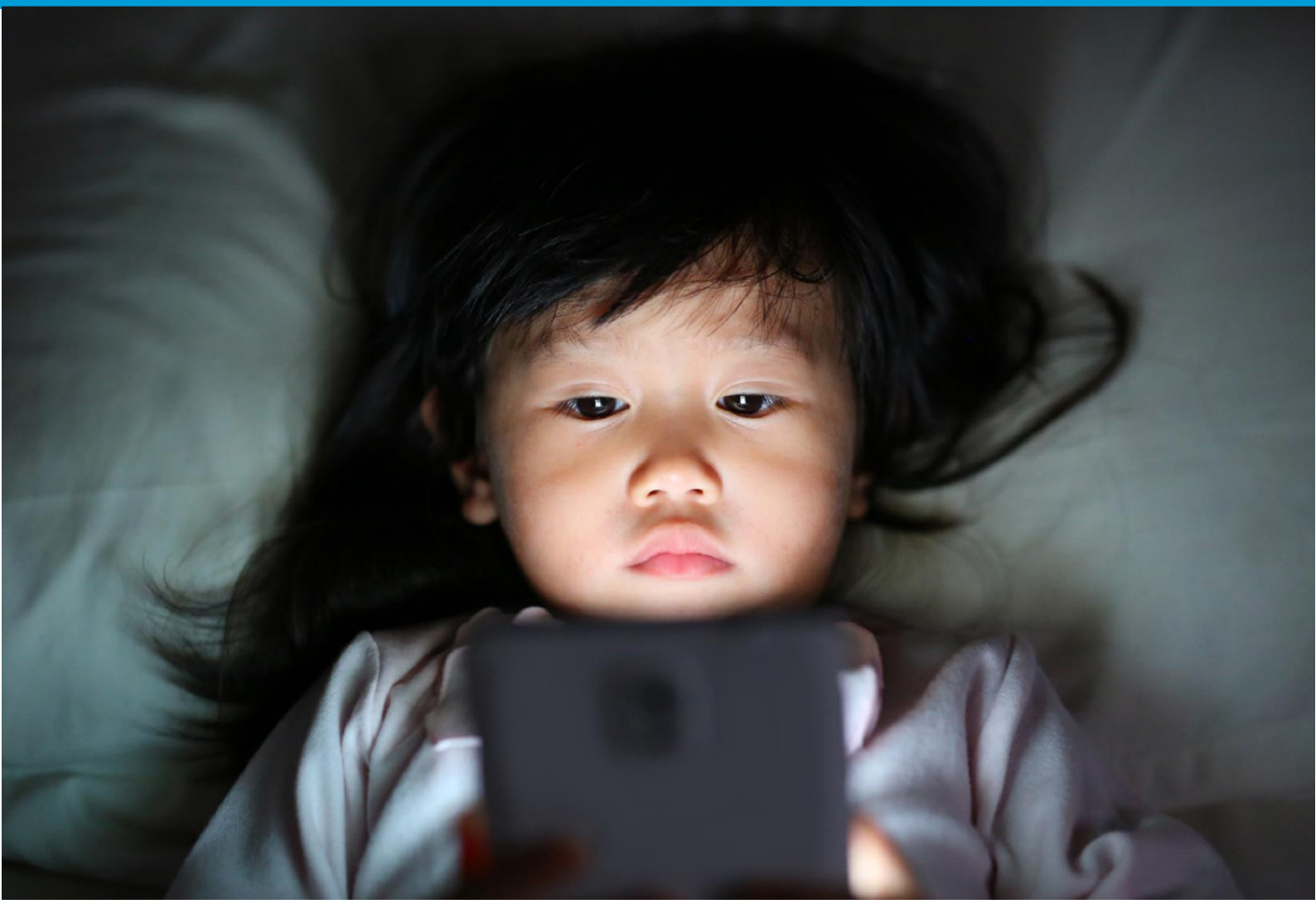
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Udhëzime për Mbrojtjen Online të Fëmijëve

2020



Udhëzime për Mbrojtjen Online të Fëmijëve

2020

Mirënjohje

Këto udhëzime janë zhvilluar nga Unioni Ndërkombëtar i Telekomunikacionit (ITU) dhe një grup pune autorësh kontribues nga institucionet kryesore aktive në sektorin e teknologjisë së informacionit dhe komunikimit (TIK) si dhe në çështjet e mbrojtjes së fëmijëve (në internet) dhe përfshijnë organizatat e mëposhtme :

ECPAT International, rrjeti Global Kids Online në Internet, Partneriteti Global për t'i dhënë fund dhunës ndaj fëmijëve, projekti HABLATAM, rrjeti i pasigurt i qendrave më të sigurta të internetit (Insafe), INTERPOL, Qendra Ndërkombëtare për Fëmijët e Zhdukur dhe të Shfrytëzuar (ICMEC), Aleanca Ndërkombëtare e Aftësisë së Kufizuar, Unioni Ndërkombëtar i Telekomunikacionit (ITU), Fondacioni i Shikimit të Internetit (IWF), Shkolla Ekonomike e Londrës, Zyra e Përfaqësuesit Special të Sekretarit të Përgjithshëm mbi Dhunën ndaj Fëmijëve dhe Raportuesi Special për shitjen dhe shfrytëzimin seksual të fëmijëve, Privatisht SA, RNW Media, Qendrat e Internetit më të Sigurt në MB, Aleanca Globale e WePROTECT (WPGA) dhe Fondacioni Botëror i Fëmijërisë USA.

Grupi i punës u drejtua nga David Wright (UK Safer Internet Centers / SWGfL) dhe i koordinuar nga Fanny Rotino (ITU).

