ipak, rapidne digitalne promjene predstavljaju izazov za sektor ograničenih kapaciteta i resursa, kao i rizik i prijetnju za sigurnost i dobrobit raseljene djece. Djeca koja su ranjiva offline najvjerovatnije će biti ranjiva i online, a to se posebno odnosi na djevojčice, LGBTQI mlade, djecu migrante i raseljenu djecu. Pandemija bolesti COVID-19 također je naglasila i izazove koji prate u potpunosti digitalni pristup. Uprkos sve većoj digitalnoj povezanosti, neke raseljene populacije još uvijek nemaju pristupa uređajima, a mnogi od njih su nepovjerljivi prema agencijama koje prikupljaju i koriste njihove podatke, što može dovesti do isključivanja – ili samo-isključivanja – djece koja bi imala najviše koristi od digitalnih programa.

Da bi ovaj sektor uspješno iskoristio izuzetno pozitivne i transformativne potencijale novih tehnologija, od suštinske je važnosti da izradimo i u naš rad ugradimo smjernice i politike o digitalnoj zaštiti koje će biti dovoljno agilne i fleksibilne da održe korak s rapidnim promjenama digitalnog krajolika.

Ako želimo iskoristiti pozitivne prednosti digitalnih tehnologija, a u isto vrijeme zaštititi raseljenu djecu s kojom radimo od potencijalne štete, Save the Children i druge agencije hitno moraju proširiti svoje digitalne kapacitete, znanja i vještine kako bismo u potpunosti ocijenili rizike za zaštitu djece koji dolaze od novih tehnologija i kako bismo proveli politike i prakse da te rizika ublažimo. Ove politike i prakse moraju biti dovoljno agilne i fleksibilne da održe korak s promjenama u područjima u kojima još uvijek ne postoje jasni pravni okviri.

Ova studija naslanja se na naš izvještaj o "Raseljenoj djeci i novim tehnologijama" iz 2019. godine, a u njoj predstavljamo kako sektor odgovara na rizike za zaštitu djece koji dolaze od digitalnih tehnologija, kao i naše preporuke za neposredne i praktične naredne korake kojima se osigurava da svako dijete migrant i raseljeno dijete ima koristi od digitalnih inovacija i da bude zaštićeno.

U okviru istraživanja obavljeni su razgovori sa zaposlenicima Save the Children u SAD-u, UK, Keniji, Danskoj, Švicarskoj, Libanu, Etiopiji, El Salvadoru, Afganistanu i na Balkanu, kao i sa vanjskim stručnjacima za tehnologije i inovacije unutar humanitarnog sektora. Ovi razgovori nadopunjeni su sveobuhvatnim pregledom stručne literature u vidu akademskih, organizacijskih i sektorskih izvještaja i dokumenata. Pouke iz ovog istraživanja poduprijet će izgradnju kapaciteta unutar organizacije Save the Children i ponuditi korisne preporuke za cijeli sektor, što će nam pomoći da osiguramo odgovornu upotrebu digitalnih tehnologija, uključujući i u izradi programa namijenjenih djeci i mladima u pokretu i raseljenoj djeci i mladima.

Zaštita od rizika koje donose digitalni programi

Četiri su osnovna područja zaštite djece od rizika u kontekstu digitalnih programa vezanih za migraciju i raseljenost.

1

Isključenost i samo-isključenost

Djeca bez pristupa odgovarajućim uređajima isključena su iz digitalnih programa i digitalnih setova podataka, što im otežava pristup određenim uslugama, a agencijama otežava učinkovito planiranje i provođenje programa zbog nedostatka podataka o toj djeci. Do samo-isključenosti dolazi kada se djeca sama izuzimaju iz digitalnih programa, često zato što nemaju povjerenja u to kako će njihovi podaci biti korišteni ili zato što se brinu za svoju privatnost.

2

Šteta prouzrokovana humanitarnim inovacijama

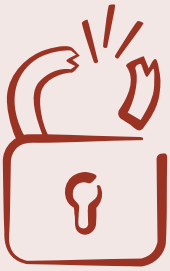
Inovacije podrazumijevaju rizike, naročito kada koriste neispitanu tehnologiju u radu s ugroženim populacijama (npr. razvoj proizvoda i testiranje mobilnih platformi za novac ili aplikacija za praćenje kontakata). Humanitarne agencije obično nemaju jednaka stručna znanja o digitalnoj tehnologiji kao kompanije koje pružaju tu tehnologiju, pa se mogu naći u nepovoljnom položaju kada procjenjuju potencijalne rizike ili štete koje inovacije mogu donijeti djeci u pokretu.

3

Povećana opasnost od štete na internetu

Agencije mogu nenamjerno izložiti djecu rizicima kada im obezbijede uređaje ili pristup internetu i kada ih potiču da koriste internet ili društvene medije, kada s njima ostvaruju kontakt putem društvenih medija ili kada objavljuju slike djece ili priče o njima na internetu. Društveni mediji mogu pojačati postojeće rizike za djecu u pokretu i raseljenu djecu, koja i na internetu mogu biti podložnija zloupotrebi, zlostavljanju i iskorištavanju.

4



Zloupotreba podataka i nepravilno postupanje s podacima

Agencije prikupljaju izrazito osjetljive podatke, uključujući biometrijske podatke, podatke o DNK i lokaciji, kako bi djeci pružale usluge i zaštitu, ali ponekad nisu svjesne da se ovi podaci mogu zloupotrijebiti čak i kada je izvršena enkripcija, depersonalizacija ili anonimizacija. U radu s više partnera, donatora, vladinih i privatnih organizacija, može doći do nejasnoća o tome kako upravljati razmjenom podataka i ko je za njih odgovoran. Nadalje, može biti teško odrediti do koje mjere su podaci djece zaštićeni i kojim propisima kada agencije pružaju usluge ljudima iz više zemalja i u više zemalja.

U osnovi ovih rizika postoji niz unakrsnih pitanja koja značajno utiču na naše kolektivne kapacitete da identificiramo, spriječimo i ublažimo rizike za zaštitu djece. To su:

- **Digitalna pismenost:** mnogi humanitarni akteri imaju ograničeno razumijevanje načina na koji digitalni podaci i analitika podataka utiču na programe koji se bave migracijama i raseljenim osobama.
- **Izazovi u pogledu kapaciteta:** ovi izazovi zajednički su za sve agencije, uključujući i one najveće koje imaju najviše resursa, ali su veći za manje agencije i "lokalne" partnere u zaštiti djece kojima nedostaje znanja, kapaciteta, sistema i budžeta da bi mogli pratiti stroge politike objavljivanja na društvenim medijima koje im nameću humanitarne agencije ili donatori. Lokalni partneri često nemaju kapaciteta za provođenje neophodnih sistema za sigurno upravljanje podacima ili ne prijavljuju incidente vezane za zaštitu djece jer nemaju uspostavljen odgovarajući sistem za te potrebe. Neprovođenje odgovarajućih politika digitalne zaštite također može biti rezultat nedostatka (dobrog) prijevoda na lokalne jezike. Ove je posebno značajno u kontekstu globalnih napora ka većoj lokalizaciji.
- **Povjerenje:** izbjeglice i migranti nemaju uvijek povjerenja da će agencije ispravno prikupiti i zaštititi njihove podatke, a ponekad su takvi prigovori na mjestu. Mnogo je priča o tome kako policijske vlasti zloupotrebljavaju podatke, naročito u svrhu ulaženja u trag i praćenja pojedinaca. Nedostatak povjerenja u to da će agencije etički koristiti podatke može dovesti do toga da djeca samu sebe izuzimaju iz digitalnih programa, a često su to djeca koja bi od takvih intervencija imala najviše koristi. .

Aktuelne politike i prakse digitalne zaštite

Save the Children ima snažnu osnovu politika za zaštitu djece i sigurnost podataka na kojoj je moguće graditi robusnije napore u pravcu digitalne zaštite. Postoji visok nivo svijesti i kritičkog razmišljanja o uticaju digitalnih uređaja i novih tehnologija na djecu. Organizacija prepoznaje mogućnosti koje nude digitalne tehnologije i inovacije u borbi da se djeci pruži zaštita i da se spriječi njihovo isključivanje.

Širom sektora, postojeće politike i prakse zaštite uglavnom ne razmatraju rizike povezane s promjenama u novom digitalnom okruženju.

Svijest osoblja o pitanjima zaštite kod digitalnog programiranja također je u mnogim područjima visoka, a uključuje i svijest o digitalnom jazu i o tome kako nedostatak pristupa može dovesti do isključenja ranjive djece; kako zlostavljanje na internetu može dovesti do samo-isključivanja; svijest o koristima i potencijalnim rizicima koji se pojavljuju kada djeca koriste internet i kada Save the Children koristi digitalne platforme u svom radu; kao i svijest o sigurnosti i privatnosti podataka.

Širom sektora, postojeće politike i prakse zaštite uglavnom ne razmatraju rizike povezane s promjenama u novom digitalnom okruženju. Nedostatak specifičnog etičkog okvira i okvira za zaštitu djece može i djecu i agencije i njihove partnere izložiti nepotrebnom riziku. Dosad su se rasprave s humanitarnim agencijama i donatorima uglavnom ticale zaštite djece na internetu (npr. od trgovine ljudima i od iskorištavanja). Rijetki postojeći resursi govore o specifičnom presijecanju zaštite djece i digitalnog programiranja i digitalnih inovacija.

Preporuke za unapređenje digitalnih zaštita u humanitarnom sektoru

Da bi ovaj sektor uspješno iskoristio izuzetno pozitivne i transformativne potencijale novih tehnologija, od suštinske je važnosti da izradimo i u naš rad ugradimo smjernice i politike o digitalnoj zaštiti koje će biti dovoljno agilne i fleksibilne da održe korak s rapidnim promjenama digitalnog krajolika, prilagodljive različitim kontekstima u kojima radimo i redovno ažurirane. Moramo dati prioritet ulaganju u naše kolektivne kapacitete da izvučemo koristi iz digitalnih tehnologija i odgovorimo na izazove koje nam postavljaju, kako bismo postigli bolje učinke za djecu migrante i raseljenu djecu i pružili im zaštitu.

U ovom izvještaju identificirano je sedam ključnih ciljeva na koje se sektor treba usmjeriti kako bi spriječio nanošenje štete i isključivanje djece kada se radi o programima koji se oslanjaju na digitalne tehnologije.

1

Osigurati digitalnu inkluziju za sve

Programi trebaju nastojati da unaprijede pristup digitalnom okruženju za djecu jer to može donijeti značajne koristi, ali istovremeno moraju biti inkluzivni u odnosu na djecu koja nemaju pristupa digitalnom okruženju kako bi izbjegli isključivanje određenih ciljanih populacija. Proširenjem skupova podataka tako da uključuju pojedince koji imaju, kao i one koji nemaju pristup digitalnom okruženju moguće je spriječiti iskrivljene zaključke.

2

Uspostaviti povjerenje u sistem

Nedostatak povjerenja predstavlja ključnu prepreku za učešće djece u digitalnom programiranju, pa je stoga za potrebe izgradnje povjerenja ključno osigurati da vlasti, vlade i privatni sektor ne zloupotrebljavaju podatke o djeci.

Moglo bi biti korisno uraditi dodatno istraživanje o mjeri u kojoj nedostatak povjerenja u sistem, agenciju ili sektor odvraća djecu od pružanja podataka. Također bi bilo korisno istražiti dodatne prepreke za razmjenu podataka kod djece jer bi to doprinijelo boljem razumijevanju potencijalnih prepreka za učešće u digitalnim programima i načina da se one otklone.

3

Izraditi jasne okvire za partnerstvo u inovacijama

Partnerstva s inovativnim kompanijama iz privatnog sektora donose mnoge prednosti i mogućnosti. Međutim, postoji i rizik da te kompanije imaju drugačije prioritete ili agende. Potrebne su jasne politike, okviri, dubinske provjere i procjene rizika u odnosu na koristi koje će biti prilagođene humanitarnim inovacijama i javno-privatnim partnerstvima.

Procjene rizika također se mogu osloniti na inovacijski set alata organizacije Response Innovation Lab i na njene Principe digitalnog razvoja koji daju smjernice za izradu programa. Temeljni humanitarni principi mogu poslužiti kao osnova za procjenu rizika kod implementacije digitalnog programiranja:

1. nenanošenje povreda,
2. humanost,
3. neutralnost,
4. nepristrasnost i
5. nezavisnost.

Pritom bi ih trebalo preorijentirati ka praktičarima i prilagoditi potrebama djece u pokretu i raseljene djece.

4

Osigurati da digitalni programi odražavaju potrebe i zabrinutosti korisnika

Neophodno je da učešće i povratne informacije od djece i odraslih u lokalnim zajednicama budu odraženi u politikama zaštite, programiranju i zagovaranju. Zajednice je potrebno uključiti u izradu i ocjenu novih digitalnih programa, a njihovo učešće treba poduprijeti uspostavljanjem etičkog odbora i jasnih kanala za prigovore i transparentno dijeljenje rezultata.

5

Unaprijediti digitalnu pismenost i kapacitete u sektoru

Agencije su dužne djeci pružiti zaštitu kada im omogućuju da pristupe mobilnim uređajima, internetu i drugim digitalnim tehnologijama, ali kapaciteti terenskog osoblja i osoblja u lokalnim agencijama još uvijek predstavljaju rizik za učinkovito pružanje digitalne zaštite.

Lokalni uredi moraju imati dovoljne kapacitete da provode zaštitu djece koja je kontekstualno relevantna i prilagodljiva kako bi održala korak s novim platformama i tehnologijama. Potrebno je uspostaviti jasne smjernice i prilagoditi ih kontekstu potreba, dostupnosti resursa i kapacitetima lokalnih organizacija.

Potrebno je pružiti podršku lokalnim uredima kako bi prilagodili politike lokalnim režimima zaštite podataka i utvrdili kontakt osobe za specifične smjernice u lokalnom kontekstu i uskladiti sisteme za pohranjivanje i sigurnost podataka kako lokalni uredi ne bi morali upravljati višestrukim sistemima.

Svim organizacijama i partnerima mora biti dostupna obuka za izgradnju svijesti o važnosti toga da zaštita podataka i digitalna zaštita mora biti "svačija odgovornost", kao što je to slučaj s tradicionalnom zaštitom.

6

Izraditi jasno vlasništvo, upravljanje i obučavanje

Digitalne inovacije napreduju brže od nacionalnog zakonodavstva, pa je stoga potrebno da agencije izrade politike i prakse koje će biti dovoljno agilne i fleksibilne kako bi održale korak s promjenama u područjima za koja još uvijek ne postoji jasno zakonodavstvo. U nekim slučajevima partnerske organizacije predstavljaju rizik jer njihovi manje robusni sistemi ne mogu pružiti adekvatnu sigurnost podataka.

Organizacije moraju izraditi procedure upravljanja koje jasno utvrđuju ko je odgovoran za koje aspekte politike i prakse digitalne zaštite i jasno navode nivo vještina i svijesti koji je neophodan za provođenje te politike. Odgovornost za upravljanje, održavanje i ažuriranje procedura ili sistema ne treba biti povjerena samo jednom zaposleniku.

Svim organizacijama i partnerima mora biti dostupna obuka za izgradnju svijesti o važnosti toga da zaštita podataka i digitalna zaštita moraju biti "svačija odgovornost", kao što je to slučaj s tradicionalnom zaštitom. U obuke također trebaju biti uključena pitanja rizika s metapodacima, potencijala za ponovnu identifikaciju kod anonimiziranih podataka i druga aktuelna pitanja vezana za podatke i privatnost podataka.

7

Izraditi praktične i dosljedne sisteme i procese za upravljanje podacima

Sektoru su potrebne praktične smjernice za zaštitu i upravljanje podacima koje će biti kontekstualno i operativno relevantne. Agencije također trebaju ulagati u bolje usklađivanje sistema za pohranu i sigurnost podataka.

Nadalje, agencije trebaju razumjeti posljedice po ugled, pravne i finansijske posljedice loših i nedosljednih procesa, kao i ponekad dalekosežne posljedice po dijete. Kad se pristupa bilo kakvom digitalnom programiranju, potrebno je tražiti etički i pravni savjet stručnjaka.

Kako bi se osiguralo da izrađene smjernice i setovi alata budu praktični i prilagodljivi lokalnim kontekstima, bit će potrebno provesti dalja istraživanja, uključujući i dodatne studije slučaja na nivou regija i zemalja.

Praktični naredni koraci

Aktuelne sektorske smjernice o digitalnim zaštitama su nejasne i složene. Tek rijetki resursi govore o specifičnom ukrštanju zaštite djece i digitalnog programiranja i digitalnih inovacija.

Saradnja s drugim agencijama od ključnog je značaja za izgradnju normi koje će biti primjenjive širom sektora, kao i kapaciteta i resursa za obuku osoblja i rukovodilaca o digitalnoj zaštiti djece.

Ovo su akcije koje Save the Children i drugi u sektoru mogu preduzeti sada, ne samo za potrebe djece u pokretu i raseljene djece, već za sprečavanje štete koja se djeci nanosi na internetu u širem smislu.

Izraditi set alata za digitalnu zaštitu u kojem će biti:

A Smjernice i politike o zaštiti za nove programe digitalnih inovacija, a koje se mogu prilagoditi lokalnim kontekstima i koje podupire obuka.

B Alat za procjenu rizika koji se može koristiti u radu s partnerima iz privatnog sektora i lokalnim agencijama. Procjene rizika moraju uključivati specifična pitanja o inovativnim pristupima, zaštiti i sigurnosti podataka (npr. rizik od monetizacije podataka), digitalnim tehnologijama, razmjeni podataka i aktuelnim rizicima za zaštitu.

C Jasni kanali komunikacije putem kojih osoblje, partneri i korisnici mogu izraziti svoje zabrinutosti.

Revidirati i ažurirati politike o zaštiti, društvenim medijima, zaštiti podataka, sigurnosti podataka i informiranom pristanku tako da budu kontekstualno specifične, prilagođene lokalnom jeziku i propisima, a pritom uzeti u obzir nove tehnologije i digitalne platforme koje su najviše u upotrebi (npr. WhatsApp i Facebook grupe).

Izraditi okvire istraživanja, praćenja i evaluacije kako bi identificirali i razmotrili kratkoročne i dugoročne koristi, rizike i štetu od eksperimentacije i inovacija.

Izraditi regulatorni okvir s partnerima kako bi se osigurali dovoljni kapaciteti i razumijevanje tehnologije.

Raditi s privatnim partnerima kako bi bili u toku i znali koje uređaje i internetske platforme djeca koriste, kako ih koriste (npr. posuđeni uređaji, ograničena upotreba) i kakvi su im stavovi o njima (npr. pristupačnost, svrha upotrebe, pitanja privatnosti, nanesena šteta).

Investirati u obuku za regionalne i nacionalne urede u svrhu poboljšanja digitalne pismenosti osoblja i naglasiti povezane rizike za zaštitu djece i kako ih ublažiti.

Uspostaviti fokalne tačke unutar organizacije za utvrđivanje najbolje prakse i pružanje smjernica o privatnosti i zaštiti podataka u nacionalnom kontekstu.

Investirati u bolju usklađenost sistema za pohranu i sigurnost podataka tako da nacionalni uredi ne moraju upravljati višestrukim sistemima, a u skladu s resursima i preferencijama ureda.

Lucia Zoro / Save the Children

Ključne komponente u izradi digitalne intervencije

- **Ugraditi jasne sporazume i ocjene o tome koji se podaci mogu dijeliti s vladom i privatnim sektorom** i u koje svrhe.
- Razmotriti ugrađivanje **miješanog prikupljanja podataka** (npr. offline i online) tako da programi ne budu izrađeni na način da daju prednost djeci koja imaju pristup tehnologiji.
- Izgraditi **učešće zajednice** u ranoj fazi implementacije kako bi odgovorili na zabrinutosti na lokalnom nivou.
- Uspostaviti **interni etički odbor** za vrijeme planiranja i implementacije programa
- Provesti detaljnu **procjenu rizika** koja će razmotriti upravljanje podacima i sigurnost podataka, razmjenu i upotrebu podataka, digitalne tehnologije i inovacije, kao i aktuelne rizike za zaštitu.
- **Pružiti obuku** kako bi se osiguralo da osoblje ima odgovarajuće vještine za **provođenje procjena rizika**.
- **Tražiti pravi savjet** za uspostavljanje neophodnih sporazuma s partnerima za inovacije i/ili digitalne tehnologije.

U ovom izvještaju je, pored ovih praktičnih narednih koraka, identificirana i dodatna dobra praksa za praktičare kako bi se osiguralo da svako dijete migrant i raseljeno dijete može imati koristi od digitalnog programiranja i biti zaštićeno.

Francesco Alesi / Save the Children

UVOD

Usvajanjem novih tehnologija sektor nastoji unaprijediti efikasnosti, poboljšati sposobnosti za donošenje odluka i pokrenuti unapređenje kvaliteta programa. Ipak, rasprostranjenost i dinamika tehnoloških inovacija dovodi u prvi plan hitnu potrebu za programom sveobuhvatne i robusne podrške kako bismo osigurali da upotreba novih tehnologija ne prouzrokuje neželjene posljedice po djecu.

Save the Children je prepoznat kao sektorski lider u zaštiti djece. Ovaj izvještaj donosi preporuke o narednim koracima koje sektor treba preduzeti kako bi osigurao provođenje snažnih politika i prakse zaštite djece, kako bismo iskoristili prednosti digitalnih inovacija, ublažili rizike i prebrodili sve probleme sa zaštitom koji se pojave.

Studija organizacije Save the Children iz 2019. godine o aktuelnim digitalnim tehnologijama u izradi programa za djecu u pokretu i raseljenu djecu utvrdila je niz procjepa koji se odnose na sprečavanje štete i preporučila da Save the Children ojača svoju organizacijsku praksu digitalne zaštite.4 Izvještaj koji trenutno čitate naručen je kako bi doprinio izradi praktičnih okvira i alata koje Save the Children i druge agencije mogu koristi za ublažavanje rizika koji nastaju sa usvajanjem i upotrebom aktuelnih digitalnih tehnologija u izradi programa i zagovaranju za djecu u pokretu i raseljenu djecu.

Humanitarne agencije ugrađuju aktuelne i nove digitalne alate i tehnologije u razne aspekte svog programiranja i rada. Nastupanje pandemije bolesti COVID-19 početkom 2020. godine i kasnije naredbe vlada da se ograniče okupljanja primorale su sektor da veoma brzo postane ovisan o novim digitalnim tehnologijama kako bi mogao doprijeti do ugroženih populacija i pružiti im podršku. Organizacije rade na identifikaciji načina za implementaciju svojih programa na daljinu ili preko interneta, gdje je to moguće.

Digitalne tehnologije i inovacije imaju ogroman potencijal da preobraze programiranje s migrantskim i raseljenim populacijama, a naročito da podrže upravljanje predmetima i spajanje porodica.5 Međutim, digitalne tehnologije uvode i etičke dileme, rizike i potencijalnu štetu, naročito za djecu koja su već ranjiva.

Politike i prakse za zaštitu djece nisu išle ukorak s tehnološkim promjenama. Većina organizacija radi s tradicionalnim politikama i praksama zaštite koje ne uzimaju u obzir rizike povezane s aktuelnim promjenama u novom digitalnom okruženju. To ranjivu djecu izlaže rizicima za njihovu zaštitu koje moramo ublažiti ako namjeravamo zaštiti djecu kojoj pružamo usluge od potencijalne štete.

Uprkos općenitom kaskanju politike i prakse digitalnih zaštita širom sektora, počeli su se pojavljivati džepovi dobre prakse i prije nastupanja pandemije bolesti COVID-19. Ovo je prilika za Save the Children da prilagodi i ojača postojeće protokole i procedure i uspostavi dobru praksu za digitalnu zaštitu djece koja će im biti od koristi sada i u budućnosti.

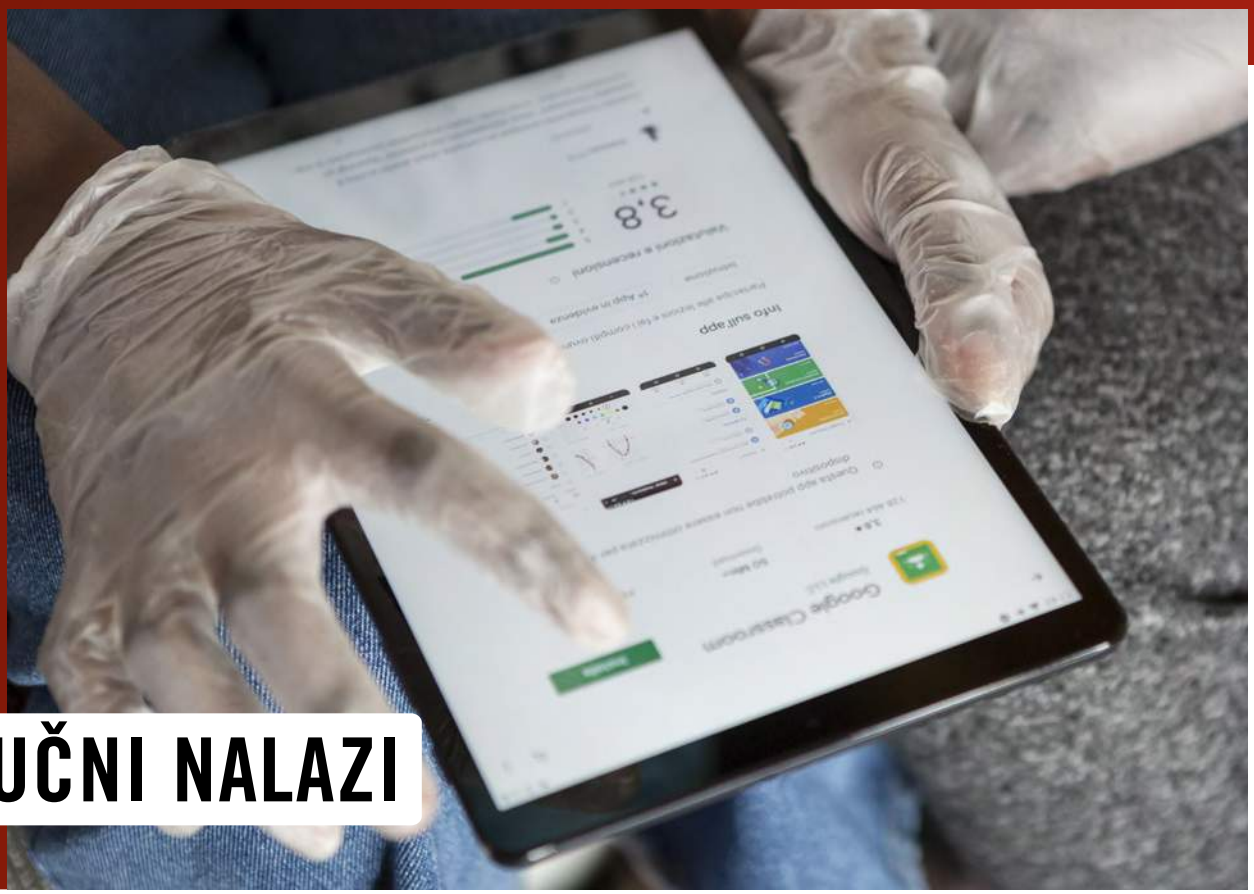
Politike i prakse za zaštitu djece nisu išle ukorak s tehnološkim promjenama. Većina organizacija radi s tradicionalnim politikama i praksama zaštite koje ne uzimaju u obzir rizike povezane s aktuelnim promjenama u novom digitalnom okruženju.