Këto udhëzime nuk do të ishin të mundshme pa kohën, entuziazmin dhe përkushtimin e autorëve kontribues. Kontribute të paçmueshme u morën gjithashtu nga COFACE-Familjet Evropë, Këshilli i Evropës, Komisioneri Australian eSafety, Komisioni Evropian, Grupi e-Worldwide (e-WWG), OECD, Rinia dhe Media në Qendrën Berkman Klein për Internet dhe Shoqëria në Universitetin e Harvardit si dhe qeveritë individuale dhe palët e interesuara të industrisë që ndajnë një objektiv të përbashkët për ta bërë internetin një vend më të mirë dhe më të sigurt për fëmijët dhe të rinjtë.

ITU është mirënjohëse për partnerët e mëposhtëm, të cilët kanë kontribuar për kohën dhe vështrimet e tyre të vlefshme: (të renditura sipas rendit alfabetik të organizatës):

- Martin Schmalzried (COFACE-Families Europë)
- Livia Stoica (Këshilli i Europës)
- John Carr (ECPAT Internacionale)
- Julia Fossi and Ella Serry (eSafety Komisioner)
- Manuela Marta (Komisioni Europian)
- Salma Abbasi (e-WWG)
- Amy Crocker and Serena Tommasino (Partneritet për t'i dhënë fund dhunës ndaj fëmijëve)
- Lionel Brossi (HABLATAM)
- Sandra Marchenko (ICMEC)
- Karl Hopwood (Siguri)[1]
- Lucy Richardson (Aleanca Ndërkombëtare e Aftësisë së Kufizuar)
- Matthew Dompier (Interpol)
- Fanny Rotino (ITU)
- Tess Leyland (IWF)
- Sonia Livingstone (Shkolla ekonomike e Londës & Global Kids Online)
- Elettra Ronchi (OECD)

[1] *Under the Connecting Europe Facility (CEF), European Schoolnet runs, on behalf of the European Commission, the Better Internet for Kids platform, which includes the coordination of the Insafe network of European Safer Internet Centres. More information is available at* www .betterinternetforkids .eu

- Manus De Barra (Zyra e Përfaqësuesit Special të Sekretarit të Përgjithshëm për Dhunën ndaj Fëmijëve)
- Deepak Tewari (SA private)
- Pavithra Ram (RNW Media)
- Maud De Boer-Buquicchio (United Raportuesi Special i Kombeve për shitjen dhe abuzimit seksual të fëmijëve)
- David Wright (UK Safer Internet Centres/SWGfL)
- Iain Drennan and Susannah Richmond (WePROTECT Aleanca Globale)
- Lina Fernandez and Dr. Joanna Rubinstein (Fondacioni i Fëmijëve në USA)
- Sandra Cortesi (Rinia dhe Media)

ISBN

978-92-61-30121-7 (Paper version)

978-92-61-30451-5 (Electronic version)

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

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

Please consider the environment before printing this report.

Parathënie

Në një botë ku Interneti përshkon pothuajse çdo aspekt të jetës moderne, mbajtja e përdoruesve të rinj të sigurt në internet është shfaqur si një çështje gjithnjë e më urgjente për çdo vend.

ITU zhvilloi grupin e saj të parë të Udhëzimeve për Mbrojtjen Online të Fëmijëve që nga viti 2009. Që nga ato ditë të hershme, Interneti ka evoluar përtej njohjes. Ndërsa është bërë një burim pafundësisht më i pasur për fëmijët për të luajtur dhe për të mësuar, ai është bërë gjithashtu një vend shumë më i rrezikshëm për ata që të ndërmarrin pa shoqërim.

Nga çështjet e privatësisë tek përmbajtja e dhunshme dhe e papërshtatshme, tek mashtruesit në Internet dhe spektri i pastrimit në internet, abuzimit seksual dhe shfrytëzimit, fëmijët e sotëm përballen me shumë rreziqe. Kërcënimet po shumohen, dhe autorët e krimit veprojnë gjithnjë e më shumë në të njëjtën kohë në shumë juridiksione të ndryshme ligjore, duke kufizuar efektivitetin e përgjigjeve dhe dëmshpërblimeve specifike të vendit.

Për më tepër, pandemia globale COVID-19 pa një rritje të numrit të fëmijëve që u bashkuan botës për herë të parë, për të mbështetur studimet e tyre dhe për të ruajtur ndërveprimin shoqëror. Kufizimet e vendosura nga virusi jo vetëm që nënkuptonin që shumë fëmijë më të vegjël filluan të ndërvepronin në internet shumë më herët sesa prindërit e tyre mund të kishin planifikuar, por nevoja për të mashtruar me angazhimet e punës bëri që shumë prindër të mos ishin në gjendje të mbikëqyrnin fëmijët e tyre, duke i lënë të rinjtë të rrezikonin të kishin një përmbajtje të papërshtatshme. ose duke qenë në shënjestër të kriminelëve në prodhimin e materialit për abuzim seksual të fëmijëve.

Më shumë se në çdo kohë më parë, mbajtja e fëmijëve të sigurt në internet kërkon një përgjigje bashkëpunuese dhe të koordinuar ndërkombëtare, duke kërkuar përfshirjen aktive dhe mbështetjen e një numri të gjerë të palëve të interesuara - nga aktorët e industrisë duke përfshirë platformat e sektorit privat, ofruesit e shërbimeve dhe operatorët e rrjetit, te qeveritë dhe civilët shoqërisë.

Duke e njohur këtë, në vitin 2018 Shtetet Anëtare të ITU kërkuan diçka më shumë sesa rifreskimi në kohë i Udhëzimeve të COP që është ndërmarrë në mënyrë periodike në të kaluarën. Në vend të kësaj, këto udhëzime të reja të rishikuara janë rimenduar, ri-shkruar dhe ri-dizajnuar nga themeli për të pasqyruar zhvendosjet shumë të rëndësishme në peizazhin dixhital në të cilin gjenden fëmijët.

Përveç përgjigjes ndaj zhvillimeve të reja në teknologjitë dhe platformat dixhitale, ky botim i ri adreson një lakunë të rëndësishme: situatën me të cilën përballen fëmijët me aftësi të kufizuara, për të cilët bota në internet ofron një linjë jetësore veçanërisht të rëndësishme për pjesëmarrjen e plotë - dhe përmbushëse - të shoqërisë. Konsiderimi i nevojave të veçanta të fëmijëve migrantë dhe grupeve të tjera të ndjeshme është përfshirë gjithashtu.

Për politikëbërësit, ne shpresojmë që këto udhëzime të shërbejnë si një themel i fortë mbi të cilin do të zhvillojnë strategji gjithëpërfshirëse, me shumë aktorë kombëtarë, duke përfshirë konsultime dhe dialogje të hapura me fëmijët, për të zhvilluar masa më të synuara dhe veprime më efikase.

Në zhvillimin e këtyre udhëzimeve të reja, ITU dhe partnerët e saj u përpoqën të krijonin një kornizë mjaft të përdorshme, fleksibile dhe të adaptueshme bazuar në standardet ndërkombëtare dhe qëllimet e përbashkëta - veçanërisht Konventën për të Drejtat e Fëmijëve dhe Synimet e KB të Zhvillimit të Qëndrueshëm. Në frymën e vërtetë të rolit të ITU si thirrës global, unë jam krenar për faktin se këto udhëzime të rishikuara janë produkt i një përpjekjeje bashkëpunuese globale dhe janë bashkëautorë të ekspertëve ndërkombëtarë të tërhequr nga një komunitet i gjerë me shumë aktorë. Jam gjithashtu i kënaqur të prezantoj maskotën tonë të re COP, Sango, një karakter miqësor, i paturpshëm dhe i patrembur i projektuar tërësisht nga një grup fëmijësh, si pjesë e programit të ri ndërkombëtar të ITU për të rinjtë.

Doreen Bogdan-Martin

Në një epokë ku gjithnjë e më shumë të rinj po vijnë në internet, këto Udhëzime COP janë më jetike se kurrë. Bërësit e politikave, industria, prindërit dhe edukatorët - dhe vetë fëmijët - të gjithë kanë një rol jetësor për të luajtur. Unë jam mirënjohës, si gjithmonë, për mbështetjen tuaj, dhe unë pres që të vazhdojmë bashkëpunimin tonë të ngushtë për këtë çështje kritike.

Director, Telecommunication Development Bureau

Hyrje

Tridhjetë vjet më parë, gati të gjitha qeveritë u zotuan të respektojnë, mbrojnë dhe promovojnë të drejtat e fëmijëve. Konventa e KB për të Drejtat e Fëmijëve (CRC) është traktati ndërkombëtar për të drejtat e njeriut më i ratifikuar në histori. Ndërsa progres i dukshëm është arritur në tre dekadat e fundit, sfidat e rëndësishme mbeten dhe fushat e reja të rreziqeve për fëmijët janë shfaqur.

Në vitin 2015, të gjitha kombet rinovuan angazhimin e tyre ndaj fëmijëve në agjendën 2030 dhe 17 Qëllimet Universale të Zhvillimit të Qëndrueshëm (SDG). Qëllimi 16.2 për shembull kërkon që t'i jepet fund abuzimit, shfrytëzimit dhe të gjitha formave të dhunës dhe torturës ndaj fëmijëve deri në vitin 2030. Por mbrojtja e fëmijëve është një fije e zakonshme brenda 11 prej 17 SDG-ve. UNICEF i vendos fëmijët në qendër të agjendës 2030 siç përshkruhet në Figurën 1.

Figura 1: Fëmijët, ICTs, and SDGs

Agjenda 2030 për Zhvillim të Qëndrueshëm njeh që TIK-et mund të jenë një mundësues kryesor për arritjen e SDG-ve. Përhapja e teknologjisë së informacionit dhe komunikimit (TIK) dhe ndërlidhja globale ka potencialin për të përshpejtuar përparimin njerëzor, për të kapërcyer ndarjen dixhitale dhe për të zhvilluar shoqëritë e dijes. Më tej përcakton synime specifike për përdorimin e TIK për zhvillimin e qëndrueshëm në arsim (Qëllimi 4), barazia gjinore (Qëllimi 5), infrastruktura (Qëllimi 9 - qasje universale dhe e përballueshme në internet) dhe Qëllimi 17 - partneritete dhe mjetet e zbatimit. TIK-u ka fuqinë të transformojë thellësisht ekonominë në tërësi duke qenë një forcë shtytëse në arritjen e secilës prej 17 SDG-ve. TIK kanë bërë tashmë lëvizjen e tyre duke fuqizuar miliarda individë në të gjithë botën - duke siguruar qasje në burimet arsimore dhe kujdesin shëndetësor dhe shërbime të tilla si qeveria elektronike dhe mediat sociale, ndër të tjera.

Shpërthimi i teknologjisë së informacionit dhe komunikimit ka krijuar mundësi të papara për fëmijët dhe të rinjtë për të komunikuar, lidhur, shkëmbyer, mësuar, aksesuar informacion dhe për të shprehur mendimet e tyre për çështje që ndikojnë në jetën e tyre dhe komunitetet e tyre.

Por qasja më e gjerë dhe më e disponueshme në internet dhe teknologji mobile gjithashtu paraqet sfida të rëndësishme për sigurinë dhe mirëqenien e fëmijëve - si në internet dhe jashtë linje.

Për të zvogëluar rreziqet e botës dixhitale, ndërsa u mundëson më shumë fëmijëve dhe të rinjve të marrin përfitimet e saj, qeveritë, shoqëria civile, komunitetet lokale, organizatat ndërkombëtare dhe industria duhet të bashkohen në qëllimin e përbashkët. Në veçanti janë të nevojshëm politikëbërësit për të arritur një qëllim ndërkombëtar për t'i mbajtur fëmijët të sigurt në internet.