Terenski rad za ovaj izvještaj proveden je od decembra 2019. do aprila 2020. godine. Ključni intervjui obavljeni su sa 47 članova osoblja Save the Children širom SAD-a, UK, Kenije, Danske, Švicarske, Libana, Etiopije, El Salvadora, Afganistana i Balkana i u 12 drugih agencija (vidi Prilog 3 za više detalja). Obuhvaćeni su pristupi zaštitama i programiranju od prije nastupanja COVID-19, kao i prelazak s 'normalnog' programiranja na digitalno i programiranje na daljinu uslijed nastupanja pandemije bolesti COVID-19.

Ovaj izvještaj:

- istražuje postojeće politike i prakse digitalne zaštite za djecu u pokretu i raseljenu djecu;
- procjenjuje rizike digitalnog programiranja i način na koji Save the Children upravlja digitalnim zaštitama;
- identificira okvir rizika koji Save the Children može koristiti za pružanje digitalne zaštite u programiranju i
- preporučuje naredne korake za Save the Children i širi sektor kako bi osigurali da možemo iskoristiti prednosti digitalnog programiranja, a zaštiti djecu od štetnosti.

Vrijedi naglasiti da ovaj izvještaj nije formalna evaluacija, niti nastoji ponuditi konačne smjernice, alate ili obrasce. Umjesto toga, ovaj izvještaj se naslanja na iskustva u sektoru i postojeću literaturu kako bi ukazao na procjepe u digitalnoj zaštiti djece i pruža preporuke organizaciji Save the Children i drugim humanitarnim agencijama o tome kako da unaprijede digitalne zaštite u svim svojim područjima rada. Nadamo se da će omogućiti diskusije Save the Chidlren i drugih agencija o smjernicama i podršci neophodnoj za sistematičnije provođenje digitalnih zaštita kroz cijeli ciklus programiranja.



Francesco Alesi / Save the Children

KLJUČNI NALAZI

Digitalna tehnologija je sveprisutna u 2020. godini[6] i ima potencijal da donese ogromne koristi programiranju za populacije u pokretu i raseljene populacije. Novi pristupi u analitici podataka mogu se upotrijebiti za predviđanje masovnih raseljavanja i kao podrška digitalnim sistemima upravljanja predmetima, čime se dramatično poboljšava kapacitet humanitarnih agencija da odgovore na ove izazove i pruže podršku djeci u pokretu. Pandemija bolesti COVID-19 pokazala je koliko je za agencije ključan pristup osnovnoj tehnologiji i kanalima društvenih medija kako bi provele svoje programe, komunicirale s pogođenim zajednicama, dijelile informacije o javnom zdravlju i prevenciji virusa i provodile procjene potreba.[7]

Ipak, povećana upotreba digitalnih tehnologija i inovacija humanitarnim agencijama stvara etičke dileme. Nove tehnologije sa sobom nose nove, složene rizike za sigurnost djece koji se stalno mijenjaju. Dosad su se rasprave s agencijama za dječija prava i donatorima uglavnom fokusirale na zaštitu djece na internetu od vanjskih prijetnji kao što su vrbovanje, pornografija, trgovina djecom, iskorištavanje i zlostavljanje. Sektor tek sad počinje istraživati kako da odgovori na novonastale rizike i razmatrati načine na koje bi nehotice mogao prouzrokovati ili povećati rizike za djecu i zajednice kad proširuje vlastitu upotrebu digitalnih tehnologija i snimanja podataka.

Digitalne tehnologije mogu predstavljati dragocjen alat za unapređenje efikasnosti, širine i dubine usluga koje humanitarne agencije mogu pružiti, a digitalni podaci mogu unaprijediti ciljano usmjeravanje usluga i praćenje koristi. Međutim, neke agencije brine to što se efikasnosti i inovacijama trenutno daje prioritet u odnosu na efekte i kvalitet.[8] Donatori su ponekad poticali upotrebu naprednih tehnologija i prikupljanje velikih količina ličnih podataka kao načina da se unaprijedi ekonomičnost i spriječe prevare. S druge strane, agencije podatke o korisnicima ponekad posmatraju kao prednost koja im pomaže da razumiju kontekst svojih programa i unaprijede njihovu provedbu.[9]

Kako je njihova vrijednost rasla, podaci su postali dragocjena roba koja se nudi u zamjenu za finansiranje. Humanitarne agencije trebale bi odvagati potencijalne koristi ovog pristupa u odnosu na potencijalne negativne učinke za pogođenu djecu i zajednice. Zadržavanje velikih količina ličnih ili osjetljivih podataka izlaže agencije pravnim rizicima i rizicima po njihov ugled zbog mogućnosti zloupotrebe i lošeg upravljanja podacima. Ako bi podaci procurili zbog nedovoljnog pridržavanja protokola za informatičku sigurnost ili zbog nekog hakerskog incidenta ili krađe identiteta, to bi moglo dovesti do ozbiljnog javnog skandala ili pravnih posljedica, a također bi moglo predstavljati značajan rizik za osobu ili osobe na koje se podaci odnose. Podaci kojima bi se zbog takvog incidenta ostvario pristup mogli bi omogućiti zlonamjernim akterima da nanesu štetu, prošire dezinformacije ili da podrivaju povjerenje u određenu instituciju ili humanitarni sektor u cijelosti.[10]

Humanitarne organizacije moraju stalno unapređivati svoje razumijevanje pitanja zaštite podataka i ažurirati svoje interne politike kako bi održale korak s dinamikom tehnološkog razvoja i rapidnih promjena u zakonima o privatnosti podataka širom svijeta.

Dosad su se agencije u svom pristupu digitalnoj zaštiti uglavnom fokusirale na to da zaštite djecu od povreda dok koriste internet. Globalno stavljanje naglaska na zaštitu podataka i privatnost potaklo je sektor da se također fokusira na digitalne rizike i rizike vezane za podatke koje bi mogli prouzrokovati njihovi vlastiti programi.

Humanitarne organizacije moraju stalno unapređivati svoje razumijevanje pitanja zaštite podataka i ažurirati svoje interne politike kako bi održale korak s dinamikom tehnološkog razvoja i rapidnih promjena u zakonima o privatnosti podataka širom svijeta. Save the Children je, na primjer, 2017. godine uveo ažuriranu globalnu politiku zaštite podataka kako bi postigao usklađenost s Općom uredbom o zaštiti podataka Evropske unije (GDPR) koja je stupila na snagu u maju 2018. godine. Nadalje, i COVID-19 i Grand Bargain11 tjeraju agencije da lokaliziraju svoj pristup. Agencije moraju ne samo održavati vlastite vještine i kapacitete za digitalnu zaštitu, već moraju također naći načine da i svoje lokalne partnere podrže u tim aktivnostima.

U ostatku ovog izvještaja dat je pregled rizika povezanih s digitalnim tehnologijama, načina na koje Save the Children i širi sektor trenutno upravljaju tim rizicima kroz svoju politiku i praksu, a date su i preporuke za unapređenje ublažavanja rizika u područjima gdje su uočeni nedostaci.

Tipologija digitalnih rizika za djecu u pokretu i raseljenu djecu

Ova studija identificirala je četiri kategorije rizika koji nastaju uslijed usvajanja digitalnih alata i programa.

1. Isključenost i samo-isključenost
2. Šteta prouzrokovana humanitarnim inovacijama
3. Povećana opasnost od štete na internetu
4. Zloupotreba podataka i nepravilno postupanje s podacima

Ova područja su usko međusobno povezana. Faktori rizika uključuju pristup digitalnim alatima i povezivanju; znanja i kapacitete vezane za nove tehnologije i digitalne podatke; preklapajuće uloge i interese (prvenstveno djece, porodica i zajednica, humanitarnog sektora, privatnog sektora, vlada i nevladinih aktera); pitanja etike i odnose moći; transparentnost i odgovornost te povjerenje u prikupljača podataka.

Ni pojedinačne agencije ni sektor u cijelosti nisu pripremljeni da odgovore na ovu složenu mješavinu tehnologija i faktora rizika. Agencijama su potrebni prošireni kapaciteti, znanja i vještine kako bi u potpunosti procijenile rizike i negativne posljedice i kako bi provele politike i ustanovile praksu za njihovo ublažavanje.

Slika 1

Tipologija digitalnih rizika za djecu u pokretu i raseljenu djecu

1 Isključenost i samo-isključenost

Sljedeći rizici od isključenja mogu nastati kod uvođenja digitalnih tehnologija:

A Nedostatak pristupa uređajima i internetu ostavlja neku djecu u zaostatku

B Tehnologija koja nije prilagođena djeci može ih isključiti iz primanja neophodnih usluga

C Nestabilan mobilni pristup internetu može dovesti do isključenja

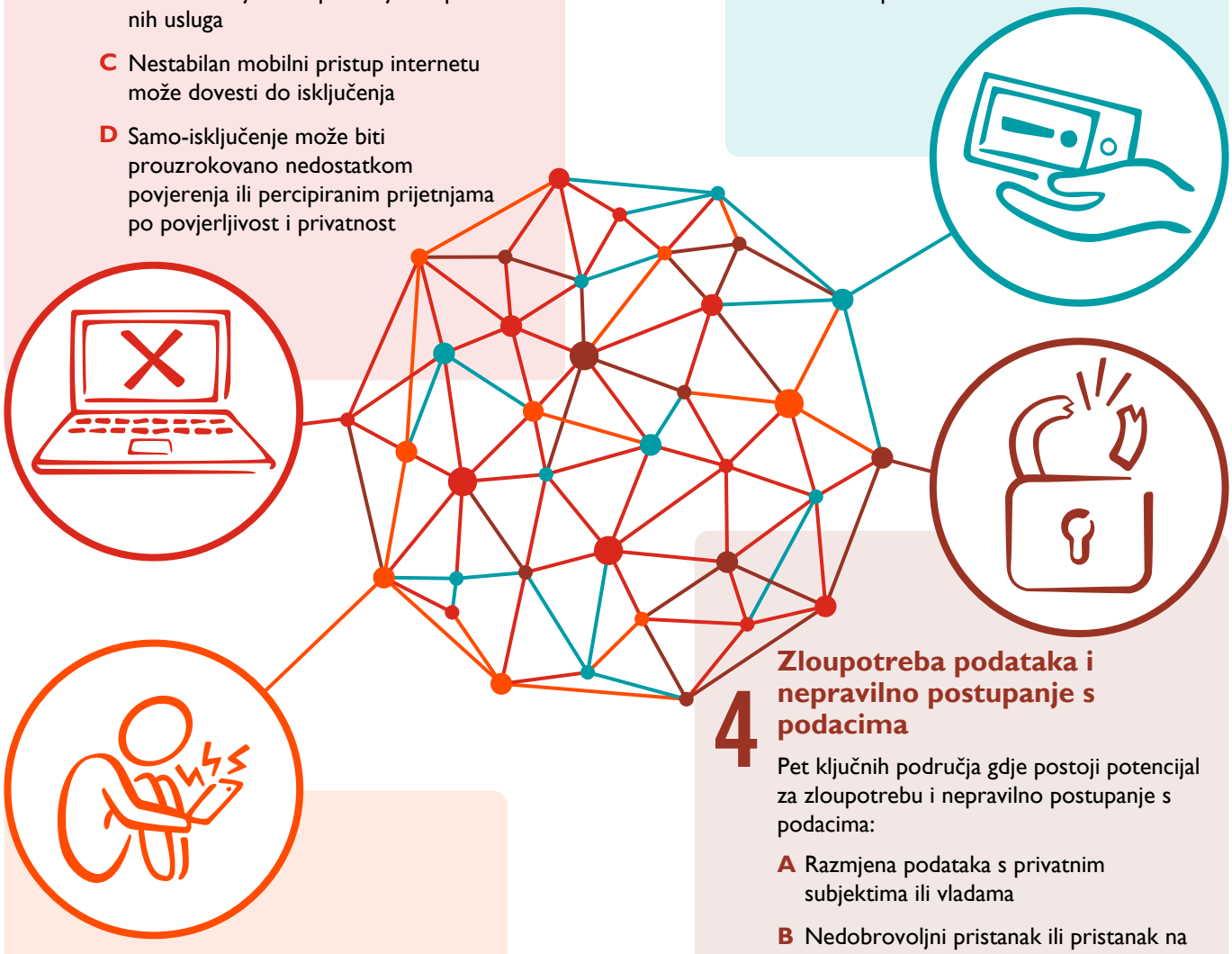
D Samo-isključenje može biti prouzrokovano nedostatkom povjerenja ili percipiranim prijetnjama po povjerljivost i privatnost

2 Šteta prouzrokovana humanitarnim inovacijama

A Nedostatak odgovornosti agencije

B Prioriteti privatnog sektora mogu podrivati potrebe pogođenih populacija

C Netestirani pristupi dodaju potencijalni rizik za ugrožene skupine



3 Povećana opasnost od štete na internetu

A Agencije mogu nehotice povećati izloženost djece opasnostima na internetu zbog nedostatka smjernica

B Društveni mediji pojačavaju tradicionalne rizike za djecu u mješovitim kontekstima migracije i raseljenosti

4 Zloupotreba podataka i nepravilno postupanje s podacima

Pet ključnih područja gdje postoji potencijal za zloupotrebu i nepravilno postupanje s podacima:

A Razmjena podataka s privatnim subjektima ili vladama

B Nedobrovoljni pristanak ili pristanak na osnovu obmane

C Obavezno dijeljenje podataka u zamjenu za primanje vitalne podrške

D Različiti pravni okviri u različitim zemljama usložnjavaju izradu programa za više zemalja

E Nedostatak zakona o privatnosti podataka fokusiranih na djecu u zemljama domaćinima

1 Isključenost i samo-isključenost

Isključenost i samo-isključenost odnose se na rizike da će djeca i drugi korisnici biti izostavljeni iz digitalnog programiranja i digitalnih skupova podataka. UNICEF upozorava da 'digitalni jaz' razdvaja ljude koji su digitalno povezani od onih koji nisu, a utiče na to kako djeca komuniciraju i ostvaruju pristup informacijama. Faktori koji utiču na iskustvo djece na internetu uključuju vrstu uređaja kojima imaju pristup, nivo njihovih digitalnih vještina i educiranosti, njihove porodične prihode i dostupnost sadržaja na njihovom jeziku. Neka djeca se nađu u digitalnom prostoru u kojem njihov jezik, kultura i zanimanja ne postoje, što im iskustvo interneta čini otuđujućim ili stranim i dovodi do niže stope angažiranosti i upotrebe.[12]

Sljedeći rizici od isključenja nastaju kod uvođenja digitalnih tehnologija:

A Nedostatak pristupa uređajima i internetu ostavlja djecu u zaostatku

Pristup i upotreba digitalnih uređaja, alata, platformi i usluga postali su globalno rasprostranjeniji u posljednjoj deceniji. Procjenjuje se da je do 2017. godine preko 50% svjetskog stanovništva imalo pristup internetu putem mobilnih usluga prijenosa podataka ili fiksne širokopojasne mreže.[13] Međutim, pristup je obično veći za bogatije, urbane, muške populacije.

Agencije su izrazito brzo usvajale digitalne tehnologije, ali mnogi korisnici kojima agencije trebaju pružati usluge imaju ograničen pristup ili uopće nemaju pristupa mobilnim uređajima i internetu, pa zato ne mogu imati koristi od usluga na internetu. UNICEF procjenjuje da skoro 9 od 10 mladih ljudi (uzrasta 15–24) koji trenutno ne koriste internet živi u Africi, Aziji ili na Pacifiku. Afrika ima najviši udio onih koji ne koriste internet u dobnoj skupini od 15 do 24 godine starosti. U Bangladešu i Zimbabveu manje od 1 od 20 djece mlađe od 15 godina koristi internet. Čak i kad imaju pristup uređaju djeca često neće koristiti internet zbog loše povezanosti i visoke cijene usluga prijenosa podataka.[14]

Djeca zbog nedostatka povjerenja u digitalne platforme sama sebe isključuju. Na učešće također može uticati identitet djeteta i ranija iskustva na internetu.

Kada je 2020. godine izbila pandemija bolesti COVID-19, pogoršao se problem digitalne isključenosti jer se sve više usluga i programa koje pružaju agencije ubrzo premjestilo na internet. Izostavljeni su mnogi ljudi koji nemaj pristup mobilnim uređajima i internetu; (osoblje navodi da u nekim izbjegličkim kampovima i kampovima za interno raseljene osobe nije bilo pristupa ni osnovnim tehnologijama kao što su radio i televizija, a da ne govorimo o pametnim telefonima, laptopima i tabletima). Kako se ovaj digitalni trend bude nastavljao, a možda i povećavao, tako će se nastaviti i povećavati rizik od isključenja. S jedne strane, na ovaj način djeca i mladi mogu osigurati veću privatnost. S druge, međutim, nedostatak digitalnog pristupa znači da neka djeca neće imati 'digitalni otisak'. Nisu zastupljeni unutar podataka i zato ih nema kada agencije generiraju uvide, planiraju i pružaju usluge i kada donose odluke o raspodjeli resursa. Pored toga, djeca koja nisu u mogućnosti pružiti specifične podatke (npr. digitalni ID) nekad ne mogu dobiti pristup digitalnim programima i uslugama.

Visoki komesar Ujedinjenih nacija za izbjeglice (UNHCR) navodi da se raseljene populacije suočavaju s ozbiljnim izazovima u pogledu digitalne povezanosti u urbanim i ruralnim oblastima i u kampovima. Još uvijek postoje veliki procjepi u podacima kada se radi o rasprostranjenosti digitalnih tehnologija, upotrebi i odnosu prema ICT-u među populacijama raseljenih.[15]

B Tehnologija koja nije prilagođena djeci može ih isključiti iz primanja neophodnih usluga

Biometrija je, na primjer, osmišljena za odrasle i neće nužno jednako dobro funkcionirati u radu s djecom. Tako recimo prepoznavanje lica može pogriješiti 3–5 godina kada procjenjuje nečiju starost,[16] a postoje i dobro poznati izazovi kod identifikacije ljudi tamnije puti. Također, još uvijek nije jasno da li je učinkovito uzimati otiske prstiju novorođenčadi. Ove vrste grešaka u biometrijskom prepoznavanju mogu dovesti do isključivanja iz vitalnih usluga i uspostaviti barijere za marginalizirane i ugrožene skupine, uključujući i djecu.[17]

C Nestabilan mobilni pristup internetu može dovesti do isključenja

Mnoga domaćinstva imaju jedan zajednički telefon, ali pristup može biti nejednak unutar domaćinstva. Globalna studija koju su 2019. godine proveli Girl Effect i Vodafone anketirala je 3.000 djevojčica[18] i otkrila da je pristup mobilnoj telefoniji često neravnomjeran, nedosljedan i pod snažnim uticajem lokalnih rodnih normi. Umjesto binarne razlike između 'nema pristupa mobilnom telefonu' i 'ima pristupa mobilnom telefonu', djevojčice navode da je njihov pristup mobilnom telefonu često promjenjiv i nepouzdan.

Rod i uzrast su faktori kod posjedovanja telefona (što ne treba brkati s pristupom telefonu i upotrebom telefona). Dječaci u nekim zemljama 1,5 puta češće posjeduju bilo kakav telefon od djevojčica, a 1,8 puta češće imaju pametni telefon. Mladi od 18 do 19 godina češće posjeduju telefon nego mladi od 15 do 17 godina.[19]

Neka djeca s invaliditetom imat će malo do nimalo pristupa mobilnom telefonu, što će ih učiniti nevidljivim u digitalnom svijetu i u digitalnim podacima. U studiji koju je 2019. provelo udruženje GSMA20 navodi se da je za izbjeglice s invaliditetom u kampu Bidi Bidi 68% manja vjerovatnoća da će imati pristup mobilnom telefonu, da će ga posjedovati ili koristiti.

Caroline Trutmann Marconi / Save the Children

D Samo-isključenje može biti prouzrokovano nedostatkom povjerenja ili percipiranim prijetnjama po povjerljivost i privatnost

Djeca često posuđuju ili dijele telefon, na primjer od roditelja, poslodavca, humanitarnih agencija, a u slučaju mnogih djevojčica i od starijeg brata.[21] To **čini pristup osjetljivim informacijama rizičnim i umanjuje povjerljivost,** pa tako može ograničiti i vrstu informacija koju djeca, a naročito djevojčice, traže ili dijele na internetu i potaknuti ih da se samo-isključe. Na primjer, u slučajevima nasilja u porodici ili opasnog rada, djeca bi mogla htjeti da istraže mogućnosti migracije ili bijega, ali to postaje teže kada je telefonska komunikacija pod kontrolom drugih ili je drugi mogu pratiti. Ankete koje procjenjuju rasprostranjenost mobilnih telefona prema broju domaćinstava koja posjeduju uređaj, a ne prema broju djece koja posjeduju vlastiti uređaj, često propuste ovu nijansu.

Osim toga, a naročito u slučaju djevojčica, bitna je i razlika između neograničenog u odnosu na ograničeni pristup uređaju. Čak i kad djevojčice posjeduju vlastiti uređaj, način na koji ga koriste često je pod kontrolom ili nadzorom članova porodice, što znači da će radi zaštite samih sebe djevojčice često biti manje slobodne u svom izražavanju i istraživanju informacija kada koriste takve uređaje.[22,23]

U slučaju djevojčica, bitna je razlika između neograničenog u odnosu na ograničeni pristup uređaju... radi zaštite samih sebe djevojčice će često biti manje slobodne u svom izražavanju i istraživanju informacija kada koriste takve uređaje.

Djeca zbog nedostatka povjerenja u digitalne platforme često sama sebe isključuju. Izbjegličke i migrantske populacije mogu odlučiti da ne koriste aplikacije i digitalne usluge ako nemaju povjerenja u agencije koje ih promoviraju ili ako osjete da će ih korištenje tih aplikacija ili davanje podataka izložiti rizicima.[24] To može dovesti do samo-isključenja ponukanog potrebom da sami sebe zaštite od invazivnih praksi snimanja i razmjene podataka ili zato što bi ih aplikacije mogle izložiti rizicima.

Djeca se samo-isključuju i tako što odbijaju pružiti podatke o sebi, pružaju lažne podatke ili jednostavno ne učestvuju u programima. Agencije trebaju procijeniti da li nedostatak povjerenja u sistem, agenciju ili sektor čini da se djeca ustežu od pružanja podataka iz straha da će se tako izložiti rizicima.

Na učešće također može uticati identitet djeteta i ranija iskustva na internetu. Djeca koja su bila žrtve vršnjačkog i drugog zlostavljanja na internetu zbog svog identiteta mogu odlučiti da se samo-isključe sa internetskih platformi ili da smanje svoje učešće. Šire vladine politike i stepen slobode govora također utiču na nivo učešća. U kvalitativnom istraživanju provedenom u Džakarti u Indoneziji 2019. godine, djevojčice otkrivaju da su manje komentirale na platformama društvenih medija kada je vlada povećala cenzuru određenih tema na internetu, uključujući teme reproduktivnog zdravlja i seksualnosti, pitanja LGBTQI, političkih mišljenja i blasfemije. Djevojčice su često navodile istaknute medijske izvještaje o pojedincima koji su pretučeni ili uhapšeni zbog komentara na internetu i objašnjavale da su zbog toga prestale objavljivati komentare kako bi izbjegle maltretiranje preko društvenih medija.[25]

2 Šteta prouzrokovana humanitarnim inovacijama

Agencije sve više koriste nove digitalne tehnologije za pružanje podrške djeci u pokretu i raseljenoj djeci, kao što su, na primjer, tehnologije koje djeci pomažu da pristupe informacijama, uspostave identitet (npr. digitalni ID) ili saznaju gdje mogu dobiti podršku. Dosta ovih inovacija odvija se putem javno-privatnih partnerstava i može biti zasnovano na naglasku koji donator stavlja na inovacije, skaliranje, učinkovitost ili odgovornost, ili na interesu privatnog sektora za razvoj i testiranje proizvoda, uz želju da se poboljšaju iskustva pogođenih populacija.[26,27] Humanitarne agencije često ne posjeduju jednaka stručna znanja iz digitalnih tehnologija kao kompanije koje pružaju te tehnologije.
To znači da mogu doći u nepovoljan položaj kada procjenjuju potencijalne rizike ili štetu koje inovacija može nanijeti djeci u pokretu i raseljenoj djeci.