Për t'iu përgjigjur sfidave të paraqitura nga zhvillimi i shpejtë i TIK dhe sfidave të mbrojtjes së fëmijëve që ato sjellin, Iniciativa për Mbrojtjen Online të Fëmijëve (COP) u nis si një iniciativë ndërkombëtare me shumë palë nga Unioni Ndërkombëtar i Telekomunikacionit (ITU) në nëntor 2008 Kjo iniciativë synon të sjellë së bashku partnerë nga të gjithë sektorët e komunitetit global për të krijuar një përvojë të sigurt dhe fuqizuese në internet për fëmijët në të gjithë botën.

Për më tepër, Konferenca e Plotfuqishme e Bashkimit Ndërkombëtar të Telekomunikacionit mbajtur në Dubai në 2018, riafirmoi rëndësinë e Iniciativës COP duke e pranuar atë si një platformë për të rritur ndërgjegjësimin, për të ndarë praktikat më të mira dhe për të siguruar ndihmë dhe mbështetje për Shtetet Anëtare, veçanërisht vendet në zhvillim , në zhvillimin dhe zbatimin e hartave të COP. Ai gjithashtu njohu rëndësinë e mbrojtjes së fëmijëve në internet brenda kornizës së Konventës së Kombeve të Bashkuara për të Drejtat e Fëmijëve dhe traktateve të tjera të të drejtave të njeriut duke inkurajuar bashkëpunimin midis të gjithë aktorëve të përfshirë në mbrojtjen në internet të fëmijëve.

Konferenca njohu Axhendën 2030 për Zhvillim të Qëndrueshëm, duke adresuar aspekte të ndryshme të mbrojtjes në internet të fëmijëve në Qëllimet e Zhvillimit të Qëndrueshëm (SDG), në veçanti SDG 1, 3, 4, 5, 9, 10 dhe 16; më tej njohu Rezolutën 175 (Rev. Dubai, 2018), mbi mundësinë e aksesit për personat me aftësi të kufizuara dhe personat me nevoja specifike për telekomunikacionin / teknologjinë e informacionit dhe komunikimit (TIK) dhe Rezolutën 67 (Rev. Buenos Aires, 2017) të Zhvillimit Botëror të Telekomunikacionit Konferencë (WTDC), mbi rolin e Sektorit të Zhvillimit të Telekomunikacionit ITU (ITU-D) në mbrojtjen në internet të fëmijëve.

Në fund të vitit 2019, Komisioni Broadband i ITU / UNESCO për Zhvillim të Qëndrueshëm nisi Raportin e Sigurisë Online të Fëmijëve me rekomandime vepruese se si ta bëni Internetin më të sigurt për fëmijët.

Në vitin 2009, grupi i parë i udhëzimeve për mbrojtjen në internet të fëmijëve u lëshuan nga ITU në kontekstin e Iniciativës COP. Gjatë dekadës së fundit, Udhëzimet e COP janë përkthyer në shumë gjuhë dhe janë përdorur nga shumë vende të botës si pikë referimi për hartat rrugore dhe strategjitë kombëtare në lidhje me mbrojtjen në internet të fëmijëve. Ata u kanë shërbyer njësive të qeverisë kombëtare, organizatave të shoqërisë civile, institucioneve të kujdesit për fëmijët, industrisë dhe shumë aktorëve të tjerë në përpjekjet e tyre për mbrojtjen në internet të fëmijëve.

Më konkretisht, udhëzimet janë përdorur për hartimin, zhvillimin dhe zbatimin e strategjive kombëtare të mbrojtjes së fëmijëve në internet në shumë shtete anëtare si Kameruni, Gabon, Gambia, Gana Kenia, Sierra Leona, Uganda dhe Zambia në rajonin e Afrikës; Bahreini dhe Omani në rajonin arab; Brunei, Kamboxhia Kiribati, Indonezia, Malajzia, Birmania dhe Vanuatu në rajonin e Paqësorit të Azisë; dhe Bosnja, Gjeorgjia, Moldavia, Mali i Zi, Polonia dhe Ukraina në rajonin e Evropës.

Për më tepër, udhëzimet kanë ndërtuar themelin për ngjarjet rajonale të tilla si Konferenca Rajonale për Mbrojtjen Online të Fëmijëve (ACOP): Fuqizimi i Qytetarëve të Ardhshëm Dixhital, në Kampala, Uganda (2014) dhe Konferenca Rajonale ASEAN për Mbrojtjen Online të Fëmijëve të mbajtur në Bangkok , Tajlandë (2020)

Sipas Rezolutës 179 (Rev. Dubai, 2018), ITU në bashkëpunim me partnerët e iniciativës COP dhe palët e interesuara janë udhëzuar të azhurnojnë katër grupe udhëzimesh duke marrë parasysh zhvillimet e teknologjisë në industrinë e telekomunikacionit, duke përfshirë udhëzimet për fëmijët me aftësi të kufizuara dhe fëmijët me nevojat specifike.

Si rezultat i këtij procesi, këto udhëzime janë azhurnuar dhe rishikuar në mënyrë të konsiderueshme nga ekspertët dhe palët e interesuara përkatëse, duke krijuar një grup të gjerë rekomandimesh për t'i mbajtur fëmijët të sigurt në botën dixhitale. Ato janë rezultat i një përpjekje bashkëpunuese me shumë aktorë, duke shfrytëzuar njohuritë, përvojën dhe ekspertizën e shumë organizatave dhe individëve nga e gjithë bota në fushën e mbrojtjes në internet të fëmijëve. Ata synojnë të krijojnë bazat për një botë të sigurt dhe të sigurt kibernetike për brezat e ardhshëm. Ato kanë për qëllim të veprojnë si një plan, i cili

mund të përshtatet dhe të përdoret në të një mënyrë që është në përputhje me zakonet dhe ligjet kombëtare ose lokale. Për më tepër, këto udhëzime adresojnë çështje që prekin të gjithë fëmijët dhe të rinjtë nën moshën 18 vjeç, duke njohur nevojat e ndryshme të secilës grupmoshë. Për më tepër, ato synojnë të adresojnë nevojat e fëmijëve në kushte të ndryshme të jetesës dhe fëmijëve me nevoja të veçanta dhe aftësi të kufizuara. Udhëzimet gjithashtu forcojnë fushën e mbrojtjes në internet të fëmijëve, duke adresuar të gjitha rreziqet, kërcënimet dhe dëmet që fëmijët mund të hasin në internet dhe t'i ekuilibrojnë këto me kujdes me përfitimet që bota dixhitale mund të sjellë në jetën e fëmijëve.

Shpresohet se këto udhëzime jo vetëm që do të çojnë në ndërtimin e një shoqërie më gjithëpërfshirëse të informacionit, por gjithashtu mundësojnë që Shtetet Anëtare të ITU të përmbushin detyrimet e tyre ndaj mbrojtjes dhe realizimit të të drejtave të fëmijëve siç përcaktohet në Konventën e KB për të Drejtat e Fëmijë, i miratuar nga rezoluta 44/25 e Asamblesë së Përgjithshme të KB të 20 nëntorit 1989 dhe Dokumenti i Rezultateve të Samitit Botëror për Shoqërinë e Informacionit (WSIS).

Përmes nxjerrjes së këtyre udhëzimeve, iniciativa COP u bën thirrje të gjithë aktorëve për të zbatuar politika dhe strategji që do të mbrojnë fëmijët në hapësirën kibernetike dhe promovojnë aksesin e tyre më të sigurt në të gjitha mundësitë e jashtëzakonshme që mund të sigurojnë burimet në internet.

Përmbajtja

Lista e tabelave dhe figurave

Tabelat

Figurat

Boxes

Permbajtja e Dokumentit

1.1 Qellimi

Qeveritë kombëtare kanë detyrimin të sigurojnë mbrojtjen e fëmijëve si në botën fizike ashtu edhe në atë virtuale. Në një kuptim të rëndësishëm, sepse teknologjitë e reja sot janë integruar plotësisht në jetën e kaq shumë fëmijëve dhe të rinjve në një numër mënyrash ku nuk ka më kuptim të përpiqesh të bësh dallime të forta midis ngjarjeve të botës reale dhe ngjarjeve në internet. Të dyja janë gjithnjë e më të ndërthurura dhe të ndërvarura.

Krijuesit e politikave dhe të gjithë aktorët e tjerë aktual luajnë një rol shumë të rëndësishëm. Shpejtësia me të cilën po zhvillohet teknologjia do të thotë që shumë nga metodat tradicionale të politikë-bërjes nuk i përshtaten më këtij qëllimi. Krijuesve të politikave u kërkohet të përpunojnë një kornizë ligjore që është adaptive, gjithëpërfshirëse dhe e përshtatshme për qëllimin në ndryshimin e shpejtë të moshës dixhitale për të mbrojtur fëmijët në internet.

Qëllimi i këtyre udhëzimeve është t'u ofrojë politikëbërësve në Shtetet Anëtare të ITU një kornizë miqësore për përdoruesit dhe fleksibël për të kuptuar dhe vepruar sipas detyrimit të tyre ligjor për të siguruar mbrojtjen e fëmijëve në të dy botët reale, fizike dhe virtuale.

Udhëzimet e bëjnë këtë duke adresuar disa pyetje të rëndësishme për politikëbërësit:

1) Çfarë është mbrojtja e fëmijëve në internet?
2) Pse unë si politikëbërës duhet të kujdesem për mbrojtjen në internet të fëmijëve?
3) Cili është konteksti ligjor, socio-politik dhe i zhvillimit të vendit tim?
4) Si duhet të fillojnë politikë-bërësit të marrin në konsideratë dhe të formojnë një politikë efektive dhe të qëndrueshme për mbrojtjen e fëmijëve në internet në vendin e tyre?

Duke vepruar kështu, udhëzimet mbështeten në modelet, kornizat dhe burimet ekzistuese për të ofruar kontekst dhe pasqyrë të praktikave të duhura nga e gjithë bota.

1.2 Fushëveprimi

Fusha e mbrojtjes në internet e fëmijëve përfshin cdo rrezik ndaj të cilit fëmijët ekspozohen në internet, duke mbuluar një gamë të gjerë rreziqesh që kërcënojnë sigurinë dhe mirëqenien e fëmijëve. Eshtë një sfidë komplekse që duhet trajtuar nga këndvështrime të shumta, përfshirë legjislacionin, qeverisjen, arsimin, politikat dhe shoqërinë.

Për më tepër, mbrojtja në internet e fëmijëve duhet të bazohet në të kuptuarit e rreziqeve, kërcënimeve dhe dëmeve të përgjithshme dhe specifike në mjediset dixhitale. Kjo kërkon përkufizime të qarta dhe vendosjen e parametrave të qartë për ndërhyrjen që përfshijnë dhe bëjnë dallimin midis akteve që përbëjnë një krim dhe atyre që megjithëse nuk janë të paligjshme, paraqesin një kërcënim për mirëqenien e një fëmije.

Për këtë qëllim, udhëzimet japin një përmbledhje të kërcënimeve aktuale dhe dëmtimeve me të cilat përballen fëmijët në mjediset dixhitale. Kjo e lartë përmendur si dhe shpejtësia me të cilën teknologjia , kërcënimet dhe dëmet shoqëruese janë në zhvillim do të thotë që shpejtësia dhe metoda tradicionale e politikëbërjes nuk është në gjendje të mbajë ritmin.Krijuesit e politikave në epokën dixhitale duhet të ndërtojnë korniza ligjore dhe politike që janë mjaft adaptive dhe gjithëpërfshirëse për të trajtuar sfidat ekzistuese dhe për të parashikuar ato që do të vijnë. Arritja e kësaj kërkon bashkëpunim me secilin palë të interesuar, përfshirë industrinë e TIK, komunitetin kërkimor, shoqërinë civile, publikun dhe vetë

fëmijët. Ky proces mund të mbështetet duke marrë parasysh parimet gjithëpërfshirëse në mbrojtjen e fëmijëve në internet.