A Nedostatak odgovornosti agencije

Inovacija sa sobom nosi inherentan rizik od propusta ili grešaka zato što podrazumijeva eksperimentaciju. Humanitarne inovacije s izuzetno ugroženim skupinama kao što su djeca ili zajednice pogođene krizom povlači istu vrstu etičkih pitanja kao i testiranje medicinskih postupaka i farmaceutskih proizvoda na krajnje ugroženim skupinama. Trenutno ne postoje obavezni ni široko rasprostranjeni okviri u području razvoja i humanitarnih poslova koji bi usmjeravali i držali odgovornim one koji provode ovu vrstu eksperimentacije.[28] Neophodne su dodatne predostrožnosti kada se eksperimenti provode u stvarnom životu, a ne u bezbjednim prostorima laboratorija.

Populacije pogođene krizom kao što su izbjeglice i raseljeni često nemaju mnogo izbora o tome da li žele učestvovati u takvim eksperimentima, a mnogi stručnjaci za privatnost podataka i etiku koji rade u humanitarnom sektoru vjeruju da istinski informiran pristanak nije moguć u kriznim i vanrednim situacijama.[29] Ako se ne provodi uz jasnu etičku perspektivu i procjene rizika, transparentnost, pristanak, principe dužnosti brižnog postupanja i odgovornosti prema pojedincima i zajednicama koje u njoj učestvuju, inovacija ima potencijal da im nanese štetu.

Kritički pristup etici i logistici testiranja novih tehnologija s ugroženim populacijama pomaže da se te populacije zaštite, a nadamo se doprinosi razvoju boljih tehnologija koje će im unaprijediti živote.

B Prioriteti privatnog sektora mogu podrivati potrebe pogođenih populacija

Sklapanje partnerstava s vladom i privatnim sektorom može omogućiti širi opseg i održivost rada u određenoj zemlji ili kontekstu. Privatni sektor donosi prijeko potrebnu tehničku ekspertizu i finansiranje kojim se mogu unaprijediti kapaciteti i programiranje. Međutim, ako takva partnerstva nisu pažljivo provjerena i procijenjena, mogu dovesti do više štete nego koristi. Privatni sektor ima sofisticiraniju ekspertizu za tehnologiju od humanitarnih agencija, a može imati i drugačije prioritete, što otežava provođenje učinkovite digitalne zaštite i nadzora. Ovo se dodatno usložnjava deficitarnim sredstvima agencija i može sektor dovesti u iskušenje da sklopi partnerstva koja nisu baš idealna ili nisu u potpunosti provjerena i procijenjena.

Humanitarne agencije, vlade i privatni sektor imaju interes da tehnologiju primijene efikasno i ekonomično, ali efikasnost, rasprostranjenost i sama tehnologija ne smiju zasjeniti iskustva pogođenih populacija. Ovo utiče na to kako se sredstva raspodjeljuju, ko vodi procese inovacija i ko će prvenstveno od njih imati koristi.[30]

C Netestirani pristupi dodaju potencijalni rizik za ugrožene skupine

Trenutno postoji nedostatak pravnih propisa i zaštita veznih za podatke koji se odnose na tehnološke inovacije u humanitarnim kontekstima. Nedostatak jasnih politika, okvira, temeljitih provjera i procjena rizika u odnosu na koristi prilagođenih humanitarnim inovacijama i javno-privatnim partnerstvima izlaže ugrožene populacije riziku, a potencijalno i šteti. Ovo je posebno zabrinjavajuće kada humanitarne inovacije uključuju djecu iz izrazito ugroženih ili nedovoljno zastupljenih skupina.

Netestirani pristupi u nekim okruženjima nose visok rizik i naglašavaju potrebu da agencije izrade strukturiran proces procjene rizika i uticaja na najugroženije.[31,32]

3 Povećana opasnost od štete na internetu

Šteta može nehotice nastati zbog nedovoljnog kapaciteta za upravljanje podacima u teškim kontekstulnim okolnostima, ali također postoji i potencijal da šteta bude prisutna i pri usvajanju novih pristupa.

Agencije imaju dužnost brižnog postupanja u odnosu na zaštitu djece kada im omogućuju pristup mobilnim uređajima i internetu ili drugim digitalnim tehnologijama. Mogu nehotice djecu izložiti rizicima na internetu kada im omogućuju pristup uređajima ili internetskim vezama, kada ih ohrabruju da koriste internet ili društvene medije, kada s njima stupaju u kontakt putem društvenih medija i kada na internetu koriste slike djece i priče o njima. Iako su mnoga djeca i mladi već aktivni na internetu, kada im agencije omoguće pristup internetu ili mobilnoj telefoniji tako da djeca mogu otići na internet, kada djeca objavljuju sadržaje ili kada se o njima objavljuju sadržaji, izrazito ranjiva djeca mogu biti izložena rizicima na internetu za koje su nespremna. Na ovaj način im može biti omogućeno da donesu rizične izbore ili da pristupe sadržajima koji nisu bezbjedni. Također mogu biti izloženi osobama i grupa koji ih žele iskoristiti ili im na drugi način nanijeti štetu.

Više je izvještaja u kojima se ističu situacije kada su tradicionalni rizici – uključujući zlostavljanje i korupciju, trgovinu ljudima, rodno zasnovano nasilje, iskorištavanje koje provode policijske vlasti i regrutiranje koje provode oružane snage – pogoršani na društvenim medijima.

Još je 2013. godine u izvještaju koji su izradili Plan International i Oak Foundation zabilježeno da djeca u pokretu koriste mobilne telefone i internet tokom svoje migracije ili raseljenosti, da se njima pomažu kako bi bolje isplanirali svoje putovanje, locirali sigurna mjesta usput i redovno se javljali porodici i prijateljima, provjeravali sigurna mjesta u zemljama porijekla, tranzita i po dolasku na odredište.[33]

Sljedeći rizici se mogu pojaviti kada su djeca izložena digitalnom okruženju i društvenim medijima:

A Agencije mogu nehotice povećati izloženost djece opasnostima na internetu zbog nedostatka smjernica

Pristup digitalnom prostoru bez vodiča i uz nedostatak svijesti predstavlja rizik za djecu.[34] Dosta je pisano o rizicima na internetu i 'cyber' prostoru za djecu i mlade, kao što su vršnjačko zlostavljanje, spolno vrbovanje, seksualno iskorištavanje, ovisnosti o videoigricama, promjena normi i vjerovanja, regrutiranje u nasilničke ili ekstremističke grupe, samopovređivanje, iznuđivanje, 'sexting', pojačan vršnjački pritisak, kao i gubitak samopouzdanja uslijed poređenja s vršnjacima koji je povezan s povećanjem depresije i anksioznosti među adolescentima i mladima.[35–37]

Općenito govoreći, djeca koja podliježu riziku od zlostavljanja mimo interneta, također su u opasnosti na internetu.[38–40] Istraživanja su pokazala da najvećem riziku podliježu: *"djevojčice, djeca iz siromašnih domaćinstava, djeca u zajednicama koje imaju ograničeno razumijevanje različitih oblika seksualnog zlostavljanja i iskorištavanja djece, djeca koja ne pohađaju školu, djeca s invaliditetom, djeca koja pate od depresije ili problema s mentalnim zdravljem i djeca iz marginaliziranih skupina."*[41]

Djevojčice su izložene većem riziku od zlostavljanja na internetu u poređenju s dječacima, a rizik od 'cyber' vršnjačkog zlostavljanja naročito je visok za LGBTQI djecu.[42–44] Nasilje i diskriminacija, kako na internetu tako i mimo njega u zemljama porijekla može navesti LGBTQI mlade na migraciju tokom koje često postaju žrtve nasilja i zlostavljanja ako završe u pritvoru ili kad se pokušaju integrirati u zemljama odredišta. Ovo naročito vrijedi u slučaju transrodnih mladih.[45]

Djeca migranti podliježu većem riziku od vršnjačkog zlostavljanja u odnosu na domaću djecu, kako se navodi u studiji provedenoj u Italiji,[46] a UNHCR upozorava da su djeca u pokretu i ona koja žive u kampovima izložena povišenom riziku od nasilja i zlostavljanja.[47] Shodno tome, možemo pretpostaviti da su djeca izbjeglice, djeca u pokretu i raseljena djeca naročito u opasnosti od zlostavljanja, vršnjačkog zlostavljanja i od iskorištavanja na internetu.

B Društveni mediji pojačavaju tradicionalne rizike za djecu u mješovitim kontekstima migracije i raseljenosti

Rizik od izloženosti društvenim medijima je novo područje istraživanja koje još uvijek obrađuje iskustva djece kako ih sve više ima pristup internetu.
Više je izvještaja u kojima se ističu situacije kada su tradicionalni rizici – uključujući zlostavljanje i korupciju, trgovinu ljudima, rodno zasnovano nasilje, iskorištavanje koje provode policijske vlasti i regrutiranje koje provode oružane snage – pogoršani na društvenim medijima. Primjeri ovih situacija dati su u produžetku teksta.

Maltretiranje, korupcija, nasilje i zlostavljanje koje čine policija, granični službenici, oružane snage, civilne grupe, pripadnici šire javnosti i drugi

Društveni mediji su bili korisni u prokazivanju zloupotrebe položaja u El Salvadoru, ali postoji visok rizik od odmazde, a nedostatak daljeg postupanja vlasti čini da se pojedinci boje za svoju ličnu sigurnost ako prijavljuju zloupotrebu, a ne mogu to učiniti anonimno.[50]

Na Balkanu je anti-migrantskim mrzilačkim grupama dozvoljeno da ostanu na Facebooku uprkos zahtjevima drugih korisnika Facebooka da budu uklonjene.[49]

Posmatrači u Mjanmaru kažu da su stranice na Facebooku korištene za širenje mržnje i provociranja nasilja protiv Rohindža mjesecima, ako ne i godinama prije nego što je Facebook konačno preduzeo korake protiv njih.[48]

Trgovina ljudima, prevara i iskorištavanje koje čine krijumčari

Mobilni telefoni olakšali su krijumčarima da iskorištavaju porodice tako što ih ucjenjuju i traže otkupninu za puštanje njihove djece,[51] a društveni mediji mogu doprinijeti dezinformiranju i pogrešnom informiranju koje migrante izlaže većem riziku.[52] Krijumčari oglašavaju svoje usluge kako bi doprli do ljudi koji su odlučili migrirati i kako bi pridobili i one koji i nisu nužno razmatrali opciju migriranja. Neki krijumčari koriste društvene medije da se predstavljaju kao NVO sa zadatkom organiziranja bezbjednog puta u Evropu morem ili kao 'pravni savjetnici' za pitanja azila.[53–55]

Trgovci ljudima mogu naći ranjivo dijete na otvorenom kanalu i vrbovati ga da pređe na 'tamni kanal' (zatvorenu mrežu), gdje je vlastima teže identificirati trgovce ljudima.
Na primjer, u Srbiji se WhatsApp koristi za dječju prostituciju kod kuće.[56]

Rodno zasnovano nasilje, uključujući seksualno zlostavljanje i seksualno iskorištavanje djevojčica i dječaka, prostituciju, transakcijski seks, i prisilni brak

Predatori mogu koristiti naloge na društvenim medijima kako bi lakše identificirali ljude kojima je potreban novac i koji su zbog toga podložniji iskorištavanju. U tom smislu društveni mediji postaju ulazna tačka za trgovce ljudima da zloupotrebljavaju djecu u svrhu rada, trgovine ljudima, prosjačenja, i mreža za seksualne usluge.

Navođenje ličnih računa za plaćanje uobičajeno je na profilima na društvenim medijima unutar internetskih zajednica marginaliziranih skupina, uključujući žene, osobe drugačije boje kože, imigrante i osobe koje se identificiraju kao LGBTQI.[58]
Mladi ljudi u SAD-u koriste mobilne internetske stranice za plaćanje kao što je Venmo kako bi prikupili novac da pokriju troškove za koje nemaju dovoljno sredstava, na primjer, da plate troškove za člana porodice kojeg imigracijske vlasti privedu ili protjeraju.

Društveni mediji pružaju jednostavan način kontaktiranja i iskorištavanja djece koja su depresivna ili usamljena, u teškim životnim okolnostima ili prisiljena da zarađuju u situacijama gdje im zakonski nije dozvoljeno da rade, kao, na primjer, kad su raseljena.[57]

Iskorištavanje koje čine policijske vlasti i povećani rizici da djeca dođu u sukob sa zakonom i budu percipirana kao kriminalci

Agencija za imigraciju i carine SAD-a (ICE) objavila je 2017. godine da će koristiti umjetnu inteligenciju za ocjenjivanje vjerovatnoće da će neko ko želi imigrirati postati pozitivno koristan član društva.
Naučnici u području podataka podigli su uzbunu da će ova vrsta modela najvjerovatnije biti pristrasna i neprecizna i da će zvaničnicima ICE-a omogućiti da proizvoljno izdvoje određene skupine ili pojedince pod krinkom nepristrasnog algoritma.[59]
Također je prijavljeno i više slučajeva kada je ICE koristio društvene medije i informacije koje su prikupile kompanije koje trguju podacima za profit kako bi imigrantima ušao u trag i uhapsio ih.[60]

Regrutiranje koje vrše oružane snage i grupe

U Grčkoj je osoblje organizacije Save the Children prijavilo svoje zabrinutosti da se društveni mediji koriste za radikalizaciju ranjive djece i mladih migranata.

Poruke i propaganda na društvenim medijima specifično su izrađene da navuku mlade ljude. Utvrđeno je da su mlade izbjeglice bez pratnje podložnije radikalizaciji ako su razdvojene od svojih roditelja. Također postoje mišljenja da mladi ljudi koji su izbjeglice mogu biti autonomno radikalizirani putem sadržaja na internetu.[61] Ovo se ponekad naziva 'pretvaranjem informacija u oružje'.[62]

Tako su, na primjer, u El Salvadoru mladi putem društvenih mreža izloženi vršnjačkom zlostavljanju, prijetnjama i ohrabrenjima da se pridruže bandama. Ako odbiju, često osjećaju da moraju migrirati van zemlje.[63]

4 Zloupotreba podataka i nepravilno postupanje s podacima

Dok digitalna inkluzija pomaže djeci da ostvare prava na informacije i učešće, kao i da ostvare pristup vitalnim uslugama, povećana digitalna inkluzija znači da će veća količina izuzetno osjetljivih podataka (npr. biometrijski podaci, podaci o DNK i lokaciji) biti snimljena, a to povećava rizike.

Iako postoji veliki potencijal za izvlačenje zaključaka iz inače raštrkanih podataka tako što će biti objedinjeni i razmijenjeni, ovo podrazumijeva dobre namjere i dobru praksu na svim stranama. U radu s lokalnim i međunarodnim partnerima za implementaciju, donatorima, vladama i/ili organizacijama iz privatnog sektora, može biti nedovoljno jasno kako treba upravljati razmjenom podataka i ko je za to odgovoran. Nadalje, može biti teško odrediti do koje mjere su podaci djece zaštićeni i kojim propisima kada agencije pružaju usluge ljudima iz više zemalja i u više zemalja.

Colin Crowley / Save the Children

Vrste podataka koji predstavljaju veći rizik od nanošenja štete

Određene vrste podataka mogu predstavljati veći rizik od nanošenja štete ili zloupotrebe. Agencije trebaju imati jasne politike i procjene rizika u odnosu na koristi kojima će se voditi njihova upotreba ove vrste identifikatora, posebno za djecu.

Međutim, neke humanitarne agencije možda neće imati dovoljno svijesti o tome kako se određene vrste podataka mogu koristiti. Može postojati pretpostavka da su šifrirani i depersonalizirani podaci anonimni, a zapravo su podložni praćenju do izvora i reidentifikaciji ili drugim vrstama zloupotrebe za koje su sposobni sofisticiraniji akteri.

Određene vrste podataka mogu predstavljati veći rizik od nanošenja štete ili zloupotrebe. Agencije trebaju imati jasne politike i procjene rizika u odnosu na koristi kojima će se voditi njihova upotrebe ove vrste identifikatora, posebno za djecu

Pored anonimizacije i deidentifikacije mikro podataka, agencije također trebaju razmisliti o tome kako da provedu deidentifikaciju i anonimizaciju zbirnih podataka i kako da otklone poveznice između zbirnih podataka i skupina ljudi. Organizacije često pristupaju ličnim podacima djece i razmjenjuju ih na osnovu legitimnog interesa da pruže usluge. Međutim, pružanje usluge ne opravdava
uvijek rizik ili potencijalnu štetu koju može prouzrokovati prikupljanje podataka, a većina organizacija nije uspostavila dovoljno snažne procjene rizika u odnosu na koristi kako bi to prosudila. Najosjetljivije vrste podataka koje sa sobom nose veći rizik za djecu opisane su na sljedećim stranicama.

Biometrijski podaci

Biometrijski podaci, kao što su otisci prstiju, skeniranje rožnice i prepoznavanje lica smatraju se 'osjetljivim podacima' prema GDPR-u, što znači da upotrebi biometrijskih podataka mora prethoditi procjena uticaja na privatnost, a ako se ovakvi podaci prikupljaju, moraju se osigurati specijalne zaštite podataka. Biometrijski podaci ponekad se koriste za identifikaciju djece u zemljama koje nemaju učinkovite sisteme registracije rođenja.[64]

Biometrijska identifikacija se može koristiti u pozitivne svrhe, kao što je pomoć pri upravljanju predmetima i spajanju porodice. Međutim, pošto su biometrijski podaci jedinstveni identifikatori, njihova zloupotreba može nanijeti ozbiljnu štetu. Biometrijski podaci omogućuju donošenje preciznih zaključaka o privatnim životima i tačnim kretanjima ranjivih ljudi, što može imati ozbiljne posljedice ako vlade zemalja domaćina ili zemalja porijekla zatraže ili zahtijevaju humanitarne biometrijske podatke kako bi im prenamijenili svrhu i koristili ih za potrebe nacionalne sigurnosti, imigracije ili provedbe zakona.

Nadalje, prepoznavanje lica je ocijenjeno kao pristrasan alat zbog razlika u stopi tačnosti. Naime, rezultati su tačniji kada se primjenjuje na ljudima svjetlije puti u odnosu na ljude tamnije puti. Ovo dovodi do više slučajeva pogrešne identifikacije pojedinaca tamnije puti, što je izrazito problematično kada ovaj alat koriste agencije za provedbu zakona ili imigraciju.[65]

UNICEF, Oxfam i World Vision izdali su upozorenja ili uveli zabrane (privremeno ili na drugi način) za upotrebu biometrijskih podataka.

DNA

DNK predstavlja još jedan način za jedinstvenu identifikaciju pojedinaca i pružanje personalizirane pomoći. Iz DNK moguće je saznati spol osobe, medicinsku anamnezu, buduće zdravstvene rizike, porodične odnose i još toga.

Poput biometrijskih podataka, i DNK je invazivan, stalni jedinstveni identifikator koji, ako se uzima od djece, može dovesti do cjeloživotnih rizika za privatnost i trajnih implikacija. Na primjer, podaci o DNK mogu se koristiti kao osnova za praćenje i targetiranje.[66] Zbog njegovih razmjera i intruzivnosti, većina agencija izbjegava upotrebu DNK testiranja za rutinske operacije, jer postoji rizik po privatnost da će biti prikupljeno više ličnih podataka nego što je neophodno za određeni zadatak, a i UNICEF ne preporučuje prikupljanje DNK podataka.

Marieke van der Velden / Save the Children

Lokacijski podaci

Lokacijski podaci mogu pružiti korisne informacije za populacije migranata i raseljenih. Tako je, na primjer, Međunarodna organizacija za migracije (IOM) izradila aplikaciju koja pruža lokacijske informacije o skloništima duž migrantske rute od Centralne Amerike do Sjedinjenih Država.

Međutim, ono što zabrinjava je rizik da će lokacijske podatke zloupotrijebiti vlade ili druge grupe kako bi pojedincima ušle u trag i pratile ih. Postoje saznanja da su mladi i njihove porodice bili zabrinuti da bi zbog IOM-ove aplikacije mogli postati mete onima koji bi im nanijeli štetu (npr. krijumčarima, lokalnim naoružanim grupama ili lopovima) zato što je bilo lako pronaći lokacije skloništa na internetu. Porodice su preferirale da koriste maramice koje je dijelio Crveni krst, a na kojima bi bila karta sa označenim lokacijama skloništa.[67]

Za vrijeme krize s ebolom 2016. godine dovedeno je u pitanje to što je nekoliko vlada humanitarnim agencijama ustupilo evidencije podataka mobilne telefonije kako bi ih koristili za traženje kontakata. Nije bilo jasno da li se digitalno traženje kontakata može učinkovito koristiti za zaustavljanje širenja ebole i da li je otvaranje evidencije podataka privatnih mobitela dovelo do nepotrebnog otkrivanja ličnih podataka.[68]

Pandemija bolesti COVID-19 također je iznijela na vidjelo ovu problematiku kada su u mnogim zemljama širom svijeta predložene aplikacije za 'traženje kontakata'. U ovom slučaju bi to značilo da putem mobilnih lokacijskih podataka (putem Bluetootha ili GPS-a) pojedinci, a u nekim slučajevima i vlade, mogu utvrditi kada je pojedinac bio u određenoj blizini druge osobe čiji je test na virus bio pozitivan. Protivljenje je bilo široko rasprostranjeno jer su mnogi smatrali da je njihova učinkovitost nedovoljna da opravda količinu podataka koje bi prikupljale. Također je bilo riječi o strahu da će ovi podaci potencijalno koristiti i u druge svrhe, posebno zato što su u njihovu izradu bile uključene kompanije iz privatnog sektora poznate po saradnji s vladama za potrebe nadziranja stanovništva.[69,70]

Thomas Jepson-Lay / Save the Children

Anonimizirani i deidentificirani podaci

Anonimizirani i deidentificirani podaci ljude izlažu manjem riziku jer su iz njih izbrisane informacije iz kojih je moguće utvrditi identitet ili su agregirani u tolikoj mjeri da je nemoguće identificirati pojedince. Proces uklanjanja ličnih identifikacijskih podataka iz mikropodataka kako bi postali anonimni naziva se anonimizacijom ili deidentifikacijom podataka.

Međutim, anonimizirani podaci još uvijek mogu predstavljati rizik za pojedince. Čak i kad ih je nemoguće identificirati iz jedne izolirane datoteke mikro podataka, može biti moguće izvršiti reidentifikaciju pojedinaca uz pomoć (statističkog) uparivanja s drugim skupovima podataka. Zbog obima podataka o ljudima koji se sada (direktno i indirektno) prikupljaju i zbog toga što se skupovi podataka često kombiniraju i spajaju, postaje sve lakše identificirati pojedince unutar skupova podataka.

Metapodaci

Metapodaci pružaju informacije o drugim podacima. To su, na primjer, podaci o datumu, vremenu, geolokaciji i postavkama kamere spašeni u digitalnoj fotografiji, ili podaci o pošiljatelju, primatelju, datumu i vremenu slanja, imenu servera koji šalje i koji prima i adresama koji prate email poruku. Metapodaci o mobilnim komunikacijama mogu otkriti razne vrste informacije, kao što su lokacija i kretanje osobe.

Metapodaci sa društvenih medija i evidencije mobilnih telefona korišteni su za mapiranje društvenih veza među pojedincima. Čak i kad je sadržaj transakcija šifriran, podaci o tim transakcijama nisu. Stoga je moguće sklopiti sliku o aktivnosti na internetu koja otkriva fizičko prisustvo osobe uključene u tu aktivnost.

To znači da se metapodaci mogu koristiti za praćenje, targetiranje i odmazdu protiv pojedinaca i grupa. Neke vlade, na primjer, koriste podatke prikupljene sa pametnih telefona tražitelja azila kako bi potvrdile njihove izjave iz zahtjeva za azil.[71]

Grupni podaci

Grupnim podacima je posvećeno manje pažnje nego ličnim podacima; zakonodavstvo o podacima većinom je usmjereno na zaštitu ličnih podataka na nivou pojedinca. Međutim, pojedinci se često grupiraju na osnovu određenih demografskih karakteristika kao što su etnička pripadnost, religija, genetika, povezanost s određenom političkom grupom ili zajednička geolokacija kao što je selo ili lokalna zajednica. Mnogi novi pristupi podacima koje razvija privatni sektor za potrebe marketinga i političkog mikro-targetiranja imaju za cilj grupiranje sličnih pojedinaca kako bi im otkrili profil, obično za potrebe oglašavanja ili komunikacija za promjenu ponašanja koje navode određenu grupu bliže nekom političkom mišljenju ili ponašanju.[72]

Čak i kada pojedinac nije precizno identificiran unutar grupe, taj pojedinac još uvijek može biti izložen šteti zbog pripadnosti grupnim podacima, čak i kada su ti podaci anonimizirani.73 Rizik se može pojaviti čak i bez upotrebe sofisticiranih tehnika obrade podataka kao što je profiliranje. Jedna je organizacija, na primjer, geolocirala putanje djece do škole kako bi napravila vizualizaciju razdaljine koju djeca pređu da bi išla u školu. Ovakvo grupiranje i geolociranje mjesta gdje se djeca okupljaju i kuda pješače do škole može ih izložiti riziku od povrede ili nasilja ili maltretiranju koje vrše oružane grupe.

Mogućnost zloupotrebe ili nepravilne upotrebe kod prikupljanja i razmjene podataka

Ovdje razmatramo pet ključnih područja u kojima postoji mogućnost zloupotrebe ili nepravilne upotrebe podataka koja nastaje uslijed prikupljanja i razmjene podataka o djeci.