1.3 Parimet Kryesore

Njëmbëdhjetë parime ndër-sektoriale të paraqitura këtu, të cilat të marra së bashku, do të ndihmojnë në zhvillimin e një strategjie kombëtare për mbrojtjen në internet të fëmijëve me perspektivë dhe holistike.

Renditja e këtyre parimeve pasqyron më tepër një tregim logjik sesa një renditje të bazuar në rëndësinë e secilës prej tyre.

Një strategji kombëtare e mbrojtjes në internet e fëmijëve duhet:

1. Të bazohet në një vizion holistik që përfshin qeverinë, industrinë dhe shoqërinë;

2. Të rezultojë nga një mirëkuptim dhe analizë gjithëpërfshirëse e mjedisit të përgjithshëm dixhital, duke iu përshtatur rrethanave dhe përparësive të vendit;

3. Të respektojë dhe të jetë në përputhje me të drejtat themelore të fëmijëve siç janë të miratuara në KB

Konventa për të Drejtat e Fëmijëve dhe konventat dhe ligjet e tjera kryesore ndërkombëtare;

4. Të respektojë dhe të jetë në përputhje me ligjet dhe strategjitë e brendshme ekzistuese, të njëjta dhe të ngjashme, siç janë ligjet e abuzimit të fëmijëve ose strategjitë e sigurisë së fëmijëve;

5. Të respektojë të drejtat dhe liritë civile të fëmijëve, të cilat nuk duhet t'i flijohen mbrojtjes;

6. Të zhvillohen me pjesëmarrjen aktive të të gjithë aktorëve aktual, përfshirë fëmijët, duke adresuar nevojat dhe përgjegjësitë e tyre dhe duke përmbushur nevojat e grupeve të pakicave dhe të tepricave;

7. Të hartohet për të harmonizuar me planet më të gjera të qeverisë për prosperitetin ekonomik dhe social dhe për të maksimizuar kontributin e TIK në zhvillimin e qëndrueshëm dhe përfshirjen sociale;

8. Të përdorë instrumentet më të përshtatshme të politikës në dispozicion për të realizuar objektivin e saj, duke marrë parasysh rrethanat specifike të vendit;

9. Të vendosen në nivelin më të lartë të qeverisë, i cili do të jetë përgjegjës për caktimin e roleve dhe përgjegjësive përkatëse dhe shpërndarjen e burimeve të mjaftueshme njerëzore dhe financiare;

10. Të ndihmojë në ndërtimin e një mjedisi dixhital që fëmijët, prindërit / kujdestarët dhe palët e interesit mund t'i besojnë;

11. Të udhëzojë përpjekjet e palëve të interesuara për të fuqizuar dhe edukuar fëmijët mbi shkrim-leximin dixhital për të mbrojtur veten në internet.

1.4 Përdorimi i udhëzimeve

Këto udhëzime marrin në konsideratë hulumtimin përkatës, modelet dhe materialin ekzistues, dhe përcaktojnë rekomandime të qarta për zhvillimin e një strategjie kombëtare të mbrojtjes në internet të fëmijëve.

• Seksioni 2 prezanton mbrojtjen në internet të fëmijëve dhe jep pasqyra në hulumtimet e fundit, përfshirë aspektet në lidhje me teknologjitë e reja në zhvillim, kërcënimet kryesore dhe dëmet për fëmijët.

• Seksioni 3 përcakton mënyrën e përgatitjes për një strategji kombëtare të mbrojtjes së fëmijëve online, përfshirë palët e interesuara përkatëse, shembujt ekzistues të përgjigjeve ndaj kërcënimeve dhe dëmtimeve në internet dhe përfitimet e të pasurit një strategji kombëtare.

• Seksioni 4 përfshin rekomandimet për kornizat dhe zbatimin.

• Seksioni 5 përshkruan listat kombëtare të kontrollit për të zhvilluar një strategji kombëtare të mbrojtjes së fëmijëve online.

• Seksioni 6 jep materiale referuese të dobishme.

2. Prezantimi

Në vitin 2019, më shumë se gjysma e popullsisë së botës përdorën internetin. Grupi më i madh i përdoruesve janë ata të moshës nën 44 vjeç, me përdorim po aq të lartë në mes të moshës 16 deri në 24 vjeç dhe 35 deri në 44 vjeç. Në nivelin global, një në tre fëmijë përdor internetin (0-18 vjeç). Në vendet në zhvillim, fëmijët dhe të rinjtë po drejtojnë përdorimin e Internetit dhe parashikohet se gjatë pesë viteve të ardhshme, kjo popullsi do të dyfishohet. Brezat e rinj po rriten me internetin dhe shumica janë duke u lidhur me teknologjinë e rrjetit celular, veçanërisht në jugun global.

Megjithëse aksesi në internet është thelbësor për realizimin e të drejtave të fëmijëve, ekzistojnë ende pabarazi të konsiderueshme rajonale, kombëtare, gjinore dhe të tjera të qasjes që kufizojnë mundësitë për vajzat, fëmijët me aftësi të kufizuara, fëmijët nga pakicat dhe grupet e tjera të prekshme. Për sa i përket ndarjes dixhitale gjinore, hulumtimet tregojnë se në çdo rajon përveç Shteteve të Bashkuara të Amerikës, përdoruesit meshkuj të Internetit janë në masë të madhe se përdoruesit femra. Në shumë vende, vajzat nuk kanë të njëjtat mundësi hyrjeje si djemtë, dhe atje ku kanë, vajzat jo vetëm që monitorohen dhe kufizohen në përdorimin e Internetit në një masë shumë më të madhe, por ato gjithashtu mund të hasin rreziqe në lidhje me sigurinë në përpjekjet për të hyrë Interneti . Eshtë e qartë se fëmijët dhe të rinjtë që nuk kanë aftësi dixhitale ose flasin gjuhë e pakicave nuk mund të gjejnë lehtësisht përmbajtje përkatëse në internet, dhe se fëmijët nga zonat rurale te cilët kanë më pak aftësi dixhitale, kalojnë më shumë kohë në internet (veçanërisht duke luajtur lojëra) dhe marrin më pak ndërmjetësim prindëror dhe monitorimi.

Sidoqoftë, asnjë bisedë rreth rreziqeve dhe kërcënimeve nuk mund të zhvillohet pa pranuar natyrën jashtëzakonisht pasuruese dhe fuqizuese të teknologjisë dixhitale. Interneti dhe teknologjitë dixhitale po transformojnë mënyrën tonë të të jetuarit dhe kanë hapur shumë mënyra të reja për të komunikuar, për të luajtur lojëra, për të shijuar muzikë dhe për t'u angazhuar në një grup të madh kulturor, arsimor dhe zhvillimi aftësish.

Ashtu si fëmijët dhe të rinjtë shpesh janë në qëndër të adaptimit dhe përshtatjes me mundësitë e reja të ofruara nga interneti, ata gjithashtu janë duke u ekspozuar ndaj një vargu çështjesh të lidhura me sigurinë dhe mirëqenien, të cilat duhet të pranohen dhe të ballafaqohen nga shoqëria. Eshtë thelbësore të diskutohen hapur rreziqet që ekzistojnë për fëmijët dhe të rinjtë në internet. Diskutimi hap një platformë nga ku fëmijët dhe të rinjtë mund të mësojnë se si të njohin rrezikun dhe të parandalojnë ose trajtojnë dëmet në rast se ato materializohen, si dhe avantazhet dhe mundësitë që mund të ofrojë interneti.

Në shumë pjesë të botës, të rinjtë kanë një kuptim të mirë të disa prej rreziqeve me të cilat përballen në internet. Hulumtimet kanë treguar, se shumica e fëmijëve dhe të rinjve janë në gjendje të dallojnë ngacmimin në internet nga shakatë ose mashtrimet në internet. Ata e pranojnë që ngacmimi në internet ka një dimension publik dhe është krijuar për të dëmtuar, megjithatë balancimi i mundësive dhe rreziqeve në internet të një fëmije mbetet një sfidë.

Për Shtetet Anëtare të ITU, mbrojtja e fëmijëve dhe të rinjve në internet vazhdon të jetë një përparësi, që duhet të ekuilibrohet me kujdes me përpjekjet për të promovuar mundësi për fëmijë dhe të rinj në internet, dhe se duhet të bëhet në një mënyrë që të mbrojë fëmijët dhe të rinjtë pa ndikuar në aksesin e tyre ose qasjen e publikut të gjerë në informacion, ose aftësinë për të shijuar lirinë e fjalës, shprehjes dhe shoqërimit.

Ekziston një nevojë e qartë për investime të dedikuara dhe zgjidhje kreative për të adresuar rreziqet me të cilat përballen fëmijët dhe të rinjtë, jo më pak për shkak të ndarjes dixhitale midis fëmijëve dhe të rriturve që kufizon udhëzimet nga prindërit, mësuesit dhe kujdestarët. Në të njëjtën kohë, ndërsa fëmijët dhe të rinjtë rriten dhe bëhen prindër dhe anëtarë aktivë të shoqërisë, ekziston një mundësi e mundshme dhe e palejueshme që ata të ulin ndarjen dixhitale.

Në bazë të saj, ndërtimi i besimit në internet duhet të jetë në qendër të politikës publike. Qeveritë dhe shoqëria duhet të punojnë me fëmijë dhe të rinj për të kuptuar perspektivat e tyre dhe për të ndezur debat të mirëfilltë publik rreth rreziqeve dhe mundësive. Mbështetja e fëmijëve dhe të rinjve për të menaxhuar rreziqet në internet mund të jetë efektive, por qeveritë gjithashtu duhet të sigurojnë që ekzistojnë shërbime adekuate

mbështetëse për ata që përjetojnë dëm në internet, dhe se fëmijët janë të vetëdijshëm se si t'i përdorin ato shërbime.

Disa vende përpiqen të alokojnë burime të mjaftueshme për të trajtuar shkrim-leximin dixhital dhe sigurinë e fëmijëve në internet. Sidoqoftë, fëmijët tregojnë se prindërit, mësuesit, kompanitë e teknologjisë dhe qeveritë janë lojtarë të rëndësishëm në zhvillimin e zgjidhjeve për të mbështetur sigurinë e tyre në internet. Shtetet Anëtare të ITU kanë treguar gjithashtu se ka një mbështetje të konsiderueshme për ndarjen e zgjeruar të njohurive dhe përpjekjet e koordinuara për të siguruar sigurinë e një numri më të madh të fëmijëve në internet.

Fëmijët dhe të rinjtë po lundrojnë në një peisazh dixhital gjithnjë e më të ndërlikuar dhe adaptimi me zhvillimin e inteligjencës artificiale, analitikë të të dhënave, robotikë, realitet virtual dhe të shtuar si dhe Interneti i Gjërave janë në rrugën e transformimit të praktikave mediatike të fëmijëve. Kjo kërkon politikëbërje dhe investime për fëmijët, prindërit dhe komunitetet e së ardhmes aq sa për sot.

2.1 Çfarë është mbrojtja internet e fëmijëve në internet?

Teknologjitë në internet paraqesin shumë mundësi që fëmijët dhe të rinjtë të komunikojnë, të mësojnë aftësi të reja, të jenë krijues dhe të kontribuojnë për një shoqëri më të mirë. Por ato gjithashtu mund të sjellin rreziqe të reja, siç janë ekspozimi i tyre ndaj çështjeve të privatësisë, përmbajtjes së paligjshme, ngacmimit, bulizmit në internet, keqpërdorimit të të dhënave personale ose shfrytëzimit për qëllime seksuale dhe madje edhe abuzimit seksual të fëmijëve.