A Razmjena podataka s privatnim subjektima ili vladama

Vlade, tijela za imigraciju i provedbu zakona i privatni sektor mogu sarađivati s humanitarnim agencijama s namjerom da profitiraju od podataka koje prikupljaju te agencije ili da na osnovu njih targetiraju određene populacije.[74] Neki pojedinci uključeni u razvoj zajedničkih baza podataka postavljaju pitanje da li potencijalni rizici premašuju koristi i da li po ovim pitanjima trenutno postoji dovoljno kritičkog razmišljanja u sektoru zaštite djece.[75]

Podatke o populacijama izbjeglica i migranata ne treba dijeliti s vladama, milicijama i nedržavnim akterima koji ih mogu vidjeti kao mete za progon, hapšenje ili protjerivanje. Na primjer, podaci o djetetu koje je bivši pripadnih neke oružane grupe ne bi smjeli završiti među predmetima vladinog zvaničnika koji bi te informacije mogao iskoristiti na način da tom djetetu nanese štetu. Poznati su slučajevi kad su privatne kompanije nudile svoje usluge agencijama za zaštitu djece i humanitarnim organizacijama, a istovremeno su pružale usluge digitalnih istraga vladinim agencijama za potrebe pronalaženja i privođenja izbjeglica i migranata.[76]

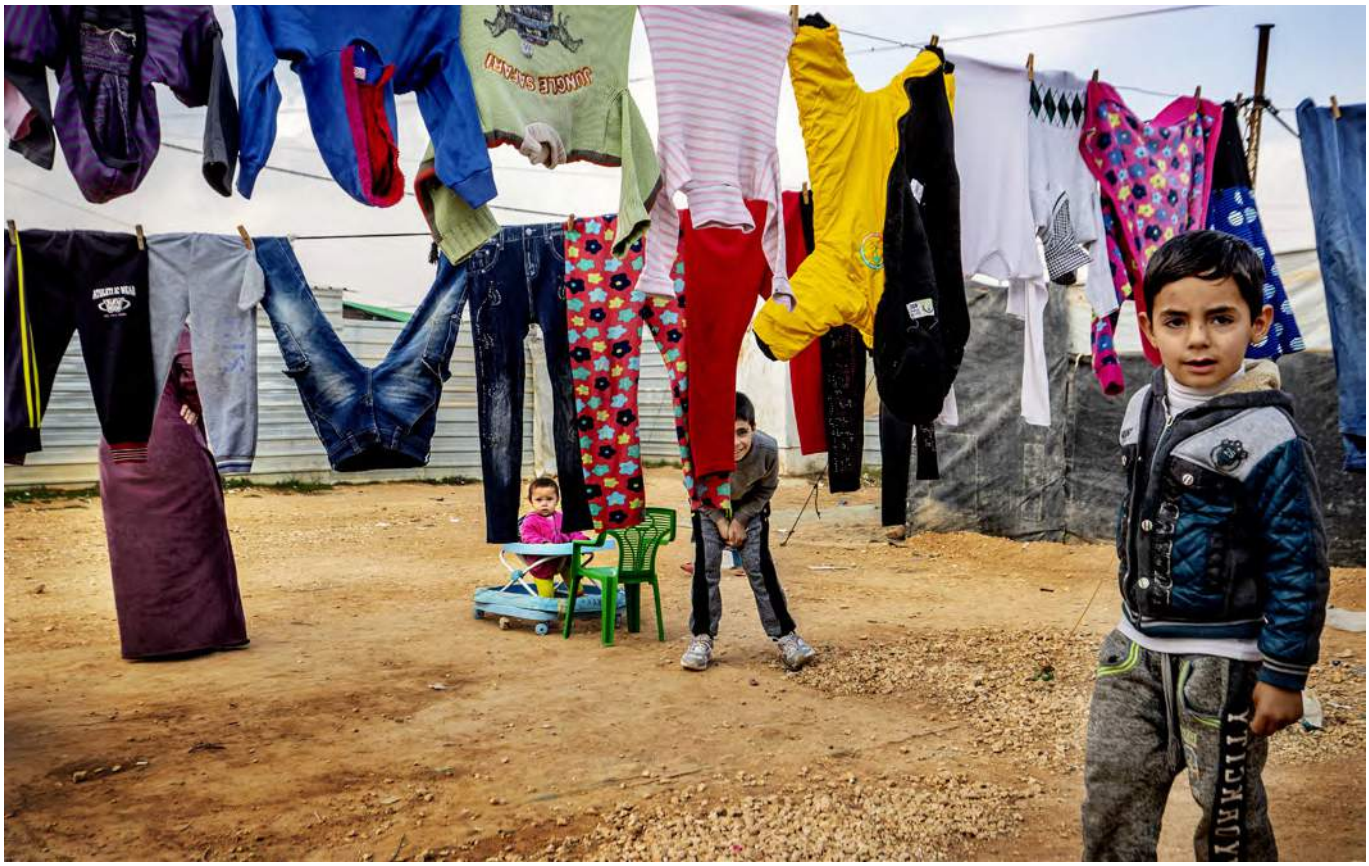
Korištenje podataka za identifikaciju i praćenje ljudi u svrhu deportacije

Privacy International navodi da je nekoliko kompanija za analitiku podataka izbjeglo ispitivanje njihove uloge u pružanju podataka za baze podataka ICE-a. Podaci koje su kompanije iz privatnog sektora pružale ICE-u uključivali su podatke iz biračkih spiskova, popisa, internetskih izdanja novina na lokalnom, nivou savezne države i saveznom nivou, registara seksualnih prijestupnika, internetskih kolačića, alata za praćenje elektronske pošte, aplikacija za pametne telefone i programa za praćenje trećih strana, kompanija s kojima su ljudi imali interakciju na internetu i mimo njega, društvenih medija, internetskih kvizova, anketa, nagrada, finansijskih kompanija i drugih kompanija za podatke, kao i iz mnogih drugih izvora. Ove kompanije ICE-u prodaju sisteme za analizu podataka koje ova agencija i drugi koriste za identificiranje i praćenje ljudi i njihovih porodica u svrhe koje uključuju i deportaciju.[77]

Potencijalni rizici kod prikupljanja osjetljivih informacija od izbjeglica

Nakon što su za UNHCR proveli istraživanje i izvještaje o studijama slučaja za pojedinačne zemlje, Privacy International istakao je niz potencijalno štetnih scenarija koje može prouzrokovati prikupljanje osjetljivih informacija od izbjeglica:

1. UNHCR podijeli pojedinačni predmet s nacionalnim vlastima za imigraciju i kontrolu granica zemlje azila što dovodi do pritvora članova porodice u zemlji porijekla.
2. Mlada izbjeglica prisiljena na seksualne odnose zarazi se HIV-om. Ova informacija biva prenesena lokalnim vlastima zbog obaveze razmjene podataka o zdravlju. To dovodi do prisilnog vraćanja izbjeglice u njegovu/njenu zemlju porijekla gdje on/ona biva stigmatiziran/a ili ubijen/a.
3. Agencije UN-a i partneri za implementaciju pristupaju spisku imena i geografskih lokacija pojedinaca u kampu kako bi učinkovitije dijelili pomoć. Porijeklu podataka se izgubi trag, a greške u skupovima podataka koji se dijele ostaju neispravljene. S vremenom postane nemoguće identificirati mjesta gdje se podaci nalaze jer organizacije nastavljaju da ih razmjenjuju. Laptop na kojem su podaci biva ukraden, a nemoguće je s tim u vezi odrediti prirodu i stepen rizika.[78]



Pim Ras / Save the Children

Kada humanitarne agencije vladama usptupe velike skupove podataka o izbjeglicama, migrantima i tražiteljima azila, to također povlači za sobom rizike i razloge za zabrinutost. Tu je od suštinskog značaja pitanje povjerenja. U jednom slučaju pojavila se tvrdnja da je jedna agencija UN-a vladi zemlje domaćina ustupila skupove podataka o izbjeglicama i migrantima. Nije jasno da li se to stvarno desilo, ali i sama glasina je bila dovoljna da prouzrokuje stres i tjeskobu izbjeglicama i agencijama koje nisu pristale na podjelu skupova podataka sa identitetima izbjeglica, uključujući i biometrijske podatke.[79]

Pojava bolesti COVID-19 stavila je ovu vrstu pitanja u prvi plan jer se humanitarni programi gotovinskih uplata odvijaju paralelno s vladinim programima socijalne zaštite, a vlade traže da humanitarne agencije s njima podijele svoje spiskove korisnika gotovinskih uplata. Razmjena podataka s vladama može narušiti povjerenje između partnera za implementaciju i velikih agencija, a također može učiniti da se izbjeglice i migranti ne žele registrirati i da se boje pristupiti uslugama.[80] Studija provedena na sirijskim izbjeglicama otkrila je da humanitarni radnici i zvaničnici lokalnih vlasti uživaju najniže povjerenje.[81] Jedna druga studija navodi da je od 33% izbjeglica traženo da pruže lične ili osjetljive podatke o svojoj porodici ili situaciji za koje su kasnije žalili što su ih pružili.[82,83]

Ako odemo još i dalje, podaci o djeci mogu se koristiti da se na njih ciljano djeluje kao na potrošače, uprkos propisima u mnogim zemljama koji to zabranjuju. Privatni svjetovi djece otkrivaju se akterima iz privatnog sektora koji imaju komercijalne interese i koji koriste vještačku inteligenciju i algoritme za praćenje i bilježenje svega što dijete radi na internetu, a zatim profiliraju dijete i manipuliraju društvenim okruženjem na internetu na način koji utiče na djetetovu samosvijest, društvene mreže i društveni svijet.[84] Ako organizacija Save the Children ne bude svjesna tih rizika i ako dopusti privatnom sektoru da diktira koji će podaci biti snimani, kako će se koristiti, s kim će se dijeliti i u koje svrhe, onda neće biti u mogućnosti da ublaži rizike i štetu. Neophodni su jasno propisani sporazumi za osiguranje odgovornosti.

B Nedobrovoljni pristanak ili pristanak na osnovu obmane

Pristanak podrazumijeva da osoba ili grupa osoba bude istinski informirana. Kompleksnost novih tehnologija dovodi do nesigurnosti oko toga da li pogođene populacije u potpunosti razumiju tehnologiju, protok informacija, kao i rizike i koristi kada dozvole prikupljanje i obradu svojih podataka.[85] Dinamika moći u tim situacijama može dovesti do toga da ljudi osjećaju pritisak da agencijama ustupe podatke koje ove traže, a to u nekim kontekstima neće predstavljati istinski pristanak.

Utvrditi kada postoji legitiman interes, a kada ne

ICRC je godinu i po razmatrao vrste zaštite koje su neophodne kako bi se biometrijski podaci odgovorno prikupljali i koristili. Utvrđeno je da pristanak nije valjana opcija kada pružanje pomoći zavisi od spremnosti osobe da ustupi svoje biometrijske podatke.

Na kraju je ova organizacija uspjela da uspostavi legitiman interes za prikupljanje biometrijskih podataka u jednom slučaju: za spajanje porodica ili za pronalaženje nestalih, zato što su te aktivnosti od javnog interesa i spadaju u mandat ICRC-a kao globalne humanitarne organizacije.

Međutim, organizacija nije uspjela dokazati da ima legitiman interes za prikupljanje biometrijskih podataka u drugom slučaju: upravljanje korisnicima i distribucijom. To je bilo zato što je prikupljanje biometrijskih podataka u ovom drugom slučaju imalo za cilj da unaprijedi učinkovitost i nije bilo apsolutno neophodno za podjelu pomoći koja se decenijama dijelila bez upotrebe biometrijskih podataka. Pošto biometrijski podaci nisu neophodni za podjelu pomoći, ICRC mora utvrditi da li njegov legitimni interes da uspostavi sistem upravljanja biometrijskim identitetima odnosi prevagu nad potencijalno štetnim posljedicama po prava i slobode ljudi čiji bi se biometrijski podaci snimali.

Provođenje ove procjene vaganja ICRC-ovih legitimnih interesa za prikupljanje ovih podataka u odnosu na potencijalne rizike za prava i slobode korisnika pomoglo je ICRC-u da utvrdi različite opcije za upravljanje programom za biometrijske podatke. Na kraju je ICRC revidirao svoj sistem za biometrijske podatke i našao načina da postigne ravnotežu između svojih interesa za prikupljanje biometrijskih podataka i potrebe da zaštiti privatnost podataka korisnika.[86]

U SAD-u su se u sklopu pilot programa koji je provodilo Ministarstvo domovinske sigurnosti prikupljali DNK profili migranata u imigracijskom pritvoru, uključujući i profile djece. Uzorci DNK prikupljeni su iz briseva unutrašnje strane obraza, a biometrijske informacije su iskorištene za kreiranje profila u nacionalnim krivičnim bazama podataka koje vodi FBI. Zvaničnici su navodili da će odbijanje pristanka na prikupljanje DNK uzorka rezultirati krivičnim gonjenjem. Zvaničnici su u svojoj procjeni uticaja na privatnost priznali da postoji "*...nekoliko rizika koje su istakli zagovarači, uključujući mogućnost da migranti ne budu svjesni svog pristanka na prikupljanje DNK ili da neki pritvorenici, naročito djeca, ne budu svjesni da će informacije biti kontinuirano prosljeđivane FBI-u.*" Kako bi se dijelom ublažili ovi rizici, u ustanovama ICE-a postavljene su obavijesti, a službenici carine i granične straže bili su dužni usmeno upozoriti na ove pojedinosti.[87]

C Obavezno dijeljenje podataka u zamjenu za primanje vitalne podrške

Kako bi radile na zaštiti djece, agencije imaju potrebu da prikupljaju izuzetno osjetljive informacije o djeci koje vlade i kompanije širom svijeta nemaju pravo da prikupljaju. Upravo zato što humanitarne organizacije rade sa informacijama koje se smatraju suviše osjetljivim da bi im vlade i korporacije mogle imati pristup, te organizacije imaju tim veću odgovornost da dobro štite te informacije.

Ljudi koji traže usluge ili sklonište kao izbjeglice, raseljeni ili migranti navikli su da svoje lične informacije daju u zamjenu za vitalnu podršku i usluge.[88] Trgovina ličnim podacima za usluge nije nova etička dilema, kako pokazuje duga tradicija istraživačke etike. Ipak, priroda digitalne sfere i novi načini snimanja podataka i upravljanja podacima doveli su ovu dilemu u prvi plan i nameću dodatno razmatranje etičkih aspekata koje treba uzeti u obzir.[89] Kada se podaci dijele s vladama u kontekstima gdje vlade aktivno uskraćuju prava određenim populacijama, ovo pitanje postaje još složenije.

D Različiti pravni okviri u različitim zemljama usložnjavaju izradu programa za više zemalja

Tehnološki kapaciteti, jezičke razlike, kapacitet mreže, digitalna svijest i različiti pravni okviri znače da ono što bude osmišljeno i izrađeno u okruženju centralnog ureda možda neće biti prevodivo u lokalnom kontekstu.

Tehnološki kapaciteti, jezičke razlike, kapacitet mreže, digitalna svijest i različiti pravni okviri znače da ono što bude osmišljeno i izrađeno u okruženju centralnog ureda možda neće biti prevodivo u lokalnom kontekstu.

Općenito se sektor kreće ka više lokaliziranim politikama privatnosti i zaštite podataka. Ovo kretanje je u velikoj mjeri potaknuto GDPR-om i sve većim priznavanjem potrebe za boljim upravljanjem digitalnim podacima kako bi se zaštitile ugrožene grupe i kako bi se izbjegle novčane kazne i tužbe. Mnoge humanitarne agencije sa sjedištem u Evropi i UK, uključujući i Save the Children, izradile su nove politike zaštite podataka kako bi ispoštovale GDPR koji je stupio na snagu 2018. godine.

Do 2020. godine, 132 od 194 zemlje na svijetu donijele su zakonodavstvo o privatnosti i zaštiti podataka ili je donošenje takvog zakonodavstva bilo u toku.[90] Mnogi od ovih pravnih okvira odražavaju GDPR, ali neki uvode i nove definicije i koncepte. To usložnjava programiranje koje obuhvata više zemalja jer je organizacijama teško pomiriti različite pravne okvire vezane za postupanje s podacima. Na primjer, SAD, EU i Indija koriste različite definicije, pri čemu postoje manje razlike u definiranju kategorija podataka, zbog čega je teško uskladiti orijentaciju i smjernice na globalnom nivou. Globalnim organizacijama je teško da prate različite zakone koji određuju kako trebaju prikupljati, upravljati, razmjenjivati i pohranjivati podatke.[91]

U odsustvu dosljednog pravnog okvira, politike često ne mogu pružiti odgovore na pitanja o tome kako postupati u situacijama kontradikcija u pravu. U humanitarnom sektoru agencije često provode programe u više zemalja, sa ljudima iz više zemalja. Teško je jasno razlučiti ko ima koja zakonska prava i na koga se odnose koji propisi. Neki od sagovornika s kojima su obavljeni razgovori za potrebe ovog izvještaja ovo prepoznaju kao najveću slijepu tačku humanitarne zajednice. Sposobnost pristupa i upotrebe podataka često postoji u zemljama čije vlade nisu u potpunosti demokratske i gdje su pravne i građanske zaštite slabe, a vlade mogu koristiti sofisticirane alate za nadzor da ciljaju i nanesu štetu specifičnim grupama.[92]

Osim toga, digitalni prostor napreduje brže od nacionalnog zakonodavstva. Zato agencije moraju izraditi politike i praksu koje su dovoljno agilne i fleksibilne da se prilagode promjenama u stvarnosti i obuhvate područja za koja još uvijek ne postoji jasno zakonodavstvo.

E Nedostatak zakona o privatnosti podataka fokusiranih na djecu u zemljama domaćinima

Nekoliko zemalja ima specifične pravne okvire koji obuhvataju podatke o djeci, a pošto organizacije moraju poštovati zakon, ovi pravni okviri uticali su na politike agencija.[93,94]

Međutim, mnoge zemlje koje su domaćini izbjeglicama nemaju zakone o privatnosti i zaštiti podataka, niti imaju vlasti koje bi ih provodile. Čak i kada agencija koja radi s izbjeglicama ima vlastite smjernice o upravljanju ličnim podacima, izbjeglice su dužne poštovati zakone i propise zemlje domaćina.[95,96]

Po pitanju konkretno zaštite dječijih podataka, nemaju sve zemlje zakonodavstvo koje definira posebne obaveze prema djeci na koju se podaci odnose. Vlade mogu naći velike količine ličnih podataka o djeci na internetu. Ovaj vid nadzora bio je gotovo nezamisliv u vremenu prije interneta, a iako često nije zakonit ni javno priznat, ipak čini ključni element nacionalne sigurnosti. Ne samo da se ovim podrivaju osnovni pojmovi privatnosti već se narušavaju i ljudska prava, uključujući i slobodu izražavanja. Također se tako otvaraju vrata potencijalnoj zloupotrebi državnih ovlasti.

Nacionalni zakoni i međunarodni dokumenti uglavnom se temelje na principima roditeljskog pristanka za snimanje dječijih podataka. Stoga ne postoji adekvatna zaštita dječijih prava na privatnost u situacijama gdje se ovim podacima pristupa iz ovih novih izvora.[97] Sve implikacije i potencijalni ishodi nisu u potpunosti poznati, ali ako vlade mogu povezati pojedinačne profile s podacima snimljenim putem masovnog nadzora, onda će vlasti biti u stanju da razviju i održavaju evidenciju o cjelokupnom digitalnom životu djece.[98]

Nedostatak posebnih zakona o privatnosti koji se odnose na djecu povlači ozbiljne zabrinutosti za sigurnost djece. Na primjer, raseljeno dijete koje je ranije bilo dijete vojnik moglo bi doći pod digitalni nadzor vlade protiv koje je ranije bilo prisiljeno da se bori, ili dijete s neregularnim migracijskim statusom može biti nađeno putem objave na Facebooku, a kasnije mu vlasti mogu praćenjem utvrditi lokaciju i uhapsiti ga.

Dječiji podaci korišteni za ulaženje u trag neprijavljenih članova porodice

U SAD-u su dječiji podaci korišteni za ulaženje u trag neprijavljenih članova porodice. Agencija koja je bila zadužena za brigu o djeci razdvojenoj od roditelja na granici između SAD-a i Meksika podijelila je informacije o njihovim rođacima i potencijalnim sponzorima u SAD-u sa Ministarstvom domovinske sigurnosti.

Informacije od djece zadržane na granici koja su pokušavala naći članove porodice korištene su da ti članovi porodice budu uhapšeni i deportirani. Posljedica je bila da se *"porodice boje prijaviti da sponzoriraju djecu"* i da se *"djeca koriste kao mamac za prikupljanje nezapamćenih količina informacija od imigrantskih zajednica."*[99]

Kako Save the Children pristupa digitalnoj zaštiti?

Save the Children je prepoznat kao sektorski lider u zaštiti djece. Ova organizacija ima robusne politike za zaštitu djece, a obilje istraživanja i praktičnih vodiča za implementaciju programa dostupno je interno i eksterno putem Resursnog centra organizacije Save the Children.[100] Uredi organizacije Save the Children izuzetno su aktivni u programima zaštite djece, zagovaranja i politika na internetu, a organizaciji je Komisija za dobrotvorna društva UK odala priznanje za njen rad na zaštiti djece i upravljanju rizicima i pohvalila je njene sisteme za prijavljivanje incidenata i upravljanje predmetima.

Kako bismo bolje razumjeli kako se postojeće prednosti organizacije Save the Children prenose i u digitalni prostor, pregledali smo interne dokumente i obavili skoro pedeset razgovora s osobljem iz ureda organizacije Save the Children, uključujući u njenom međunarodnom sjedištu (Centru), tri članska ureda (SAD, Danska, Švicarska) i u pet državnih ureda (Liban, Etiopija, El Salvador, Afganistan i Balkan).

Pim Ras / Save the Children

Organizacija ima solidne temelje na kojima može graditi robusnije napore za digitalnu zaštitu. Konsultacije s akterima ukazuju na to da osoblje organizacije Save the Children ima izrazito razvijenu svijest o zaštiti djece. Članovi osoblja iz svih ureda su rekli da su "svi odgovorni za zaštitu". Čini se da postoji snažan nivo kritičkog razmišljanja o uvođenju digitalnih usluga i o novim tehnologijama u programiranju, kao i duboka zabrinutost da se osigura da digitalne tehnologije i inovacije djeci ne nanesu štetu i da ih ne isključe. Zaštita je suštinska nit koja prolazi kroz organizaciju od početka do kraja programiranja i od dna do vrha organizacije. Politika i praksa zaštite djece i sigurnosti podataka općenito su snažne, a osoblje redovno pohađa obuke o njima. Politike komunikacija i društvenih medija također su dosta razvijene, a osoblje je svjesno njihovog postojanja i u većini slučajeva radi na njihovoj primjeni. Rješavanje specifičnih nedostataka u poznavanju digitalnog prostora i tehnologija, politici i orijentaciji ili smjernicama, koji se navode u ovom izvještaju, pomoglo bi unapređenju prakse zaštite i omogućilo osoblju da osjeća više samopouzdanja u svojim naporima da pruže zaštitu i bezbjedno programiranje, a time bi i organizacija imala više samopouzdanja za inoviranje.

U produžetku teksta dat je pregled svijesti osoblja organizacije Save the Children o rizicima za digitalnu zaštitu i o tome koje su postojeće politike ili prakse uspostavljene interno kako bi se odgovorilo na četiri područja identificirana u našoj tipologiji rizika.

1 Isključenost i samo-isključenost

Članovi osoblja Save the Children s kojima su obavljeni razgovori veoma su svjesni digitalnog jaza i nedostatka pristupa digitalnom okruženju za većinu ugrožene djece s kojima ova organizacija radi. Save the Children učestvuje u nekim programima za pružanje uređaja i edukativnih materijala djeci kako bi nadomjestila ovaj nedostatak pristupa (npr. Centri za sigurnost djece na internetu na Sjeverozapadnom Balkanu). Osoblje širom organizacije dobro je upoznato s tim kako pismenost, jezik, ekonomski status, uzrast i spol/rod mogu doprinijeti smanjenom pristupu digitalnom okruženju. Općenito su programi osmišljeni uzimajući u obzir zajednicu i ideju da zajednice koje rade sa Save the Children moraju imati pristupa uređajima.

Učešće organizacije Save the Children u izradi programa za sigurnost na internetu i za zaštitu djece također je unaprijedilo svijest osoblja o problemu zlostavljanja na internetu za koji neki od članova osoblja tvrde da može dovesti do samo-isključivanja. Naročito je osoblje Save the Children na Balkanu bilo svjesno potrebe za izgradnjom povjerenja među mladim ljudima ako želimo da oni koriste digitalne aplikacije ili da pružaju podatke. U Afganistanu je osoblje dosta govorilo o potrebi za uključivanjem zajednice i o lokalnoj procjeni rizika prije uvođenja tehnoloških uređaja i prikupljanja podataka na internetu zato što upotreba ovih uređaja može skrenuti pažnju oružanih grupa na organizaciju i dovesti u opasnost svakog ko učestvuje u takvim aktivnostima.

Područja koja treba osnažiti

Save the Children ima inkluzivan i konsultativan pristup u svom radu. Međutim, organizaciji bi dobro došla redovna, lokalizirana istraživanja o vrstama uređaja, platformi, kanala komunikacije i medijskih internetskih stranica koje koriste djeca u pokretu i raseljena djeca u različitim kontekstima, jer se to brzo i redovno mijenja. Ostati u toku promjena u tehnologiji i načina na koji je djeca koriste pomoglo bi organizaciji da bude sigurna da neće isključivati djecu kada osmišljava digitalne programe i komunikacije. U sklopu ovih napora Save the Children treba istražiti problematiku povjerenja u digitalnu tehnologiju kao i u razne agencije u širem sektoru, stavove prema privatnosti i iskustva djece na internetu i različitim platformama, a sve kako bi stekla bolje razumijevanje razloga za samo-isključivanje.

2 Šteta prouzrokovana humanitarnim inovacijama

Među nekim članovima osoblja postoji zabrinutost da bi Save the Children mogao postati kanal za provođenje humanitarnih inovacija u nereguliranom okruženju. Prema riječima jednog člana osoblja: *"Ljudi ne razmišljaju o budućoj upotrebi i primjeni tehnologija koje još uvijek ne razumijemo. Obično se povinujemo standardu sektora. Ali šta je sa dugoročnim posljedicama nekih od ovih pristupa?"* Prema nekim članovima osoblja, do ovog konformizma u sektoru dolazi zbog natjecanja za finansije, a ponekad i zbog zahtjeva donatora. Osoblju na nižim nivoima u organizaciji može biti teško suprotstaviti se potencijalno opasnim ili rizičnim inovacijama koje se uvrštavaju u prijedloge za finansiranje.[101]

Procjene rizika ne uključuju sistematično specifična pitanja o inovativnim pristupima, podacima i digitalnoj tehnologiji. Umjesto toga, čini se da je do pojedinačnih timova kako će ova pitanja uvrstiti u svoje procjene rizika. Uredi za programe organizacije Save the Children posjeduju različite stepene stručnog znanja o novim tehnologijama i vrstama pitanja oko zaštite podataka koja se pojavljuju kod novijih tehnologija i platformi ili s novijim pristupima podacima koji prevazilaze tradicionalno prikupljanje i obradu podataka. Odnosi moći između donatora, privatnog sektora i raznih ureda organizacije Save the Children također znače da rizični programi ili praksa mogu biti odobreni ako se smatra da donose koristi kao što su finansiranje ili unapređenje položaja organizacije.

Iako većina osoblja iz Save the Children s kojima smo razgovarali kaže da svi prijedlozi budu pregledani prije podnošenja kako bi se utvrdili i ublažili potencijalni problemi u zaštiti djece, nisu svi članovi osoblja s pouzdanjem mogli reći da su novi rizici u pogledu digitalne zaštite dovoljno ispitani, a u nekim slučajevima je proces pregledanja novih inicijativa i prijedloga bio nedovoljno jasan. Osoblje koje radi na prikupljanju sredstava za inovacije navodi da postoji etički odbor za programe javnog zdravlja i etička komisija, ali da nisu sigurni da li se u ovim forumima razmatraju i zaštite u digitalnom okruženju i na internetu. Osoblje je također izložilo zabrinutost zbog toga što proces procjene rizika nije dovoljno institucionaliziran i sistematičan i da postoji nedostatak ekspertize i obuke za procjenu inovacija, novih tehnologija i novih vidova snimanja i upotrebe podataka.[102,103] Ranije se Save the Children u procjenama rizika fokusirao na bezbjednost i sigurnost, zaštitu djece, rizike izgradnje i medicinske/farmaceutske rizike.

Save the Children još nije uvrstio analizu rizika vezanih za inovacije, nove vidove partnerstva, razmjenu podataka i nove tehnologije u svoj proces procjene rizika

Save the Children još nije uvrstio analizu rizika vezanih za inovacije, nove vidove partnerstva, razmjenu podataka i nove tehnologije u svoj proces procjene rizika. Proces je osmišljen tako da ga u pogledu ključnih područja rizika usmjeravaju uredi u zemljama, ali ipak se pojavljuju izvjesna etička pitanja vezana za javno-privatna partnerstva, inovacije i upotrebu podataka koja se moraju označiti i riješiti na nivou organizacije.[104]

Nedostatak krovnog etičkog okvira, uz ograničene kapacitete i ekspertizu za inovacije i digitalna pitanja izlaže djecu, kao i Save the Children i njegove partnere riziku. Pored toga, nedovoljno pažnje se posvećuje procjeni uticaja novih tehnologija u programima Save the Children. Kako navodi jedan član osoblja, *"mnogo je interesa u organizacije oko inovativnosti i korištenja više tehnoloških alata. Više koristi vidimo od tehnologije koja pomaže projektima da postanu efikasniji ili prošire svoj obim nego od tehnologije koja zapravo donosi koristi našim korisnicima. Volio bih da mogu reći da je djeci bolje, ali za to ne vidim puno dokaza."*[105]

Područja koja treba osnažiti

Save the Children treba uspostaviti sistematičniji i institucionaliziraniji pristup procjeni i ublažavanju rizika u ovom području, uključujući i multidisciplinarni nadzorni odbor i dobro informiranog pravnog savjetnika. Kada bi imao snažnije, više strukturirane sisteme i kapacitete za pregledanje digitalnih zaštita i procjenjivanje potencijalnih rizika, kao i za mjerenje koristi od inovacija i tehnologija, to bi za Save the Children omogućilo da sa više pouzdanja ulazi u nova inovativna programska područja i da u izradi svojih programa koristi nove tehnologije. Kako Save the Children bude osnaživao svoje lokalne urede i osoblje da donose odluke o rizicima na koje se treba više fokusirati, bit će potrebni dodatna obuka i kapaciteti kako bi osoblje bilo sigurno da posjeduje odgovarajuće znanje, vještine i podršku da donosi te odluke. Kako se budu pojavljivali novi pristupi, ako se te odluke prepuste pojedincima moguće je da ljudi "neće znati šta ne znaju", a to bi moglo prouzrokovati štetu.

Osim toga, razvoj okvira za istraživanje, praćenje i evaluaciju omogućit će organizaciji da identificira i donese odluke o kratkoročnim i dugoročnim koristima, rizicima i negativnim posljedicama eksperimentacije i inovacije.

3 Povećana opasnost od štete na internetu

Upotreba platformi društvenih medija, aplikacija i interneta u širem smislu – ili stvarna ili željena – čini dio dječijih svjetova. Noviji kanali digitalne komunikacije imaju veliki potencijal za rad Save the Children, a zbog karantena povodom pandemije COVID-19 osoblje se sada više na njih oslanja kako bi kontaktiralo s lokalnim zajednicama, partnerskim organizacijama i djecom. Digitalni svijet je poznat po svojim nepredvidivim promjenama trendova i navika, a organizacijama je često teško održati ažuriranost svojih mjera zaštite na internetu. Izazov je kako pomoći djeci i mladima da iskoriste ono što nude digitalne tehnologije, a istovremeno ih podržati u bezbjednom korištenju digitalnih platformi u sklopu programa Save the Children i u njihovim privatnim životima.

Osoblje Save the Children općenito ima veoma visok stepen svijesti o koristima i potencijalnim rizicima koji nastaju kada djeca samostalno koriste internet i mobilne telefone i kada Save the Children djeci uvede uređaje ili digitalne kanale ili kada u svom radu koristi digitalne platforme, alate i kanale društvenih medija. Nekoliko sagovornika iz različitih dijelova organizacije spomenulo je da učestvuju u programiranju zaštite djece na internetu, a većina osoblja također navodi da provode procjene rizika i mapiraju rizike kada započinju programe koji će djecu izložiti

Sprečavanje iskorištavanja i nasilja na internetu na Balkanu

Na Balkanu Save the Children provodi projekat za prevenciju seksualnog iskorištavanja i nasilja nad djecom u digitalnom okruženju. Ovo obuhvata rad s policijom; specijalizirane alate za obuku i softver za pronalaženje slučajeva zlostavljanja na internetu; rad sa školama na izradi specifičnih nastavnih programa za unapređenje svijesti među djecom o tome kako se mogu zaštititi i zagovaranje zakonodavnih rješenja.

Program okuplja NVO i institucionalne partnere koji rade na postizanju zakonskih izmjena u području društvenih mreža,[108] a ured Save the Chidlren na Balkanu također je proveo istraživanje o ovoj temi.[109] Deset članskih ureda radi na zaštiti djece na internetu kako u okviru svojih nacionalnih programa tako i globalno.[110]

Snažne politike za društvene medije usmjeravaju osoblje po pitanjima kao što su pristanak za upotrebu fotografija i članaka u komunikacijskom radu, zaštita identiteta i upravljanje slikama djece, kao i zabrana direktnog kontakta s djecom putem društvenih medija. Članovi osoblja često su se pozivali na politiku za društvene medije kada su govorili o politikama svoje organizacije za zaštitu djece.[111]

Djeca u pokretu i raseljena djeca koja dolaze iz situacija gdje su bila izložena nasilju i sukobima mogu smatrati da je primjereno dijeliti slike koje bi kod drugih izazvale šok. Zbog ovoga je teško procijeniti u kojem trenutku bi osoblje trebalo intervenirati.[112]

Save the Children koristi dječije slike i priče kao potporu aktivnostima prikupljanja sredstava i zagovaranja, ali njihovo objavljivanje na društvenim medijima i drugim kanalima može izložiti djecu zlostavljanju. Ponovo, za ovo područje postoji jasna politika, pa ipak osoblje koje radi na komunikaciji navodi da je pribavljanje pristanka za korištenje slika i priča stalni izazov. Anonimne fotografije su manje rizične, ali također privlače manje angažiranosti i manje su efektne za potrebe prikupljanja sredstava i zagovaranja. Osoblje prati utvrđeni proces pristanka, a na izazove nailazi kada dijete ne želi da se njegova slika koristi, ali se osjeća dužnim prema organizaciji Save the Children zbog pogodnosti kojima je pristupilo putem programa ove organizacije.

Save the Children

Teško je procijeniti da li ljudi razumiju kako će se njihove priče i slike koristiti i gdje mogu završiti. Djeca, roditelji i staratelji često ne znaju razliku između 'Facebooka' i 'društvenih medija'. Mogu dati pristanak za objavljivanje svojih slika i priča na društvenim medijima, ali ga povući kada shvate da ti mediji podrazumijevaju i Facebook.[113]

Osoblje u nekoliko nacionalnih ureda navodi da snažne, stroge politike Save the Children o društvenim medijima ne funkcioniraju dobro za male partnerske organizacije kojima nedostaje osoblja, znanja, kapaciteta, sistema i budžeta da bi ispunile standarde Save the Children.

Područja koja treba osnažiti

Save the Children mora ažurirati, lokalizirati i kontekstualizirati svoje politike za zaštitu djece na internetu kako se budu pojavljivale novije tehnologije i kako djeca budu sve više koristila ove uređaje i platforme bez nadzora organizacija i pazitelja, kao što je često slučaj s djecom u pokretu i raseljenom djecom. Ovo treba biti područje stalnog istraživanja i investicija. Ažurirane i kontekstualno specifične politike za digitalnu zaštitu također su neophodne i za Save the Children i za partnerske organizacije koje mogu raditi na različitim rizicima i faktorima rizika u skladu sa životnim iskustvima djece i resursima i kapacitetima na lokalnom nivou.

Save the Children mora uspostaviti regulatorni okvir sa svojim partnerima kojim će osigurati da imaju neophodne kapacitete i razumijevanje tehnologije. Osoblje je također tražilo dodatne smjernice o izradi memoranduma o razumijevanju s partnerima koji pružaju uređaje (npr. kako bi obuhvatio pitanja kao što su softver koji blokira neprimjerene internetska stranice, neprimjeren sadržaj, prati upotrebu tableta) i dodatnu orijentaciju o obavezama Save the Children i obavezama korisnika i partnera.[114] Ovo je naročito bitno s obzirom na veću fokusiranost na lokalizaciji i implikacije COVID-19 koje su dovele do većeg oslanjanja na lokalne partnere.

Čak i sa snažnim politikama, osoblju je teško procijeniti potencijalne koristi i rizike digitalnih kanala. Prema mnogim članovima osoblja, potrebno je revidirati i ažurirati politiku Save the Children o društvenim medijima kako bi odražavala stvarno stanje upotrebe društvenih medija u programima, operacijama i među djecom i mladima.
Potrebno ju je učiniti kontekstualno relevantnijom, dovoljno fleksibilnom da se brzo prilagođava promjenama na platformama i da se mijenja kako djeca budu prelazila s platforme na platformu, a osoblju treba da pomogne u razlučivanju različitih rizika za djecu. Moguće je da neće uvijek postojati čvrsto ustanovljena pravila i da će biti potrebni mehanizmi za pristup savjetima za različite situacije, a ponekad i za konkretan slučaj.

4 Zloupotreba podataka i nepravilno postupanje s podacima

Save the Children ima snažne protokole za sigurnost podataka koji su centralizirani i primjenjuju se širom organizacije. Ovi protokoli obuhvataju registraciju i šifriranje uređaja, višestruku autentifikaciju za laptope i mobilne telefone, daljinsko brisanje, upotrebu pohranjivanja u oblak i SharePoint (pohrana datoteka kojoj osoblje može daljinski pristupiti), internu razmjenu datoteka putem One Drive, kontrolu pristupa podacima i sistemima, antivirusni softver i IT politike i procedure kao što su privatnost podataka i klauzule o povjerljivosti i razmjeni podataka u ugovorima i sporazumima o partnerstvu.[115]

U svim uredima osoblje se poziva na širok raspon politika i prakse za zaštitu podataka. Osoblje očekuje od timova za IT da ih blagovremeno obavještavaju o problematici sigurnosti podataka, društvenih medija i digitalnih komunikacija.[116] Zemlje koriste zaštitni sistem za upravljanje informacijama koji se zove DATIX za centralno upravljanje predmetima zaštite djece. Zabrinutosti se prijavljuju preko interneta, a sistem automatski obavještava relevantne osobe u nacionalnim uredima, regionalnim uredima i globalno. Narednim koracima se upravlja kroz sistem.[117] Zemlje koje provode sponzorstvo djece također imaju zaštićenu bazu podataka za upravljanje podacima o sponzorstvu djece.

Digitalno upravljanje predmetima dječije zaštite ne provodi se dosljedno... to je dovelo do nedosljednog upravljanja zaštitom djece.

Save the Children International je 2017. godine počeo s primjenom politike za zaštitu podataka kako bi ispoštovao uredbu GDPR[118] koja se smatra najsnažnijim okvirom za zaštitu podataka na svijetu. Obuka je provedena širom raznih ureda koji su ohrabreni da prilagode politiku zaštite podataka svom lokalnom kontekstu i pravnom okruženju. GDPR je bila katalizator da Save the Children implementira više politika i procedura vezanih za podatke.[119] Iako su globalne politike Save the Children za IT i zaštitu podataka snažne i nastoje postići usklađenost s najstrožim propisima o zaštiti podataka, još uvijek postoje nedostaci u implementaciji i kontekstualizaciji kod toga kako različiti uredi snimaju, obrađuju i razmjenjuju podatke. Osoblje iz Save the Children International navodi da je koncept zaštite podataka za mnoge unutar organizacije još uvijek nejasan. Prema osoblju iz Save the Children UK, prvobitni pokušaj izrade globalne obuke bio je pod pretjeranim uticajem zakonodavstva UK i suviše složen, uz obilje pravnih formulacija. Drugi pokušaj globalne obuke je u pripremi, a ovaj put će biti prilagođenija osobama kojima engleski nije prvi jezik. Organizacija također još uvijek radi na primjeni politika na nivou nacionalnih ureda.[120]

Digitalno upravljanje predmetima dječije zaštite ne provodi se dosljedno. Save the Children je jedinstvena organizacija, ali ipak funkcionira kao federacija. Save the Children International direktno upravlja nacionalnim uredima, ali nema nadležnosti nad uredima (za prikupljanje sredstava) svojih članica. Ovo je dovelo do porasta nedosljednog upravljanja zaštitom djece u zavisnosti od toga da li se radi o Save the Children International ili članicama Save the Children.

Izgleda da u nacionalnim uredima postoji dobra praksa upravljanja podacima (npr. datoteke zaštićene lozinkom, brisanje podataka nakon završetka predmeta), ali ovo područje bi možda trebalo dodatno ispitati kako bi osigurali da osoblje ima neophodne alate i da su ti alati dosljedni i sigurni. Također, DATIX u nekim slučajevima nije usklađen s lokalnim procesima, kako se navodi u nekoliko ureda. To navodi osoblje da uspostavi duple sisteme (na primjer, tabele u Excelu) koji su manje sigurni u pogledu privatnosti i zaštite podataka.

Također se radi na testiranju tehnologije za sisteme digitalnog upravljanja predmetima dječije zaštite koji bi trebali pomagati timovima i socijalnim radnicima. Ponovo postoji nedosljednost u organizaciji u pogledu sistema koji se koriste i povjerenja koje osoblje prema njima pokazuje. Neki članovi osoblja su izuzetno angažirani u njihovoj implementaciji dok su drugi zabrinuti da će podaci iz sistema biti podijeljeni s vladom, a neki sumnjaju da će sistemi funkcionirati, pa su napravili vlastite pojednostavljene aplikacije za koje misle da se bolje uklapaju u njihov kontekst. Na primjer, osoblje na Balkanu navodi da djeca zbog nedostatka povjerenja često daju lažna imena i lažne datume rođenja, pa je teško bilo koga od njih pratiti, čak i u korisne svrhe.

Područja koja treba osnažiti

Osoblje Save the Children je po svemu sudeći svjesno sigurnosti podataka i posjeduje snažan centralizirani pristup. Upoznati su s rizicima za privatnost, ali uviđaju i da ovo područje nije riješeno na isti način širom institucije kao drugi vidovi zaštite i da postoji nedostatak znanja i kapaciteta veznih za nove vidove rizika za privatnost i zaštitu podataka.

Složena priroda snimanja, obrade i razmjene podataka znači da je teže procijeniti potencijalne rizike. Nedostaci postoje u pogledu svijesti, obuke i resursa. Postoji potreba za predvodnicima koji bi pomogli širenju dobre prakse kroz organizaciju. Save the Children nije usamljena u ovom i dobro bi joj došla izrada smjernica za dobru praksu i pokretanje izgradnje kapaciteta u saradnji sa širim sektorom. Kako je napomenuto u vezi s rizicima eksperimentacije i digitalnih inovacija, osoblje "ne zna šta ne zna", a to može značiti da ne postoji dovoljno kapaciteta za identificiranje i ublažavanje rizika.

Osoblje iz nekoliko nacionalnih ureda navodi da bi voljeli imati praktične smjernice za zaštitu i upravljanje podacima koje će biti kontekstualno i operativno relevantne. Obim ovih politika mora biti prilagođen lokalnoj situaciji. Stabilni kampovi i više privremeni konteksti zahtijevaju različite pristupe, a teški masivni sistemi vjerovatno neće najbolje odgovarati potrebama osoblja.[121]

Osim toga, lokalni partneri često nemaju kapacitete za implementaciju kompliciranih standarda niti neophodne IT sisteme za sigurno upravljanje podacima. Ovo pred Save the Children postavlja izazov u smislu pridržavanja politika o podacima i očuvanja sigurnosti dječijih podataka. Organizacija je pokušala izbjeći da rizik prebaci na partnere, ali izgradnja kapaciteta podrazumijeva troškove kojih donatori nisu uvijek svjesni i koje nisu uvijek spremni platiti.[122] Kako navodi jedan član osoblja, *"važno nam je da zagovaramo kod donatora kako bi počeli priznavati troškove dječije zaštite u prijedlozima projekata... Potrebno nam je finansiranje zaštite, ne samo za Save the Children, već i za naše partnere."*[123]

Osoblje ima specifična pitanja o tome kako bezbjedno koristiti podatke u specifičnim situacijama. Imaju brojna pitanja i potrebe za podrškom kroz širok raspon tehnologija i situacija, ali dostupna je tek ograničena podrška. Na primjer, osoblje s kojim su obavljeni razgovori za potrebe ovog izvještaja zatražilo je dodatnu podršku i smjernice o razmjeni podataka s partnerima, recikliranju lokalnih brojeva mobilnih telefona u sekundarne svrhe u vanrednim okolnostima, korištenju WhatsApp aplikacije za upravljanje predmetima dječije zaštite u kontekstu kampova, uspostavljanju enkripcije za aplikacije za prikupljanje podataka otvorenog koda (open source), vlasništvu podataka, čuvanju i brisanju podataka.[124]

Općenito postoje izazovi u pogledu korištenja fotografija djece. Iako postoji politika koja se na ovo odnosi, osoblje u nekim uredima tražilo je specifične smjernice za upravljanje fotografijama snimljenim na ličnim uređajima i za dijeljenje priča i fotografija raseljene djece i djece u pokretu. Neki su zabrinuti da bi donatori mogli reidentificirati djecu iz studija slučaja ako na svojim internetskim stranicama i društvenim medijima podijele njihove fotografije i priče. Dosta je smjernica dostupno, ali je teško sve to primijeniti u praksi, a smjernice se nekad ne odnose na širok raspon piranja koja se pojavljuju u praksi.[125–127]

Pristup humanitarnog sektora digitalnoj zaštiti

U studiji Save the Children iz 2019. godine o raseljenoj djeci i novim tehnologijama[128] preporučuje se institucionaliziranija politika i praksa za smanjenje potencijala za štetu od digitalnih inovacija i digitalnog programiranja. Uz primarnu zabrinutost o riziku za djecu, također postoji i zabrinutost oko usklađenosti i pravnih rizika za organizaciju, uzimajući u obzir nove propise o privatnosti i zaštiti podataka koji su usvojeni u nekoliko zemalja širom svijeta u proteklih nekoliko godina. Kako bude više digitalnog programiranja u sektoru i kako se budu nastavljale adaptacije i restrikcije neophodne zbog pandemije bolesti COVID-19, tako će uticaj i razmjeri ovih rizika najvjerovatnije također rasti.

Uz primarnu zabrinutost zbog rizika za djecu, postoji i zabrinutost oko usklađenosti i pravnih rizika za organizacije

Sveobuhvatan pregled postojećih operativnih i akademskih istraživanja, pravnih okvira, sive literature i dokumenata sa smjernicama humanitarnog sektora pokazao je da samo nekoliko resursa specifično govori o ukrštanju dječije zaštite i digitalnog programiranja, odnosno inovacija (vidi u Prilogu 2 spisak pregledanih dokumenata). Nijedan od dokumenata nije se holistički i specifično osvrnuo na digitalne zaštite u kontekstu djece u pokretu i raseljene djece. Međutim, nekoliko dokumenata sadrži neke aspekte smjernica i dobre prakse. Stoga, a da bi se stekli dalji uvidi u to kako sektor u širem smislu odgovara na problematiku zaštite djece vezanu za upotrebu digitalnih tehnologija, obavljeno je 12 razgovora s ključnim ispitanicima koji su vanjski stručnjaci identificirani pregledom literature. Uz pomoć postojećih politika identificirano je pet elemenata za učinkovitu digitalnu zaštitu: inkluzivni dizajn programa; dubinsko ispitivanje i procjene rizika za inovativna partnerstva; smjernice za zaštitu djece na internetu; smjernice za netradicionalno upravljanje podacima i procedure upravljanja i odgovornosti.

Inkluzivni dizajn programa

Inkluzivni dizajn programa pomaže agencijama da bolje razumiju digitalno okruženje i kontekst tako da njihovi programi ne isključuče djecu koja nemaju pristupa digitalnom okruženju ili koja nisu zastupljena u skupovima podataka.[129] Neke postojeće smjernice pružaju orijentaciju o provođenju istraživanja o tome kako djeca ostvaruju pristup digitalnim uređajima i internetu i kako ih koriste.[130]

Bilo bi korisno da postoje dodatne smjernice o provođenju analize dizajna programa i rizika u odnosu na koristi kako bi se identificirala područja gdje može doći do samo-isključivanja. Dizajneri programa bi onda mogli riješiti ta pitanja prije početka implementacije.[131] To bi uključivalo orijentaciju o istraživanju za potrebe dizajna kako bi se steklo razumijevanje pristupa koji djeca imaju i njihovih navika, za koje postojeće stranice i aplikacije vjeruju da su bezbjedne, kojim organizacijama i tijelima vjeruju, a kojim ne i zašto (vidi poglavlje o bezbjednom istraživanju u dokumentu Savjeti i smjernice o digitalnoj zaštiti organizacije Girl Effect).[132] Ublažavanju isključivanja i samo-isključivanja doprinijeli bi i bolja politika i smjernice za provjeru partnerstava (kako je opisano u poglavlju o bezbjednijim iskustvima na internetu i društvenim medijima), za zaštitu podataka i za institucionalno upravljanje podacima i veću odgovornost.[133]

Dubinsko ispitivanje i procjene rizika za inovativna partnerstva

Tek veoma mali broj politika postavlja 'velika' etička pitanja o humanitarnim inovacijama. Na primjer, kakve bi mogle biti dugoročne posljedice uvođenja određene tehnologije ili novog pristupa? Ako je cilj remetilačka inovacija, koga se remeti i kakve bi mogle biti posljedice? Osoblje može biti svjesno da mora zaštititi podatke, ali zaboraviti da prethodno postavi najvažnije pitanje: da li bismo uopće trebali ovo raditi? U proteklih pet godina prostor humanitarnih inovacija počeo je obraćati pažnju na to kako praćenje, evaluacija i učenje mogu podržati odgovornije inovacije. To je proizašlo iz uviđanja da inovacije mogu napraviti štetu na niz raznih načina, jednako kao što mogu donijeti koristi.

Tek veoma mali broj politika postavlja 'velika' etička pitanja o humanitarnim inovacijama. Osoblje može biti svjesno da mora zaštititi podatke, ali zaboraviti da prethodno postavi najvažnije pitanje: da li bismo uopće trebali ovo raditi?

Politike i procedure mogle bi pomoći da se riješe uzvodne implikacije potencijalno štetne tehnologije koje proizlaze iz inovativnih partnerstava s privatnim sektorom. Ono što nedostaje u setu alata za politike je proces dubinske provjere i procjene rizika kod potencijalnih koristi i štete (specifične za djecu) koje stvaraju inovativna partnerstva. Ova vrsta smjernica pomogla bi organizacijama da razmotre potencijal kratkoročnih i dugoročnih implikacija partnerstva i da potkrijepe odluke o tome da li u takvo partnerstvo ući ili ne.[134] Na kraju, često je zaštita djece prije ne činiti nešto nego činiti nešto, kako kaže jedan stručnjak za etiku i inovacije u humanitarnom sektoru.[135] Jedan naučni rad iz 2018. godine razvrstao je rizike humanitarne eksperimentacije kako slijedi:

1. temeljni trendovi i rizik od štete;
2. distribucija štete: etička varijabilnost u humanitarnom prostoru;
3. distribucija resursa i razmatranja oskudice i
4. pravna odgovornost i šteta po ugled.

Response Innovation Lab (RIL) nudi set alata za praćenje i evaluaciju inovacija koji obuhvata, na primjer, izradu prototipa, pilotiranje i skaliranje,[136,137] a Principi digitalnog razvoja nude smjernice o dizajniranju digitalnog programiranja na osnovu postojeće dobre prakse i ranije naučenog.[138] Ni jedan ni drugi dokument ne razmatraju djecu specifično. Smjernice organizacije Girl Effect iz 2018. godine o digitalnoj zaštiti obuhvataju inicijalni set pitanja o tome da li je inicijativa etički prihvatljiva ili podobna, a to bi moglo poslužiti kao polazište za dalju razradu ovog područja.[139] Bilo bi potrebno prilagoditi i ažurirati ova pitanja kako bi se usmjerila na djecu u pokretu i raseljenu djecu.

Temeljni humanitarni imperativi i principi također bi mogli poslužiti kao osnova za procjenu rizika kod humanitarne eksperimentacije:

1. nenanošenje povreda,
2. humanost,
3. neutralnost,
4. nepristrasnost i
5. nezavisnost.

Pritom bi ih trebalo preorijentirati ka praktičarima i prilagoditi perspektivi djece u pokretu i raseljene djece. [140]

Smjernice za zaštitu djece na internetu

Posljednjih nekoliko godina zaštita djece na internetu nalazi se na samom vrhu popisa zabrinutosti za mnoge organizacije koje rade s djecom. Dosta je smjernica za djecu; nastavnike, škole i vannastavne aktivnosti; vlade i industriju, kojima je cilj unaprijediti sigurnost djece na internetu.[141–144] Organizacija Save the Children izradila je 2014. godine, kroz konsultacije s drugim organizacijama čiji je rad fokusiran na djecu, dokument sa smjernicama Sigurnost djece na internetu,[145] a 2019. je izdala i Operativni priručnik za Centre za sigurnost djece na internetu.[146] Agencije također počinju objavljivati specifične smjernice vezane za COVID-19 o tome kako se pobrinuti za sigurnost djece na internetu u periodu kad su možda češće na internetu zbog virtuelnog školovanja i karantena.[147,148]

Zaštita djece postala je kompliciranija u okruženju interneta, na primjer kada dijete u nekom prostoru na internetu objavi da je bilo žrtva zlostavljanja. Agencije nisu uvijek dobro pripremljene da znaju kako postupati s takvim otkrićima, naročito ako komunikacijski ili digitalni tim vodi internetsku stranicu, a ne postoji već uspostavljen protokol za zaštitu djece. Ukazivanje lokalnim službama također može biti izazov s obzirom na globalnu prirodu interneta i ranije spomenute rizike za zaštitu podataka ako se od djece prikupljaju podaci o lokaciji. Savjeti i smjernice o digitalnoj zaštiti koje je izradila organizacija Girl Effect pružaju orijentaciju za postupanje u slučaju otkrića, usmjeravanja, uspostavljanja protokola za prijavljivanje na internetu, preporuka za stvaranje sigurnih i zdravih zajednica i prijedloga za moderiranje zajednica na internetu, ali postupanje u ovoj vrsti slučaja još uvijek predstavlja problem za cijeli sektor.[149]

Smjernice za upravljanje netradicionalnim podacima

Mali broj dokumenata specifično govori o odgovornom upravljanju podacima u slučaju djece, digitalnim podacima i tehnologijama, a obuhvataju i neke aspekte konteksta migracije i raseljenosti, međutim nijedan nije specifično osmišljen da osigura digitalnu zaštitu djeci migrantima i raseljenoj djeci.[150–154] Drugi dokumenti obuhvataju djecu u digitalnom svijetu, ali ne uključuju specifično kontekst migracije i raseljenosti.[155–158] Dosta je politika i povezanih dokumenata koji razmatraju upravljanje podacima u humanitarnim agencijama. Mnogi od njih spominju djecu u smislu pristanka ili prepoznaju osjetljivost dječijih podataka, ali ne bave se detaljno djecom i njihovim podacima na holistički način.[159–163] Dokumenti politike i smjernica o upravljanju podacima za vrijeme vanrednih situacija ili u kontekstu krize također postoje, ali ni oni se ne fokusiraju specifično na djecu i njihove podatke.[164–171] Ovo je područje koje je još uvijek u razvoju, a u prvom planu još nema agencija fokusiranih na rad s djecom.

Mali broj dokumenata specifično tretira odgovorno upravljanje podacima u slučaju djece, digitalnih podataka i tehnologija ... u svrhu digitalne zaštite djece u pokretu i raseljene djece.

Većina politika i smjernica o zaštiti podataka koje imaju agencije tretira tradicionalne, linearne vrste prikupljanja i upotrebe podataka, gdje agencija ili njeni partneri sami prikupljaju podatke i upravljaju njima. Ne osvrću se na to kako bi agencije mogle ili trebale pristupiti i koristiti netradicionalne formate podataka kao što su veliki podaci ili skupovi podataka koji su prikupljeni ili koje pruža privatni sektor (npr. evidencija podataka s mobilnih telefona od telekomunikacijskih kompanija ili podaci sa zadnjeg kraja (back-end) od tehnoloških kompanija). Zabrinjavajuće je što se samo nekoliko dokumenata sa smjernicama[172,173] osvrće na zaštitu demografski prepoznatljivih podataka, drugim riječima, podataka pomoću kojih je moguće identificirati širu grupu pojedinaca i/ili njihovu lokaciju. Većina politika i smjernica sadrži nedostatke u smislu etike i izazova podataka prikupljenih za potrebe prediktivne analitike, upotrebe prepoznavanja lica i biometrije i snimanja lokacijskih podataka.

Također postoji nedostatak osvrta na sve veću lakoću reidentifikacije navodno anonimiziranih podataka putem novih metoda ili uslijed tzv. 'efekta mozaika' u kojem se kombiniranjem velikih skupova podataka s različitim vrstama informacija o istoj osobi ili osobama može nehotice (ili namjerno) otkriti identitet osobe ili osoba. UN OCHA trenutno dublje istražuje ovu temu, ali još uvijek nisu izdate smjernice.[174]

Općenito je nedovoljno jasno kako upravljati razmjenom podataka i baza podataka s lokalnim i međunarodnim partnerima za implementaciju, donatorima, vladama i/ili privatnim sektorom.[175] Neke organizacije značajno su zabrinute za sigurnost podataka, naročito na nivou lokalnih partnera i osoblja s prvih linija koje možda nema redovan pristup digitalnim uređajima, sigurnoj ili dosljednoj mobilnoj ili Wi-Fi mreži ili dovoljnoj pojasnoj širini neophodnoj za korištenje alata i sigurnosnih protokola koji su obavezni za cijelu organizaciju. Osim toga, dok su se neke organizacije fokusirale na opasnost od vanjskih hakerskih upada, rješavanje problema povrede podataka zbog nepažnje ili loše sigurnosne prakse (kao što je dijeljenje lozinki ili infekcija virusom ili špijunskim softverom) možda je i najveći izazov.[176]

Procedure za upravljanje podacima i odgovornost

Politike često ne mogu odgovoriti na pitanje šta činiti u slučaju nepostojećih ili nedosljednih pravnih okvira u različitim zemljama.177 Prilagođavanje kontekstu je izazov za krovne politike digitalne zaštite. Tehnološki kapaciteti, jezičke razlike, kapacitet mreže, digitalna svijest i različiti pravni okviri, sve to znači da ono što bude osmišljeno i izrađeno u okruženju centralnog ureda možda neće biti prevodivo u lokalnom kontekstu.

Prilagođavanje kontekstu je izazov za krovne politike digitalne zaštite. Tehnološki kapaciteti, jezičke razlike, kapacitet mreže, digitalna svijest i različiti pravni okviri, sve to znači da ono što bude osmišljeno i izrađeno u okruženju centralnog ureda možda neće biti prevodivo u lokalnom kontekstu.

Pored toga, vanjskim akterima s kojima smo obavili razgovore često nije jasno ko je odgovoran za koji dio politike i prakse digitalne zaštite i koji nivo vještina i svijesti je neophodan u različitim dijelovima organizacije kako bi se osiguralo poštivanje politike.

Izazovi vezani za jezik (većina dokumenata je na engleskom), vrijeme, format i kapacitet stvaraju barijere za implementaciju politika zaštite podataka.178 Ostaje hitna potreba za boljim upravljanjem podacima i većom odgovornosti na nivou vlada, korporacija i agencija. UNICEF radi na manifestu Upravljanja podacima za djecu koji će se zalagati za veću zaštitu dječijih podataka, veću etičnost poslovnih modela u slučaju privatnog sektora i više odgovornosti na svim stranama. Ovo bi moglo pružiti osnovu za izradu daljih smjernica o odgovornosti i upravljanju.[179]

Unutar organizacija moguće je da se pojave tenzije između timova za inovacije, razvoj poslovanja i prikupljanje sredstava, s jedne strane, i timova za zaštitu djece i privatnost podataka s druge.[180] Osim toga, neophodno je više učiniti na raščlanjivanju materijala o zaštiti podataka i digitalnoj zaštiti tako da od pravnih i tehničkih formulacija dobijemo probavljive koncepte koje osoblje i partneri mogu razumjeti i primijeniti lokalno i u svom kontekstu.

Juozas Cernius / Save the Children

ZAKLJUČNA RAZMATRANJA I NAREDNI KORACI

Čvrsto uporište koje Save the Children ima u zaštiti djece postavlja ovu organizaciju u snažan položaj za pomicanje agende digitalne zaštite naprijed. Save the Children treba početi tako što će ojačati vlastitu digitalnu zaštitu djece za djecu u pokretu i raseljenu djecu, a onda je proširiti na svu djecu, pod pretpostavkom da izrada politike oko najranjivijih ujedno osigurava izradu najrobusnije politike. Ova vrsta rada ne može se odvijati u vakumu, naročito ako uzmemo u obzir da programiranje i inovacije većinom uključuju partnere iz MNVO sektora, lokalnih organizacija, vlada i privatnog sektora. Stoga je neophodan sarađivački pristup kako bi ovaj važan rad uistinu bio gurnut naprijed.

Pošto trenutno ne postoje smjernice koje se specifično odnose na ukrštanje između zaštite djece i digitalnog programiranja i inovacija, to znači da postoji prilika za Save the Children da preuzme vodstvo u ovom području. Smjernice koje izradi Save the Children, samostalno i u partnerstvu s drugim organizacijama, moraju biti fleksibilne, prilagodljive lokalnim kontekstima i redovno ažurirane kako bi održale korak s tempom digitalnih promjena. Save the Children i druge organizacije trebaju se pobrinuti da lokalne partnerske organizacije dobiju podršku u vidu obuke, resursa i drugih vidova jačanja kapaciteta kako bi osigurale da će digitalna zaštita biti usvojena i uvrštena u rad na učinkovit način.

Sektor mora ojačati svoju digitalnu zaštitu djece i sigurnije programiranje za djecu u pokretu i raseljenu djecu kako bi osigurali da djeca kojoj pružamo usluge imaju koristi od ogromnog potencijala digitalnih tehnologija, a da su istovremeno zaštićena od povreda. Ova studija poziva humanitarni sektor da osigura digitalnu inkluziju za sve; postigne veće povjerenje u agencije; osmisli jasna partnerstva za inovacije; osigura da digitalni programi odražavaju potrebe korisnika; poveća digitalnu pismenost i kapacitete; pruži jasno vlasništvo i upravljanje i izradi praktične i dosljedne procese upravljanja podacima. Inicijalni set pitanja za usmjeravanje procjene rizika u sva četiri ključna područja rizika navedena u ovom izvještaju nalazi se u Prilogu 1.

Preporuke

1

Osigurati digitalnu inkluziju za sve

Sektor mora proširiti svoje napore za unapređenje digitalne inkluzije i pristupa za najranjiviju djecu, uključujući djecu izbjeglice i migrante, jer digitalna inkluzija može donijeti značajne koristi.

Agencije trebaju uložiti u redovna, lokalizirana istraživanja i konsultacije o vrstama uređaja, platformi, kanala komunikacije i medijskih stranica na internetu koje djeca u pokretu i raseljena djeca koriste u različitim kontekstima kako bi osigurale da neće isključivati djecu kada osmišljavaju digitalne programe i komunikacije.

Također se trebaju pobrinuti da djeca bez pametnih telefona i pristupa internetu budu uključena u digitalne usluge ili da im se pruže alternative. Potrebno je utvrditi načine za proširenje skupova podataka i balansiranje analiza kako bi se izbjegli pogrešni zaključci koji su zasnovani na zastupljenosti samo onih koji imaju digitalni pristup. Ovo će zavisiti od konteksta i može podrazumijevati nastavak tradicionalnog prikupljanja podataka kako bi se osiguralo uključivanje najranjivijih kategorija.

2

Uspostaviti povjerenje u sistem

Nedostatak povjerenja predstavlja ključnu prepreku za učešće djece u digitalnom programiranju, pa je stoga za potrebe izgradnje povjerenja ključno osigurati da vlasti, vlade i privatni sektor ne zloupotrebljavaju podatke o djeci.

Moglo bi biti korisno uraditi dodatno istraživanje o mjeri u kojoj nedostatak povjerenja u sistem, agenciju ili sektor odvraća djecu od pružanja podataka. Također bi bilo korisno istražiti dodatne prepreke za razmjenu podataka među djecom jer bi to doprinijelo boljem razumijevanju potencijalnih prepreka za učešće u digitalnim programima i načina da se one otklone.

3

Izraditi jasne okvire za partnerstvo u inovacijama

Izrada okvira za istraživanje, praćenje i evaluaciju omogućit će agencijama da identificiraju i uzmu u obzir kratkoročne i dugoročne koristi, rizike i štetu od eksperimentacije i inovacija.
Agencije moraju uspostaviti strukturiran proces procjene rizika koji proizlazi iz testiranja inovacija, uključujući i jasne pristupe za učešće djece i lokalnih zajednica u izradi programa i procjeni rizika kod svake nove vrste programa. Ovo je naročito relevantno u radu s partnerima na snimanju, obradi i/ili razmjeni ličnih i osjetljivih podataka koji bi mogao djecu u pokretu i raseljenu djecu dovesti u rizik. Neophodno je u svrhu podrške pružiti obuku kako bi osoblje bilo opremljeno odgovarajućim vještinama za efektivno provođenje procjene rizika.

Moraju se uspostaviti mehanizmi za transparentno dijeljene rezultata i saznanja o inovacijama. Skupa s tim timovi za programe trebaju uspostaviti multidisciplinarni odbor za provjeru (sastavljen od internih i eksternih članova) koji će pregledati i odobravati eksperimentalna partnerstva, partnere, programe i procese sa stanovišta etike.

Osim toga, agencije se trebaju pobrinuti da imaju na raspolaganju pravne savjetnike koji će usmjeravati sve neophodne sporazume s inovacijskim i/ili digitalnim partnerima i štititi interese djece i zajednica, kao i interese organizacije Save the Children.

4

Osigurati da digitalni programi odražavaju potrebe i zabrinutosti korisnika

Neophodno je da učešće i povratne informacije od djece i odraslih u lokalnim zajednicama budu odraženi u politikama zaštite, programiranju i zagovaranju. Zajednice je potrebno uključiti u izradu i ocjenu novih digitalnih programa, a njihovo učešće treba poduprijeti uspostavljanjem etičkog odbora i jasnih kanala za prigovore i transparentno dijeljenje rezultata.

5

Unaprijediti digitalnu pismenost i kapacitete u sektoru

Neophodni su dodatna obuka i kapaciteti kako bi osoblje agencije bilo sigurno da može pružiti učinkovitu digitalnu zaštitu na lokalnom nivou.

Osoblje konkretno poziva da se uloži u:

- Orijentaciju o tome kako izraditi Memorandum o razumijevanju s partnerima koji pružaju uređaje, a kako bi se ispunile obaveze zaštite.
- Ažurirane i kontekstualno specifične politike zaštite koje su neophodne zbog pojavljivanja stalno novih tehnologija.
- Regulatorni okvir sa partnerima kojim će se osigurati da imaju neophodne kapacitete i razumijevanje tehnologije.
- Jasne, povjerljive i pristupačne kanale za izražavanje zabrinutosti i prigovora o novim pristupima, a koji će biti dostupni djeci i zajednicama, partnerima, osoblju i drugima.
- Unaprijeđene politike pristanka kojima se određuje kako pomiriti nejednakosti u odnosima moći u procesu dobijanja pristanka, a kako bi se osigurao istinski informiran pristanak.
- Obuku i izradu lokalno prilagođenih resursa na raznim jezicima i u lako probavljivim formatima.
- Obuku fokusiranu na šire koncepte digitalne zaštite, ali i na neke specijalizirane oblasti kao što su rizici kod metapodataka, potencijal za ponovnu identifikaciju kod anonimiziranih podataka i druga aktuelna pitanja vezana za podatke i privatnost podataka.
- Kontinuiranu primjenu politika za zaštitu podataka uz pružanje podrške uredima kako bi te politike prilagodili lokalnom jeziku i kontekstu, lokalnim režimima zaštite podataka i lokalnim i globalnim propisima.
- Specifične smjernice za upravljanje fotografijama snimljenim na ličnim uređajima i za dijeljenje priča i fotografija raseljene djece i djece u pokretu.
- Pregled postojećih politika o društvenim medijima i podrška lokalnim uredima da ih prilagode kako bi bile kontekstualno relevantnije.

Potrebno je utvrditi kontakte fokalnih tačaka kako bi bolju praksu proširili u organizaciji i sektoru i kako bi se pružile specifične smjernice o pitanjima privatnosti i zaštite podataka u nacionalnim kontekstima i načinima postupanja u slučaju oprečnih pravnih režima u različitim zemljama.

6

Pružiti jasne procedure vlasništva i upravljanja

Neophodan je sistematičniji i institucionaliziran pristup procjeni i ublažavanju rizika, uključujući i multidisciplinarni odbor za provjeru i dobro informirane pravne savjetnike koji mogu razmotriti i izmjeriti koristi od inovacija i tehnologija.

U skladu s tim, sektor mora razviti procese i smjernice za unapređenje svijesti o tome da je zaštita podataka "svačija odgovornost". Odgovornost za upravljanje, održavanje i ažuriranje procedura ili sistema ne treba biti povjerena samo jednom zaposleniku. Tako će se izbjeći rizik od gubitka ključnih znanja ili informacija ako taj zaposlenik napusti organizaciju. Agencije moraju sarađivati na izgradnji sektorskih normi i resursa za obuku osoblja i menadžmenta o podacima i djeci, uz poseban naglasak na djecu u pokretu i raseljenu djecu.

Agencije moraju procijeniti i ažurirati upravljanje podacima i lance odgovornosti kako bi razumjele njihovu učinkovitost i predvidjele budžet za stalna unapređenja.

7

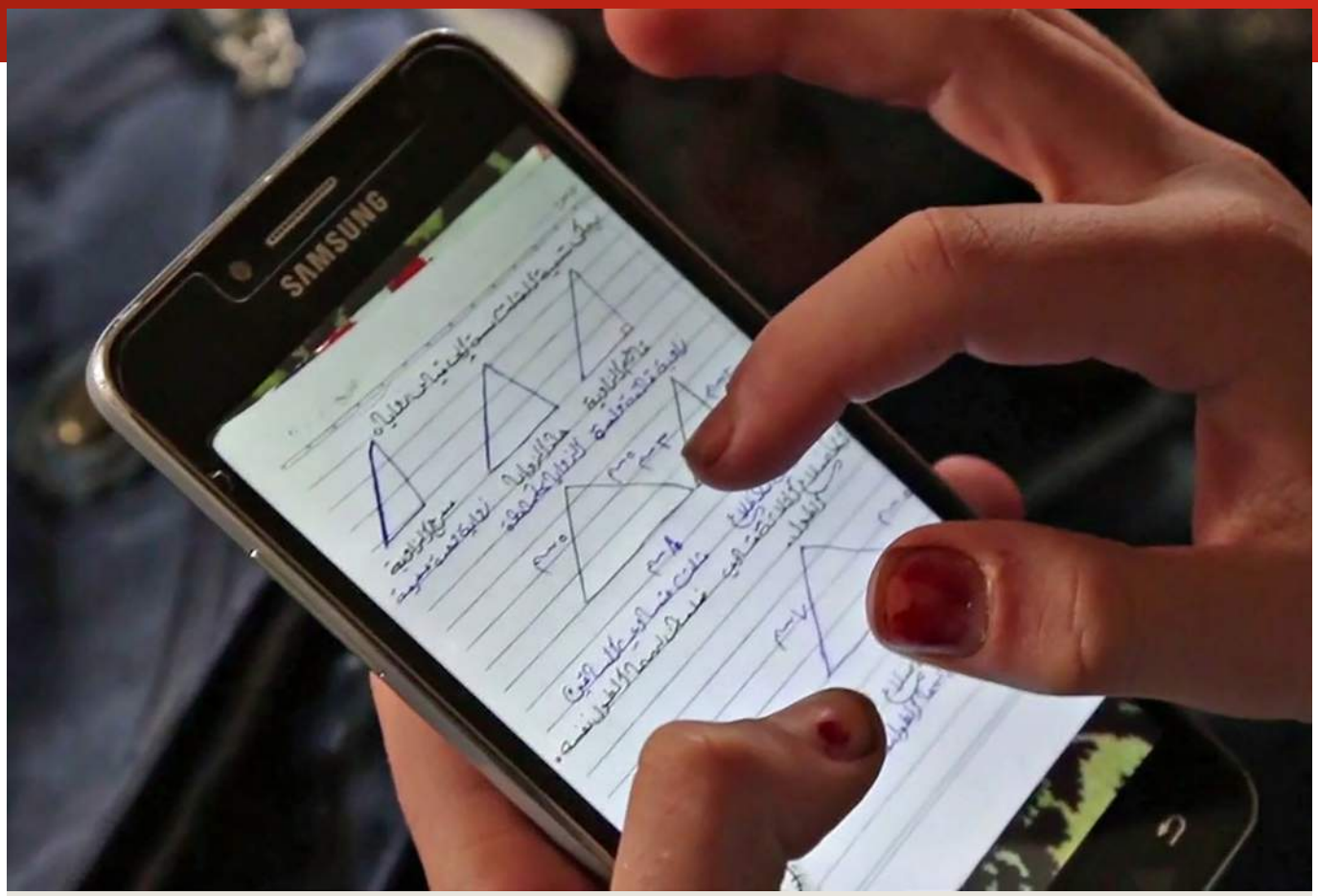
Izraditi praktične i dosljedne sisteme i procese za upravljanje podacima

Sektoru su potrebne praktične smjernice za zaštitu i upravljanje podacima koje će biti kontekstualno i operativno relevantnije. To podrazumijeva da se utvrdi odgovarajući pristup istinskom, aktivnom i informiranom pristanku na snimanje, obradu i razmjenu dječijih ličnih, osjetljivih i/ili grupnih podataka, naročito za vrijeme procesa inovacije ili eksperimentacije.

Agencije također moraju uložiti u bolje usklađivanje sistema za pohranu i sigurnost podataka kako nacionalni uredi ne bi morali upravljati višestrukim sistemima oslanjajući se na resurse i preferencije članskih ureda.

Osoblje je također zatražilo dodatnu podršku i smjernice o razmjeni podataka s partnerima, recikliranju lokalnih brojeva mobilnih telefona u sekundarne svrhe u vanrednim okolnostima, korištenju WhatsApp aplikacije za upravljanje predmetima dječije zaštite u kontekstu kampova, uspostavljanju enkripcije za aplikacije za prikupljanje podataka otvorenog koda (open source), vlasništvu podataka, čuvanju i brisanju podataka.

Kako bi provela ove preporuke, organizacija Save the Children treba oformiti radnu grupu iz svih dijelova organizacije koja će izraditi i resursima podržati mapu puta za cijelu organizaciju. Također su potrebna lokalizirana i stalna istraživanja o tome kako djeca u pokretu i raseljena djeca pristupaju i koriste internetske platforme i usluge, kako bi se održao korak s rizicima i potencijalnim povredama na koje treba obratiti pažnju. Koordinirani i zajednički sektorski pristup ključan je za primjenu ovih preporuka.



Save the Children's partner Syria Relief

Korisne smjernice i alati

- DIAL: Principi digitalnog razvoja[181] (u izradu su dodatne smjernice o inkluziji)
- Girl Effect: Savjeti i smjernice o digitalnoj zaštiti[182] (vidi poglavlje o Bezbjednom istraživanju)
- Response Innovation Lab[183] (Save the Children je partner)
- HIF i Erlha: Vodič za humanitarne inovacije[184] (praktične etičke smjernice su u izradi)
- Nenanošenje povreda: Taksonomija izazova humanitarnih inovacija[185]
- Komesarijat UK za djecu: Ko šta zna o meni[186]
- London School of Economics: Moja privatnost UK[187]
- Girl Effect: Savjeti i smjernice o digitalnoj zaštiti[188]
- End Violence against Children: Resursi na internetu o sigurnosti djece na internetu za vrijeme pandemije bolesti COVID-19[189]
- Plan International: Smjernice za politiku zaštite djece i mladih: Sigurnost na internetskim platformama[190]
- Save the Children: Postojeće smjernice o sigurnosti djece na internetu
- Save the Children: Savjeti o zaštiti i digitalnoj tehnologiji za programe: Digitalne platforme i društveni mediji
- UNICEF: Odgovorni podaci za djecu (RD4C)[191]
- UNICEF: Lica, otisci prstiju i stopala (Smjernice o biometriji)[192]
- UNOCHA: Smjernice za odgovornost prema podacima[193]
- UN: Principi zaštite ličnih podataka[194]
- USAID: Razmatranja za odgovornost prema podacima[195]

PRILOZI

Prilog 1
Inicijalna procjena rizika

Pitanja ispod mogu poslužiti kao alat podrške za inicijalnu procjenu rizika za potrebe istraživanja i identificiranja potencijalnih opasnosti.

I	Dizajn i implementacija koji uzimaju u obzir inkluziju
Pitanje za sagledavanje šireg konteksta: **Koji je rizik od isključivanja djece u pokretu i raseljene djece kada uvodimo inovacije, digitalno programiranje i inicijative s podacima?**	Šta znamo o djeci koju želimo angažirati ili podržati u smislu njihove pismenosti, jezika, kulture, tradicija, migrantskog ili raseljenog statusa, prošlih iskustava ili trauma, etničke pripadnosti, nivoa stresa ili prijetnje, rodnog identiteta i kako se rod izražava u njihovoj kulturi/zemlji porijekla i u drugim zemljama kroz koje prolaze ili u kojima borave? Isključujemo li ovu djecu zbog njihovih općih okolnosti, konteksta ili identiteta?
	Isključujemo li djecu zato što nemaju pristup ili ne koriste digitalne uređaje ili internet? Šta znamo o tome kako djeca u pokretu i raseljena djeca pristupaju internetu i digitalnim uređajima? Posjeduju li uređaje? Kakve vrste uređaja? Ili ih posuđuju ili dijele? Od koga i s kim? Kako često? Da li bilo ko drugi kontrolira ili pregleda kako koriste uređaj? Koje društvene medije i druge stranice ili kanale koriste? Koja su njihova iskustva sa lošim postupanjem ili isključivanjem u prošlosti?
	Izrađujemo li pristupe podacima koji podržavaju predrasude, ugnjetavanje i nepravdu? Kako možemo osigurati da naša analitika podataka ne ponavlja predrasude i ne služi isključivanju načina na koji prikupljamo/pristupamo/koristimo tumačimo i analiziramo podatke, uključujući algoritme koji propuste ljude, predrasude, doprinose ugnjetavanju ili nepravdi ili drugim povredama, ili specifične odluke koja nanose štetu/izostavljaju određenu djecu ili grupe djece?
	Da li se djeca samo-isključuju iz straha ili nedostatka povjerenja? Da li smo razmotrili mogućnost da djeca ne žele biti obuhvaćena/praćena zbog zabrinutosti za privatnost? Ili da možda ne žele učestvovati zbog ranijih iskustava lošeg postupanja, zlostavljanja i drugih povreda? Da li smo razmotrili mogućnost da su njihovi strahovi opravdani i našli alternativne načine da učestvuju ili da budu obuhvaćeni i da se njihov glas čuje?

2	Uvođenje digitalne izrade programa i inovacija
Pitanje za sagledavanje šireg konteksta: **Uvodimo li odgovorno digitalno programiranje i inovacije?**	Da li je ovo stvarni problem za ljude za koje izrađujemo ili dizajniramo programe? Koga smo pitali? Šta su nam rekli?
	Koja je naša motivacija za ovo što radimo? Na koju izraženu potrebu, pravo ili problem odgovaramo? Koja istraživanja/dokaze imamo o prirodi onoga što je neophodno i kako bi moglo biti dizajnirano?
	Da li je ovo ili nešto slično ranije rađeno? Šta smo naučili i primijenili iz prošlih iskustava?
	Da li je 'naš posao' da se bavimo ovim problemom ili su drugi u boljem položaju da to čine? Da li lokalni akteri već rade nešto što bismo mogli podržati? Kako će se lokalni akteri angažirati sada i kasnije?
	Da li je ovo problem koji se može riješiti tehnologijom, informacijama ili komunikacijama, ili većom količinom podataka/drugačijim podacima? Postoje li drugi načini da se riješi ovaj problem? Zašto je tehnološka ili podatkovna inovacija najbolji pristup? Kako će biti integrirana u širi program ili ekosistem? Koji su ljudi, procesi i politička volja neophodni uz tehnologiju?
	Da li koristi za djecu u pokretu i raseljenu djecu i njihove zajednice nadmašuju rizike i potencijal za nanošenje štete? Kako smo to procijenili i ko je bio uključen? Koje neželjene posljedice ili negativni ishodi mogu nastupiti i za koga?
	Postoji li dovoljno obučenosti, tehničke pismenosti i smjernica?
	Šta će se desiti kada se okonča finansiranje ili naš projekat i kada proizvod ili usluga više ne budu dostupni? Šta će biti s podacima koje smo prikupili?
	Ko bi mogao imati zle namjere ili interes za ovu inicijativu ili podatke koje bismo prikupili? Kako možemo smanjiti opasnosti?
	Kako će se upravljati projektom ili podacima i kako ćemo upravljati transparentnošću i odgovornošću prema djeci? Koje zakone i propise moramo poštovati?

3	Upotreba digitalnih komunikacija ili ohrabrivanje djece da učestvuju u digitalnom okruženju
Pitanje za sagledavanje šireg konteksta: **Koje rizike ili potencijalne povrede uvodimo ili pogoršavamo izlaganjem djece u pokretu i raseljene djece digitalnom okruženju?**	Kada djeca samostalno koriste internet i mobilne telefone, izlažemo li ih riziku kroz kontakte, sadržaje ili ponašanja? Izlažemo li ih povredama privatnosti, stigmi ili potencijalnom riziku po ugled? Da li smo našli načine da pomognemo djeci da prebrode te rizike? Znaju li gdje potražiti pomoć ili podršku?
	Kada Save the Children za djecu uvede uređaje ili digitalne kanale, da li smo izradili platforme i učešće na način da smanjimo rizik, recimo tako što ćemo pružiti zdrave zajednice na internetu s dovoljno moderiranja?
	Kada Save the Children koristi digitalne platforme ili kanale društvenih medija u svom programiranju, zagovaranju i komunikacijama, da li smo radili s djecom i njihovim porodicama kako bismo im pomogli da razumiju gdje i kako će se koristiti njihove fotografije i izjave i koji su mogući rizici? Da li ih dovoljno anonimiziramo? Da li smo im osigurali kanale koje mogu koristiti da opozovu svoj pristanak i da li smo ih uputili gdje mogu naći podršku ako pretrpe bilo koji vid štete?
	Kada mi i naši partneri ohrabrujemo djecu da se aktiviraju na internetu, da li smo uspostavili kontrole za zaštitu djece?
	Kada radimo s djecom koja imaju vlastite uređaje i profile na društvenim medijima, nalazimo li načine da im pomognemo da sama sebe zaštite od štetnih sadržaja i kontakata?
	Da li smo svjesni i da li pratimo pravne propise i industrijske standarde vezane za pristup djece platformama na internetu?

4	Snimanje, obrada i/ili razmjena dječijih podataka
Pitanje za sagledavanje šireg konteksta: **Koje rizike ili potencijalne povrede uvodimo ili pogoršavamo snimajući, obrađujući ili razmjenjujući dječije podatke?**	Poštujemo li naše protokole za sigurnost podataka i politike zaštite podataka? Da li smo se posavjetovali s našim kolegama za IT prije uvođenja novih alata, aplikacija, platformi ili podatkovnih inicijativa?
	Da li smo prilagodili neke od politika Save the Children lokalnom kontekstu i da li smo uzeli u obzir lokalne propise o privatnosti podataka?
	Da li smo planirali kako ćemo osigurati i zaštititi podatke tokom cijelog njihovog životnog ciklusa? Koristimo li nove ili aktuelne pristupe podacima koji zahtijevaju detaljniju procjenu kako bismo osigurali da djecu ne izlažemo riziku od povreda?
	Da li smo provjerili da eventualni partneri za podatke imaju kapacitet za zaštitu dječijih podataka?
	Da li smo osigurali zakonske osnove za prikupljanje i obradu podataka, uključujući pristanak i druge procedure? Da li smo osigurali da prikupljamo i obrađujemo samo one podatke koji su nam potrebni?
	Da li smo uzeli u obzir programske implikacije koje proizlaze iz nejednakih odnosa moći, nedostatka transparentnosti i odgovornosti i gubitka povjerenja kada se podaci dijele s vladom ili s privatnim sektorom?
	Da li smo uspostavili upravljanje podacima, transparentnost i odgovornost prema korisnicima?
	Da li smo proveli procjenu rizika u odnosu na koristi prije započinjanja prikupljanja i obrade podataka?

Prilog 2
Relevantne sektorske politike, smjernice i resursi

Organizacija	Tema/e	Dokument	Sažetak dokumenta i poveznica
Response Innovation Lab	Inovacije Digitalna Humanitarna	Set alata za dokumentiranje inovacija	Ovaj set alata nastoji pomoći organizacijama da bolje koriste praćenje, evaluaciju, istraživanje i povratne informacije, da pilotiraju, provode procjene i uče iz tog procesa. https://responseinnovationlab.com/evidencing-innovation/
Digital Impact Alliance	Digitalna	Prinicipi digitalnog razvoja	Principi digitalnog razvoja su živući dokument koji izlaže devet principa od pomoći organizacijama u izradi uticajnih i održivih digitalnim programa i inicijativa. https://digitalprinciples.org/
Save the Children	Sigurnost na internetu	Sigurnost djece na internetu: vodič za organizacije	Ovaj vodič je izrađen za međunarodne NVO koji koriste društvene medije s djecom i mladima, naročito one koji rade u zemljama u razvoju gdje se sve više koriste društveni mediji i sve je veća potreba za zaštitom djece na internetu. https://resourcecentre.savethechildren.net/node/8563/pdf/kcs_online_guidance_2014.pdf
ITU i UNICEF	Sigurnost na internetu	Smjernice za zaštitu djece na internetu	Djeca: https://resourcecentre.savethechildren.net/node/8473/pdf/gl-child-2009-e.pdf Roditelji, staratelji i edukatori: https://resourcecentre.savethechildren.net/node/8472/pdf/ guidelines-educ-e.pdf Industrija: https://resourcecentre.savethechildren.net/node/8470/pdf/bd_broch_industry0809.pdf Donositelji politike: https://resourcecentre.savethechildren. net/node/8471/pdf/guidelines-policy_makers-e.pdf
Save the Children	Sigurnost na internetu	Operativni priručnik za centre za sigurnost djece na internetu	Ovaj priručnik predstavlja primjere dobre prakse centara za sigurnost na internetu i analizira njihov rad. Sadrži informacije, sugestije i smjernice s preporukama za niz ideja koje bi se mogle provesti u Srbiji u svrhu zaštite djece na internetu. https://resourcecentre.savethechildren.net/node/15493/pdf/operational_handbook_for_child_online_safety__centres.pdf
End Violence Against Children	Sigurnost na internetu COVID-19	Resursi na internetu o sigurnosti djece na internetu za vrijeme COVID-19	Kampanja za okončanje nasilja protiv djece sakupila je različite resurse za sigurnost djece na internetu pri prelasku na virtuelne i daljinske usluge zbog pandemije bolesti COVID-19. https://www.end-violence.org/safe-online#covid-19

Organizacija	Tema/e	Dokument	Summary of document & link
Europol	Sigurnost na internetu COVID-19	COVID-19: Seksualno iskorištavanje	Europol je izradio savjete za roditelje i edukatore o tome kako zaštiti djecu na internetu za vrijeme pandemije COVID-19 i spriječiti seksualno iskorištavanje djece. https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation
World Vision	Djeca Digitalna Humanitarna	Partnerska politika o globalnoj zaštiti i privatnosti podataka (2019)	Ova politika nudi krovni okvir za globalnu zaštitu i privatnost podataka kod organizacije World Vision, dokumentira principe zaštite i privatnosti podataka i politike neophodne za osiguranje dosljednosti u zaštiti i privatnosti podataka, poštivanju primjenjivih zakona, primjeni dobre prakse, zaštiti informacija za ličnu identifikaciju (PII) i minimiziranju rizika od nepridržavanja regulatornih propisa i narušavanja ugleda. To je primarna politika pod kojom su sve druge politike vezane za zaštitu i privatnost podataka. Nije dostupna na internetu, ali se opisuje u ovom radu: https://www.wvi.org/sites/default/files/Discussion%20Paper%20-%20Data%20Protection%20Privacy%20%26%20Security%20for%20Humanitarian%20%20%26%20Development%20Programs%20-%20FINAL.pdf
UNICEF i ICRC	Djeca Digitalna Humanitarna	Etička razmatranja kod korištenja geoprostornih tehnologija za prikupljanje dokaza (2018)	Geoprostorne tehnologije transformirale su način na koji vizueliziramo i razumijemo društvene pojave i fizička okruženja. Značajne su prednosti kod korištenja ovih tehnologija i podataka, ali njihova upotreba također postavlja etičke dileme vezane, na primjer, za privatnost i sigurnost, kao i za potencijal stigmatizacije i diskriminacije uslijed povezanosti s određenim lokacijama. Stoga upotrebu geoprostornih tehnologija i posljedičnih podatkovnih potreba treba kritički ocijeniti iz etičke perspektive prije provedbe programa, analiza i partnerstava. Ovaj rad razmatra koristi, rizike i etička razmatranja kod prikupljanja dokaza upotrebom geoprostornih tehnologija. Propraćen je kontrolnom listom za provjeru koja se može koristiti kao praktični alat za podršku razmatranju etičke upotrebe geoprostornih tehnologija. https://www.unicef-irc.org/publications/971-ethical-considerations- when-using-geospatial-technologies-for-evidence- generation.html
UNICEF	Djeca Digitalna Humanitarna	Lica, otisci prstiju i stopala: Smjernice o procjeni vrijednosti uključivanja biometrijskih tehnologija u programima koje podržava UNICEF (2019)	Ovaj dokument daje pregled 10 ključnih pitanja i kriterija koji se preporučuju programima UNICEF-a kada procjenjuju da li uložiti u ili podržati upotrebu biometrijskih tehnologija u sklopu izrade programa. Ova pitanja pružaju kritičku perspektivu koja će pomoći da se odvažu koristi i rizici I osiguraju odgovarajuće upraviteljske strategije za bezbjednu upotrebu biometrije. https://data.unicef.org/resources/biometrics/

Organizacija	Tema/e	Dokument	Sažetak dokumenta i poveznica
PIM (koalicija različitih aktera)	Djeca Digitalna Humanitarna	Protection Information Management (PIM) Paket resursa za obuku (2018)	Protection Information Management (PIM) odnosi se na principijelne, sistematizirane i surađivačke procese za prikupljanje, obradu, analizu, pohranjivanje, razmjenu i upotrebu podataka i informacija kako bi se omogućilo djelovanje informirano dokazima za kvalitetne rezultate zaštite. Ovih pet modula obuke imaju za cilj da pomognu osoblju za zaštitu da nauče odgovorno upravljati podacima. http://pim.guide/uncategorized/pim-training-resource-pack/
Stanford	Djeca Digitalna Trgovina ljudima	Kako do kvalitetnih podataka o trgovini ljudima: svakodnevne smjernice za praktičare na prvim linijama (2018)	Ovaj dokument služi kao katalizator za ocjenu i poboljšanje postojećih napora za prikupljanje podataka – prilagođenih lokalnom kontekstu i uzimajući u obzir regionalni potencijal – za osiguranje kvalitetnih, odgovornih podataka za borbu protiv trgovine ljudima. Ovaj vodič namijenjen je kao referentni dokument koji nudi osnovne standarde i preporuke utemeljene na aktuelnom razumijevanju (u trenutku objavljivanja) kvalitetne i odgovorne podatkovnih prakse. https://handacenter.stanford.edu/publications/getting-good-human-trafficking-data-everyday-guidelines-frontline-practitioners
UNICEF	Djeca Digitalna	Odgovorni podaci za djecu (2019)	RD4C nastoji izgraditi svijest o potrebi da se posebna pažnja posveti pitanjima koja pogađaju djecu, naročito u ovom vremenu napredovanja tehnologije i uvezivanja podataka. Ohrabruje vlade, zajednice i aktere u području razvoja da u središte podatkovnih aktivnosti stave najbolje interese djece i pristup koji uzima u obzir dječija prava. Oslanjajući se na terenska istraživanja i uspostavljenu dobru praksu RD4C nastoji istaći i podržati najbolju praksu podatkovne odgovornosti; identificirati izazove i izraditi praktične alate koji će pomoći praktičarima da ih procijene i riješe; a ohrabruje i širu diskusiju o principima djelovanja, uvidima i pristupima za odgovorno upravljanje podacima. https://rd4c.org/
Girl Effect	Djeca Digitalna	Savjeti i smjernice o digitalnoj zaštiti (2018)	Ovaj dokument osoblju i partnerima nudi smjernice o zaštiti privatnosti, sigurnosti i bezbjednosti adolescentnih djevojčica pri izradi digitalnih alata i platformi, sklapanju partnerstava s drugim i korištenju podataka za praćenje, evaluaciju i učenje. Verzija iz 2018. ažurirana je s podacima o GDPR-u. https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf

Organizacija	Tema/e	Dokument	Sažetak dokumenta i poveznica
Dječiji komesar za Englesku	Djeca Digitalna	Ko šta zna o meni (2018)	Dječiji komesar zabrinut je da informacije prikupljene o nekom djetetu danas mogu ugroziti njegovu budućnost, potencijalno uticati na mogućnost studiranja, zaposlenja i pristupa finansijskim proizvodima kao što su osiguranje i krediti. Ovaj izvještaj dostupan na internetu izlaže specifične načine na koje se u UK prikupljaju dječiji podaci i istražuje moguće posljedice ovih aktivnosti. https://www.childrenscommissionergov.uk/ our-work/digital/who-knows-what-about-me/
London School of Economics	Djeca Digitalna	Moja privatnost UK (2019)	Set alata o podacima i privatnosti namijenjen djeci u UK. Obuhvata podatke, prava, nadzor i praćenje, neželjene posljedice praćenja podataka na internetu, kako zaštititi svoju privatnost i kako dobiti pomoć. http://www.lse.ac.uk/my-privacy-uk
EU	Djeca Digitalna	Opća uredba o zaštiti podataka (2018)	Opća uredba o zaštiti podataka (GDPR) uspostavlja uslove za obradu svih vrsta ličnih podataka. Sadrži specifične politike za zaštitu dječijih prava i nalaže da djeca moraju biti u stanju razumjeti obavijesti o privatnosti i da internetske usluge koje se nude djeci smiju obrađivati podatke samo uz pristanak staratelja, osim ako se ne radi o prevencijskim uslugama ili savjetovanju. Prave pojedinaca prema GDPR-u uključuju: 1 pravo da bude obaviješten; 2 pravo pristupa; 3 pravo na ispravku; 4 pravo na brisanje; 5 pravo na ograničenje obrade; 6 pravo na prenosivost podataka; 7 pravo na prigovor; 8 prava vezana za automatizirano donošenje odluka i profiliranje. https://gdpr.eu/
COPPA	Djeca Digitalna	Zakon o privatnosti i zaštiti djece na internetu (2000)	Primarni cilj COPPA-e je da roditeljima pruži kontrolu nad tim koje se informacije prikupljaju od njihove djece na internetu. Zakon je osmišljen kako bi zaštitio djecu mlađu od 13 godina, uzimajući u obzir dinamičnu prirodu interneta, a primjenjuje se na operatore komercijalnih internetskih stranica i usluga (uključujući mobilne aplikacije) usmjerenih na djecu mlađu od 13 godina koje prikupljaju, koriste ili objavljuju lične informacije od djece. COPPA se također primjenjuje na operatore internetskih stranica i usluga za opću javnost koji imaju stvarna saznanja da prikupljaju, koriste ili objavljuju lične informacije od djece mlađe od 13 godina ili izravno od korisnika neke druge internetske stranice ili usluge usmjerene na djecu. https://www.ftc.gov/tips-advice/business-center/guidance /complying-coppa-frequently-asked- questions#General% 20Questions

Organizacija	Tema/e	Dokument	Sažetak dokumenta i poveznica
UN OCHA Centar za humanitarne podatke	Digitalna Humanitarna	Smjernice za odgovornost prema podacima (2019)	Smjernice za odgovornost prema podacima OCHA-e nude set principa, procese i alate koji podržavaju sigurno, etično i učinkovito upravljanje podacima u humanitarnim intervencijama. Glavna publika za smjernice je osoblje OCHA-e uključeno u upravljanje humanitarnim podacima širom osnovnih funkcija OCHA-e, koordinacije, zagovaranja, donošenja politika, humanitarnog finansiranja i upravljanja informacijama, uz primarni fokus na terenskom radu. https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf
Sistem UN-a	Digitalna Humanitarna	Principi zaštite ličnih podataka (2019)	Ovi principi uspostavljaju osnovni okvir za obradu "ličnih podataka", koji se definiraju kao informacije vezane za identificirano fizičko lice ili fizičko lice koje može biti identificirano ("ispitanik"), od strane ili u ime organizacija iz sistema Ujedinjenih nacija u okviru njihovih mandata. Cilj principa je da: i) usklade standarde za zaštitu ličnih podataka širom organizacija sistema Ujedinjenih nacija; ii) omoguće odgovornu obradu ličnih podataka u svrhe provođenja mandata organizacija sistema Ujedinjenih nacija i iii) osiguraju poštivanje ljudskih prava i osnovnih sloboda pojedinaca, naročito prava na privatnost. https://www.unsystem.org/principles-personal-data-protection-and-privacy
UNDG	Digitalna Humanitarna	Smjernice UNDG-a o velikim podacima (2017)	Uspostavlja opće smjernice o privatnosti podataka, zaštiti podataka i etici podataka vezane za upotrebu velikih podataka koje u stvarnom vremenu prikupljaju tijela privatnog sektora u sklopu svojih poslovnih djelatnosti, a koje dijele s UN-om u svrhe jačanja operativne provedbe programa za podršku postizanja Agende za održivi razvoj do 2030. Smjernice su osmišljene da: uspostave zajedničke principe; posluže kao alat za upravljanje rizikom uzimajući u obzir osnovna ljudska prava i da uspostave principe za dobijanje, čuvanje, korištenje i osiguranje kontrole kvaliteta podataka iz privatnog sektora. https://undg.org/wp-content/uploads/2017/03/UNDG-Big-Data-Guidance-Note.pdf
Svjetski program za hranu	Digitalna Humanitarna	Vodič za zaštitu ličnih podataka i privatnosti (2016)	Sveobuhvatan vodič za zaštitu podataka od WFP-a. https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

Organizacija	Tema/e	Dokument	Sažetak dokumenta i poveznica
Međunarodna organizacija za migracije i Harvard Humanitarian Initiative	Digitalna Humanitarna	Signal Code (2017)	Signal Code nastoji pomoći napredak aktuelnih i budućih napora za stvaranje zajedničkih etičkih obaveza za praktičare. Primarni cilj ovog kodeksa je da pomogne smanjiti i spriječiti opasnost od nanošenja štete ranjivim populacijama negativno pogođenim humanitarnim informacijskim aktivnostima koje bi mogla povrijediti njihova prava. https://signalcode.org/
Oxfam	Digitalna Humanitarna	Odgovorna podatkovna politika (2016)	Politika koja fokusira opredijeljenost Oxfama da poštuje programske podatke i prava onih na koje se podaci odnose. https://oxfamilibrary.openrepository.com/bitstream/handle/10546/575950/ml-oxfam-responsible- program-data-policy-en-270815.pdf;jsessionid=9D9400BB916458CB419CE081D832B2B3?sequence=1
GSMA	Digitalna Humanitarna	Smjernice o zaštiti privatnosti kod korištenja podataka mobilnih telefona u odgovoru na izbijanje Ebole (2014)	Kada je evidencija podataka o pozivima (CDRs) korištena u odgovoru na izbijanje ebole, mobilni operatori željeli su osigurati da privatnost korisnika mobilnih usluga bude poštovana i zaštićena i da se uzmu u obzir svi povezani rizici. Ovaj dokument izlaže, u širokom smislu, standarde privatnosti koje bi mobilni operatori primjenjivali pri korištenju podataka s mobilnih telefona pretplatnika u odgovoru na izbijanje ebole. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/GSMA-Guidelines-on-protecting-privacy-in-the-use-of-mobile-phone- data-for-responding-to-the-Ebola-outbreak-_October-2014.pdf
Sunlight Foundation	Digitalni migranti	Zaštita podataka, zaštita stanovnika (2017)	Deset principa za općinske vlasti o upravljanju podacima. Ovaj dokument je izrađen kako bi pomogao općinama da zaštite migrante i nedokumentirane osobe u SAD-u nakon predsjedničkih izbora 2016. https://sunlightfoundation.com/wp-content/uploads/2017/02/Protecting-data-protecting-residents- whitepaper.pdf
USAID	Digitalna Humanitarna	Razmatranja za odgovornost prema podacima (2019)	Ovaj dokument nastoji pružiti osoblju i lokalnim partnerima USAID-a okvir iza identifikaciju i razumijevanje rizika povezanih s razvojnim podacima. Naglašava bitne zabrinutosti i pruža savjete za djelovanje kako bi pomogao onima koji koriste podatke u razvojnim programima da maksimiziraju njihovu korisnost, a istovremeno upravljaju rizikom. Uključuje i pregled literature i zakona koji razmatra koji zakoni o privatnosti u SAD-u pokrivaju, a koji ne pokrivaju nedržavljane, uključujući i nedokumentirane migrante. https://www.usaid.gov/sites/default/files/documents/15396/USAID-Using DataResponsibly.pdf

Organizacija	Tema/e	Dokument	Sažetak dokumenta i poveznica
ICRC	Digitalna Humanitarna	Zaštita podataka u humanitarnim akcijama (2017)	Ova publikacija oslanja se na prethodne smjernice ICRC-a, a uključuje nove smjernice o upravljanju ličnim podacima u humanitarnim situacijama, uključujući i smjernice o analitici podataka i velikim podacima; upotrebi UAV, dronova i satelitskih snimaka; daljinskim senzorima; biometriji; programiranju gotovinskih transfera; uslugama računarstva u oblaku i aplikacija za mobilno dopisivanje. http://reliefweb.int/sites/reliefweb.int/files/resources/4305_002_Data_protection_and_ humanitarian_action.pdf
ICRC	Digitalna Humanitarna	Biometrijska politika (2019)	Kako nove tehnologije pružaju nove mogućnosti za korištenje biometrije u različitim kontekstima, ICRC je usvojio Biometrijsku politiku da bi to korištenje bilo odgovorno i da bi se riješili izazovi zaštite podataka koji uz njega idu. https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_ adopted_29_august_2019_.pdf
CARE	Digitalna Humanitarna	Odgovoran model zrelosti podataka (2019)	Alat otvorenog koda izrađen za potrebe organizacije CARE kako bi pomogao ukazati osobama u organizacijama ili timovima na načine da unaprijede podatkovnu praksu i etiku. Model se može prilagoditi i koristiti na načine koji su prilagođeni drugim članovima tima kojima odgovornost prema podacima nije osnovni svakodnevni fokus. https://lindaraftree.com/2019/10/17/a-responsible-data-maturity-model-for- non-profits/
Mercy Corps	Digitalna Humanitarna	Smjernice o informacijama kao oružju (2019)	Ova procjena istražuje kako društveni mediji mogu doprinijeti sukobu izvan interneta koristeći se studijama slučaja iz stvarnog svijeta. Rad nudi i okvir za odgovor na takve pojave. https://www.mercycorps.org/sites/default/files/Weaponization_Social_Media_FINAL_ Nov2019.pdf

Prilog 3
Provedene konsultacije

Konsultacije sa Save the Children	
Tim ili regija	**Broj**
Timovi za operacije i programiranje	13
Liban	10
Etiopija	5
El Salvador	7
Afganistan	3
Balkan	9

Konsultacije s vanjskim organizacijama i stručnjacima	
Organizacija i stručne oblasti	**Broj**
UNHCR: zaštita djece, odgovornost	2
The Engine Room: biometrija i digitalni ID	1
OCHA: Centar za humanitarne podatke	1
GovLab: ddgovorni podaci za djecu	1
Yale: humanitarni podaci i etika	1
UNICEF: podaci, zaštita, etika istraživanja	2
ChildFund: nasilje protiv djece na internetu	1
World Vision: inovacije, humanitarni podaci	1
InterAction: podaci, zaštita	2

Bilješke

1
UNHCR, 2020.
'Global Trends Report: Forced Displacement in 2019.' https://www.unhcr.org/5ee200e37.pdf

2
Campo, S., and Raymond, N., 2019.
'Displaced Children and Emerging Technologies: Save the Children's opportunities for investment and impact', Save the Children.
https://resourcecentre.savethechildren.net/node/15382/pdf/stc_tech_innovation_study_v7_digital.pdf

3
UNHCR, 2020.
'Global Trends Report: Forced Displacement in 2019.' https://www.unhcr.org/5ee200e37.pdf

4
Campo and Raymond, op. cit.

5
Ibid.

6
Ibid.

7
Raftree, L., 2020.
'Remote Monitoring in the Time of Coronavirus.' http://merltech.org/remote-monitoring-in-the-time-of-coronavirus/

8
Skup inicijative Chatham House rule o 'Digitalnom dostojanstvu' koji je organizirao IFRC u Wilton Parku, UK, u oktobru 2019. debatirao je i o ovom pitanju.

9
Ibid.

10
Parker, B., 2020.
'Aid policy trends to watch in 2020.'
https://www.thenewhumanitarian.org/feature/2020/1/2/Humanitarian-aid-policy-reform

11
Grand Bargain je mehanizam kojim su se donatori i humanitarne organizacije obavezali da će do 2020. godine 25% globalnog humanitarnog finansiranja dodijeliti lokalnim i nacionalnim interventnim organizacijama, uz dodatna sredstva za koja nije unaprijed definirana namjena i povećano višegodišnje finansiranje za osiguranje veće predvidivosti i kontinuiteta humanitarne pomoći.

12
UNICEF, 2017.
'State of the World's Children: Children in the Digital Age.' https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

13
ITU World Telecommunication / ICT Indicators database, accessed Dec 29, 2019
https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

14
UNICEF, 2017. op. cit.

15
Rowntree, O., 2018.
'The Mobile Gender Gap Report', GSMA: London. https://www.gsma.com/ mobilefordevelopment/wp-content/uploads/2018/04/GSMA_The_Mobile_Gender_Gap_Report_2018_32pp_WEBv7.pdf

16
UNICEF, 2019.
'Faces, Fingerprints and Feet.'
https://data.unicef.org/resources/biometrics/

17
Ibid.

18
Girl Effect and Vodafone, 2019.
'Real Girls, Real Lives, Connected'.
https://static1.squarespace.com/static/5b8d51837c9327d89d936a30/t/5beaa1700e2e72ed39d21c5b/1542103477055/GE_VO_Full_Report_Digital.pdf

19
Ibid.

20
GSMA, 2019.
'Bridging the Mobile Disability Gap in Refugee Settings'. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/09/M4H_DisabilityGap.pdf

21
Girl Effect i 2CV, (2014–2018).
Niz neobjavljenih istraživačkih inicijativa u Indiji, Indoneziji, Bangladešu, Etiopiji, Nigeriji, Južnoafričkoj Republici i na Filipinima.

22
Girl Effect and Vodafone, op. cit.

23
Girl Effect and 2CV, (2014–2018), op. cit.

24
Ključni intervju, UN Agencija, mart 2020.

25
Girl Effect, 2019. Kvalitativna istraživanja u Indoneziji, neobjavljeno.

26
Raftree, L., 2013.
'Modern Mobility: The role of ICTs in child and youth migration.' Plan International and the Oak Foundation. https://resourcecentre.savethechildren.net/sites/default/files/documents/modern_mobility.pdf

27
Campo and Raymond, op. cit.

28
Humanitarian Innovation Fund and Elrha, 2019.
'Humanitarian Innovation Guide.'
https://higuide.elrha.org/enabling-factors/manage-risk/

29
The Lancet and Financial Times Commission, 2020.
'Governing health futures 2030: growing up in a digital world.' Webinar on Enabling Digital Health Futures in Humanitarian Settings: Session 3 (Sustaining the humanitarian principles in a digital era).

30
Krishnaraj, G., Hunt, M., and Schwartz, L., 2019.
'Asking the important questions of ethical humanitarian innovation'. Elrha. https://medium.com/elrha/asking-the-important-questions-of-ethical-humanitarian-innovation-1189b8c169f0

31
Bergtora Sandvik, K., Lindskov Jacobsen, K., and McDonald, S., 2017.
'Do no harm: A taxonomy of the challenges of humanitarian experimentation'.
https://international-review.icrc.org/sites/default/files/irrc_99_17.pdf

32
Bergtora Sandvik, K., 2016.
'Insecurity in the Humanitarian Cyberspace: A Call for Innovation'. https://www.alnap.org/blogs/insecurity-in-the-humanitarian-cyberspace-a-call-for-innovation

33
Raftree, 2013, op. cit.

34
UNICEF, 2017, op. cit.

35
Aynsley, C., 2014.
'Keeping Children Safe Online: A guide for organisations.' https://resourcecentre.savethechildren.net/node/8563/pdf/kcs_online_guidance_2014.pdf

36
Miller, C., 2018.
'Does Social Media Cause Depression?'
https://childmind.org/article/is-social-media-use-causing-depression/

37
Kidron, Baroness, Evans, A., Afia, J., 2019.
'Disrupted Childhood. The Cost of Persuasive Design'. 5Rights. https://5rightsfoundation.com/static/5Rights-Disrupted-Childhood.pdf

38
United Nations Broadband Commission, 2015.
'Combatting Online Violence Against Women & Girls: A Worldwide Wake-Up Call'.
https://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release

39
Blumenfeld, W. and Cooper, R., 2010.
'LGBT and allied youth responses to cyberbullying: Policy implications'.
International Journal of Critical Pedagogy.
http://libjournal.uncg.edu/index.php/ijcp/article/viewFile/72/57

40
Hinduja, S., and Patchin, J., 2010.
'Cyberbullying Research Summary: Cyberbullying and Suicide.'
https://cyberbullying.org/cyberbullying_and_suicide_research_fact_sheet.pdf

41
UNICEF, 2017, op. cit.

42
United Nations Broadband Commission, 2015, op.cit.

43
Blumenfeld and Cooper, 2010, op. cit.

44
Hinduja and Patchin, 2010, op. cit.

45
Bixby, S., 2018.
'LGBT Migrants Fled Persecution Back Home. Then They Fled the Caravan.' https://www.thedailybeast.com/lgbt-migrants-fled-persecution-back-home-then-they-fled-the-caravan

46
Caravita, S., et al., 2019.
'Being Immigrant as a Risk Factor to Being Bullied: An Italian study on individual characteristics and group processes', Child Abuse and Neglect. https://onlinelibrary.wiley.com/doi/10.1111/sjop.12565

47
UNICEF, 2017, op. cit.

48
Human Rights Council, September 17, 2018.
'Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar.' https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf

49
Intervju s osobljem Save the Children na Balkanu, april 2020.

50
Intervju s osobljem Save the Children u El Salvadoru, april 2020.

51
Bueno, O., 2019.
'"No Mother Wants Her Child to Migrate:' Vulnerability of Children on the Move in the Horn of Africa." UNICEF Office of Research (Innocenti). https://www.unicef-irc.org/publications/pdf/Child-Migration-Horn-of-Africa-part-1.pdf

52
Dekker, R., Engbersen, G., Klaver, J., and Vonk, H., 2018.
'Smart Refugees: How Syrian Asylum Migrants Use Social Media Information in Migration Decision-Making'. Sage. https://journals.sagepub.com/doi/10.1177/2056305118764439

53
Toaldo, M., 2015.
'Migrations through and from Libya: a Mediterranean challenge.' Istituto Affari Internazionali.

54
United Nations High Commissioner for Refugees, April 2017.
'From a refugee perspective: Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016.'

55
UNODC, 2018.
'Global Study on Smuggling of Migrants'. https://www.unodc.org/documents/data-and-analysis/glosom/GLOSOM_2018_web_small.pdf

56
Intervju s osobljem Save the Children u Švicarskoj, March 2020.

57
University of Toledo, October 8, 2018.
'Study details link between social media and sex trafficking.' https://phys.org/news/2018-10-link-social-media-sex-trafficking.html

58
Hussain, S., 2019.
'When bills pile up, young people turn to strangers on Venmo.' https://www.latimes.com/business/la-fi-venmo-cash-app-twitter-crowdfund-money-20190602-story.html

59
Privacy International, 2019.
'Experts object to US Immigration & Customs Enforcement's "Extreme Vetting Initiative" that will rely on AI'. https://www.privacyinternational.org/examples/3076/experts-object-us-immigration-customs-enforcements-extreme-vetting-initiative-will.

60
Rivlin-Nadler, M., 2019.
'How ICE Uses Social Media to Surveil and Arrest Immigrants.' The Intercept. https://theintercept.com/2019/12/22/ice-social-media-surveillance/

61
Rafiq, H., and Malak, N., 2018.
'Refuge, Pathways of Youth Fleeing Extremism.' https://www.quilliminternational.com/wp-content/uploads/2017/02/refuge-pathways-of-youth-fleeing-extremism-executive-summary.pdf

62
Guay, J., Gray, S., Rhynard-Geil, M., Inks, L., 2019.
'The Weaponization of Social Media: How social media can spark violence and what can be done about it'. Mercy Corps. https://www.mercycorps.org/sites/default/files/Weaponization_Social_Media_FINAL_Nov2019.pdf

63
Intervju s osobljem Save the Children u El Salvadoru, april 2020.

64
Gelb, A., and Clark, J., 'Identification for Development: The Biometrics Revolution', CGD Working Paper 315, Center for Global Development, Washington, D.C., January 2013.

65
Buolamwini, J., and Gebru, T., 2018.
'Gender Shades: Intersectional accuracy disparities in commercial gender classification', Proceedings of Machine Learning Research, vol. 81, pp. 77–91.

66
UNICEF, 2017. op. cit.

67
Intervju s osobljem Save the Children u El Salvadoru, april 2020.

68
McDonald, S., 2016.
'Ebola: A Big Data Disaster'. https://cis-india.org/papers/ebola-a-big-data-disaster

69
UNICEF Office of Research-Innocenti, 2020.
'Digital Contact Tracing and Suveillance during COVID-19'. https://www.unicef-irc.org/publications/1096-digital-contact-tracing-surveillance-covid-19-response-child-specific-issues-iwp.html

70
Zittrain, J., 2020.
'Is Digital Contact Tracing over Before it Began?' https://medium.com/berkman-klein-center/is-digital-contact-tracing-over-before-it-began-925c72036ee7

71
ICRC, 2019.
'The Humanitarian Metadata Problem: Doing No Harm in the Digital Era'. https://blogs.icrc.org/inspired/2019/06/01/footprints-ether-metadata/?linkId=100000009668523

72
Young, A., (forthcoming).
'Responsible Group Data for Children'. UNICEF.

73
Arbuckle, L., April 27, 2020.
'Aggregated data provides a false sense of security.' https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/

74
Hosein, G., and Nyst, C., 2013.
'Aiding Surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries'. Privacy International. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229

75
Ključni intervju, vanjski izvor, februar 2020.

76
Privacy International, 2019.
'Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers.' https://www.privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers

77
Privacy International, 2019.
'Who supplies the data, analysis, and tech infrastructure to US immigration authorities?' https://www.privacyinternational.org/feature/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities

78
Privacy International, 2011, op. cit.

79
ICRC, 2019.
'Digital Dignity in armed conflict: a roadmap for principled humanitarian action in the age of digital transformation'. Shared at a 'Digital Dignity' convening hosted by the IFRC at Wilton Park, UK in October 2019. The convening was managed under Chatham House Rule, therefore identifying information from this case has not been included here.

80
Ibid.

81
Internews, 2011.
'Lost: Syrian Refugees and the Information Gap'. https://www.internews.org/resource/lost-syrian-refugees-and-information-gap

82
Latonero, M., Poole, D., Berens, J., 2018.
'Refugee Connectivity: A survey of mobile phones, mental health, and privacy at a Syrian refugee camp in Greece.' Harvard Humanitarian Initiative and Data & Society. https://datasociety.net/wp-content/uploads/2018/04/Refugee_Connectivity_Web.MB4_.8-2.pdf

83
Napomena: Ova vrsta informacije izgleda nije dostupna za djecu

84
Casarosa, F., 'Protection of minors online: available regulatory approaches', Journal of Internet Law, vol. 9, March 2011, pp. 25–35.

85
Kaurin, D., 2019.
'Data Protection and Digital Agency for Refugees.' World Refugee Council Research Paper No 12. https://www.cigionline.org/sites/default/files/documents/WRC%20Research%20Paper%20no.12.pdf

86
Hayes, Ben and Massimo Marelli, 2019.
'Facilitating innovation, ensuring protection: the ICRC Biometrics Policy'. ICRC Humanitarian Law & Policy. https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/

87
Montoya-Galvez, C., 2020.
'U.S. collecting DNA samples from some migrants — including teens — in first stage of program'. https://www.cbsnews.com/news/us-collecting-dna-samples-from-migrants-including-children-first-stage-of-program/

88
Privacy International, 2011, op. cit.

89
Boyd, D., and Crawford, K., 2012.
'Critical Questions for Big Data,' Information, Communication and Society, Vol 15 – Issue 5: A decade in Internet time: The dynamics of the Internet and Society. Taylor and Francis Online. https://www.tandfonline.com/doi/abs/10.1080/1369118X.2012.678878

90
UNCTAD, 2020
'Data Protection and Privacy Legislation Worldwide.'
https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

91
The DLA Piper's Global Data Protection Handbook site provides information on data privacy policies around the world, including whether there are specific policies covering children's data and the country's age of consent for data collection.
https://www.dlapiperdataprotection.com/#handbook/world-map-section

92
Ključni intervju, vanjski izvor, februar 2020.

93
European Union, 2017.
'General Data Protection Regulation.'
https://gdpr.eu/

94
US Government's Federal Trade Commission, 2000.
'Children's Online Privacy and Protection Act.'
https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions

95
Privacy International, 2011, op. cit.

96
Green, S., Chandrasekharan, S., Schwegmann, C., Cohen, J., Sullivan, C., Raftree, L., Bari Farahi, A., Getachew, N., 2017.
'Responsible Data Practices: Literature Review.' USAID.

97
UNICEF, 2017. op. cit.

98
Nyst, C., 2017.
'Privacy, protection of personal information and reputation rights,' Children's Rights and Business in a Digital World Discussion Paper Series, United Nations Children's Fund, March 2017.

99
Bajak, Frank, 2018.
'Groups demand end to info-sharing on asylum-seeking children.' AP News.
https://apnews.com/81787a5897704a0cae82a9ceb0eea271

100
See https://resourcecentre.savethechildren.net/

101
Osoblje je u nekim slučajevima davalo neslužbene izjave, a tada ne navodimo iz kojeg su ureda i na kojem radnom mjestu rade.

102
Intervjui s osobljem Save the Children koje radi u području tehnologija i inovacija, mart 2020.

103
Intervjui s osobljem Save the Children koje radi na inovacijama, februar i mart 2020.

104
Intervju s osobljem Save the Children International, februar 2020.

105
Intervju s osobljem Save the Children u članskom uredu, februar 2020.

106
Intervju s programskim osobljem nacionalnog ureda Save the Children, april 2020.

107
Intervju s osobljem Save the Children na Balkanu, april 2020.

108
Intervju s osobljem Save the Children na Balkanu, February 2020.

109
Ivanovic´, 2019, op. cit.

110
Intervju s osobljem Save the Children u Danskoj, Švicarskoj i Sjedinjenim Državama, januar-mart 2020.

111
Intervju s osobljem Save the Children u El Salvadoru, april 2020.

112
Intervju s osobljem za komunikacije ureda Save the Children na Balkanu, april 2020.

113
Intervju s osobljem za komunikacije nacionalnog ureda Save the Children Country, april 2020.

114
Intervju s osobljem Save the Children na Balkanu, april 2020.

115
Intervjui s osobljem Save the Children na Balkanu, u El Salvadoru, Libanu, Etiopiji i osobljem Save International, april 2020.

116
Intervju s osobljem Save the Children u El Salvadoru, april 2020.

117
Intervjui s osobljem Save the Children u Libanu, Etiopiji, El Salvadoru i u sjedištu.

118
European Union, op. cit.

119
Intervju s osobljem Save the Children International, februar 2020.

120
Intervju s osobljem Save the Children International, februar 2020.

121
Intervjui s osobljem Save the Children na Balkanu, april 2020.

122
Intervju s osobljem Save the Children International, februar 2020.

123
Intervju s osobljem Save the Children na Balkanu, 2020.

124
Intervju s osobljem Save the Children u Afganistanu, El Salvadoru, na Balkanu i osobljem Save International, april 2020.

125
Intervju s osobljem Save the Children u El Salvadoru, april 2020.

126
Intervju s osobljem Save the Children na Balkanu, april 2020.

127
Intervjui s osobljem Save the Children na Balkanu, april 2020.

128
Campo and Raymond, op. cit.

129
Raftree, 2018, op. cit.

130
Raftree, 2018, op.cit.

131
Raftree, 2018, op. cit.

132
Raftree, 2018, op.cit.

133
Young, Andrew; Stuart Campo; Stefaan G. Verhulst. 2019. "Responsible Data for Children: Synthesis Report." https://rd4c.org/images/rd4c-report-final.pdf

134
Ključni intervju, vanjski izvor, februar 2020.

135
Ključni intervju, vanjski izvor, februar 2020.

136
Response Innovation Lab, Humanitarian Innovation Fund, START Network, Global Alliance for Humanitarian Innovation, Accountability and Learning Project and UKAID, 2018. "Evidencing Innovation Toolkit."

137
Napomena: Save the Children je učestvovao u testiranju ovih alata za inovacije.

138
'Principles for Digital Development', living document. https://digitalprinciples.org/

139
Raftree, Linda, 2018. "Digital Safeguarding Tips and Guidance" Girl Effect https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf

140
Bergtora Sandvik, Jacobsen and McDonald, op. cit.

141
Bueti, Cristina, Maria Jose Cantarino de Frias, John Carr, Carstensen, D., 2009. 'Guidelines for Children on Child Online Protection'. https://resourcecentre.savethechildren.net/node/8473/pdf/gl-child-2009-e.pdf

142
International Telecommunication Union and UNICEF, 2014. 'Guidelines for Industry on Child Online Protection'. https://resourcecentre.savethechildren.net/node/8470/pdf/bd_broch_industry0809.pdf

143
International Telecommunication Union and UNICEF, 2014. 'Guidelines for Policy Makers on Child Online Protection'. https://resourcecentre.savethechildren.net/node/8471/pdf/guidelines-policy_makers-e.pdf

144
International Telecommunication Union and UNICEF, 2014. 'Guidelines for Parents, Guardians and Educators on Child Online Protection.' https://resourcecentre.savethechildren.net/node/8472/pdf/guidelines-educ-e.pdf

145
Aynsley, op. cit.

146
Ivanović, 2019, op. cit.

147
End Violence against Children, April 2020. 'Stay Safe at Home. Stay Safe Online.' https://www.end-violence.org/safeonlinecovid

148
Europol, April 2020. 'COVID-19: Child Sexual Exploitation.' https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation

149
Raftree, 2018, op. cit.

150
Lutz, A., Doornbos, A., Kehl, A., Ghee, A., and DePauw, L., 2017. 'Protection, Privacy and Security for Humanitarian & Development Programs.' Edited Sherrie Simms. https://www.wvi.org/sites/default/files/Discussion%20Paper%20-%20Data%20Protection%20Privacy%20%26%20Security%20for%20Humanitarian%20%20%26%20Development%20Programs%20-%20FINAL.pdf

151
UNICEF and ICRC, 2018, "Ethical considerations when using geospatial technologies for evidence generation" https://www.unicef-irc.org/publications/971-ethical-considerations-when-using-geospatial-technologies-for-evidence-generation.html

152
UNICEF, 2019, op. cit.

153
Protection Information Management Coalition, 2018. 'Protection Information Management (PIM) Training Resource Pack'. http://pim.guide/uncategorized/pim-training-resource-pack/

154
Brunner, J., 2018. 'Getting to Good Human Trafficking Data: Everyday Guidelines for Frontline Practitioners.' Stanford. https://humanrights.stanford.edu/publications/getting-good-human-trafficking-data-everyday-guidelines-frontline-practitioners

155
Young, Campo, and Verhulst, op. cit.

156
Raftree, 2018, op. cit.

157
Children's Commissioner for England, 2018. 'Who Knows What About Me?' https://www.childrenscommissioner.gov.uk/our-work/digital/who-knows-what-about-me/

158
London School of Economics, 2019. 'My Privacy UK'. http://www.lse.ac.uk/my-privacy-uk

159
UN OCHA, 2019. 'Data Responsibility Guidelines.' https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf

160
United Nations, 2019. 'Principles on Personal Data Protection'. https://www.unsystem.org/principles-personal-data-protection-and-privacy

161
UNDG, 2017. 'Big Data Guidance Note.' https://undg.org/wp-content/uploads/2017/03/UNDG-Big-Data-Guidance-Note.pdf

162
World Food Programme, 2016. 'Guide to Personal Data Protection and Privacy.' https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

163
Raftree, L., 2019. 'Responsible Data Maturity Model.' CARE https://lindaraftree.com/2019/10/17/a-responsible-data-maturity-model-for-non-profits/

164
Harvard Humanitarian Initiative and Signal Program on Human Security and Technology, 2016. 'The Signal Code.' https://signalcode.org/code-intro/

165
Oxfam, 2016.
'Responsible Data Policy.'
https://oxfamilibrary.openrepository.com/bitstream/handle/10546/575950/ml-oxfam-responsible-program-data-policy-en-270815.pdf;jsessionid=9D9400BB916458CB419CE081D832B2B3?sequence=1

166
GSMA, 2014.
'Guidelines on the protection of privacy in the use of mobile phone data for responding to the Ebola outbreak.' https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/GSMA-Guidelines-on-protecting-privacy-in-the-use-of-mobile-phone-data-for-responding-to-the-Ebola-outbreak-_October-2014.pdf

167
Sunlight Foundation, 2017.
'Protecting Data, Protecting Residents.'
https://sunlightfoundation.com/wp-content/uploads/2017/02/Protecting-data-protecting-residents-whitepaper.pdf

168
Green et al. op. cit.

169
ICRC, 2017.
'Handbook on Data Protection in Humanitarian Action.' http://reliefweb.int/sites/reliefweb.int/files/resources/4305_002_Data_protection_and_humanitarian_action.pdf

170
ICRC, 2019.
'Biometrics Policy.' https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf

171
Guay, Gray, Rhynard-Geil and Inks, op. cit.

172
'Harvard Humanitarian Initiative and Signal Program on Human Security and Technology', 2016, op. cit.

173
Young, Campo, and Verhulst, op. cit.

174
Ključni intervju, vanjski izvor, februar 2020.

175
Ključni intervju, vanjski izvor, februar 2020.

176
Ključni intervju, vanjski izvor, februar 2020.

177
Ključni intervju, vanjski izvor, februar 2020.

178
Ključni intervju, vanjski izvor, februar 2020.

179
UNICEF, Office of Global Insight and Policy, 2020.
'Good Governance of Children's Data'.
https://www.unicef.org/globalinsight/data-governance-children

180
Ključni intervju, vanjski izvor, februar 2020.

181
Digital Impact Alliance.
https://digitalprinciples.org/

182
Raftree, 2018, op. cit.

183
Response Innovation Lab.
https://responseinnovationlab.com/evidencing-innovation/

184
Humanitarian Innovation Fund and Elrha, 2019, op. cit.

185
Bergtora Sandvik, Jacobsen and McDonald, op. cit.

186
Children's Commissioner for England, op. cit.

187
London School of Economics, op. cit.

188
Raftree, 2018, op. cit.

189
End Violence against Children, op. cit.

190
Plan International, 2020.
'Global Safeguarding Unit: Guidance on Safeguarding Children and Young People on Online Platforms.' https://plan-international.org/girls-get-equal/how-to-stay-safe-online

191
Young, Campo, and Verhulst, op. cit.

192
UNICEF, 2019, op. cit.

193
UN OCHA, 2019, op. cit.

194
United Nations, op. cit.

195
USAID, op. cit.

Kristiana Marton / Save the Children

Save the Children

Save the Children

Izdavač

Save the Children International
St Vincent's House
30 Orange Street
London
WC2H 7HH
United Kingdom

+44 (0)20 3272 0300
www.savethechildren.net

Prvi put objavljeno 2020.

© Save the Children 2020

Ova publikacija podliježe autorskim pravima, ali može biti reproducirana bilo kojom metodom bez naknade u svrhu edukacije, ali ne u svrhu preprodaje. Za umnožavanje u svim drugim okolnostima potrebno je prethodno pribaviti pismenu dozvolu od izdavača i moguće je da će biti potrebno platiti naknadu.