Këto udhëzime zhvillojnë një qasje holistike për t'iu përgjigjur të gjitha kërcënimeve dhe dëmeve të mundshme që fëmijët dhe të rinjtë mund të hasin kur fitojnë njohuri dixhitale. Ata e pranojnë që të gjithë palët e interesuara përkatëse kanë një rol në qëndrueshmërinë, mirëqenien dhe mbrojtjen e tyre dixhitale ndërsa përfitojnë nga mundësitë që mund të ofrojë Interneti.

Mbrojtja e fëmijëve dhe të rinjve është një përgjegjësi e përbashkët dhe u takon të gjithë aktorëve aktual të sigurojnë një të ardhme të qëndrueshme për të gjithë. Për të ndodhur kjo, politikëbërësit, industria, prindërit, kujdestarët, edukatorët dhe aktorët e tjerë të interesuar, duhet të sigurojnë që fëmijët dhe të rinjtë mund të përbushin potencialin e tyre - në internet dhe jashtë linje.

Ndërsa nuk ekziston ndonjë përkufizim universal për mbrojtjen në internet të fëmijëve, ai synon të marrë një qasje holistike për ndërtimin e hapësirave dixhitale të sigurta, të përshtatshme për moshën, përfshirëse dhe pjesëmarrëse për fëmijë dhe të rinj, të karakterizuara nga:

• *përgjigje, mbështetje dhe vetë-ndihmuese përballë kërcënimit;*

• *parandalimin e dëmit;*

• *një ekuilibër dinamik ndërmjet sigurimit të mbrojtjes dhe ofrimit të mundësisë që fëmijët të jenë qytetarë dixhitalë;*

• *përkrahja e të drejtave dhe përgjegjësive të fëmijëve dhe shoqërisë.*

Për më tepër, për shkak të përparimeve të shpejta në teknologji dhe shoqëri dhe natyrës pa kufi të internetit, mbrojtja në internet e fëmijëve duhet të jetë e përpiktë dhe e adaptueshme për të qenë efektive. Ndërsa këto udhëzime ofrojnë pasqyrë në rreziqet kryesore për fëmijët dhe të rinjtë në internet, përfshirë përmbajtjet e dëmshme dhe të paligjshme, ngacmimet, bulizimet në internet, keqpërdorimin e të dhënave personale, ose shfrytëzimin për qëllime seksuale dhe abuzimin seksual të fëmijëve, sfida të reja do të shfaqen me zhvillimin e inovacioneve teknologjike dhe zakonisht do të ndryshojnë nga rajoni në rajon. Sidoqoftë, sfidat e reja do të trajtohen më së miri duke punuar së bashku si një komunitet global, pasi duhet të gjenden zgjidhje të reja për këto sfida.

2.2 Fëmijët në botën dixhitale

Interneti ka transformuar mënyrën se si jetojmë. Eshtë integruar plotësisht në jetën e fëmijëve dhe të rinjve, duke e bërë të pamundur marrjen në konsideratë të botës dixhitale dhe fizike veç e veç. Një e treta e të gjithë përdoruesve të internetit sot janë fëmijë dhe të rinj dhe UNICEF vlerëson se 71 përqind e të rinjve janë tashmë në internet.

Një lidhje e tillë ka qenë jashtëzakonisht fuqizuese. Bota në internet lejon që fëmijët dhe të rinjtë të kapërcejnë disavantazhet dhe aftësinë e kufizuar dhe ka ofruar mundësi të reja për argëtim, edukim, pjesëmarrje dhe ndërtimin e marrëdhënieve. Platformat dixhitale, sot, përdoren për një larmi aktivitetesh dhe shpesh janë përvoja multi-mediatike.

Të kesh qasje dhe të mësosh të përdorësh dhe navigosh këtë teknologji shihet si kritike për zhvillimin e të rinjve dhe përdoren së pari në moshë të re. Krijuesit e politikave duhet të kuptojnë që fëmijët dhe të rinjtë shpesh fillojnë të përdorin platforma dhe shërbime para se të arrijnë moshën minimale të përshkruar, dhe për këtë arsye, arsimi duhet të fillojë herët.

Fëmijët dhe të rinjtë duan të përfshihen në bisedë dhe ata kanë një ekspertizë të vlefshme si native vendas digjitalë. Krijuesit e politikave dhe praktikuesit duhet të angazhohen me fëmijë dhe të rinj në një debat të vazhdueshëm rreth mjedisit në internet për të mbështetur të drejtat e tyre.

Aksesi në internet

Në vitin 2019, më shumë se gjysma e popullsisë së botës përdorën internetin (53.6 përqind), me rreth 4.1 miliardë përdorues. Në nivelin global, një në tre përdorues të Internetit janë fëmijë nën moshën 18 vjeç 1. Në disa vende me të ardhura më të ulëta, kjo rritet në rreth një në dy ndërsa në vendet me të ardhura më të larta, raporti është rreth një në pesë. Sipas UNICEF, në të gjithë botën, 71 përqind e të rinjve janë tashmë në internet 2. Fëmijët dhe të rinjtë janë një prani thelbësore, e përhershme dhe këmbëngulëse në Internet 3. Interneti shërben për qëllime të tjera shoqërore, ekonomike ose politike dhe është bërë një familje ose produkt i konsumatorit ose shërbim i cili është pjesë integrale e mënyrës se si jetojnë familjet dhe fëmijët dhe të rinjtë.

Në vitin 2017, rajonalisht, qasja në internet e fëmijëve dhe të rinjve është shumë e lidhur me nivelin e të ardhurave. Vendet me të ardhura të ulëta kanë tendencë të kenë më pak fëmijë përdorues të internetit sesa vendet me të ardhura të larta.

Fëmijët dhe të rinjtë në shumicën e vendeve kalojnë më shumë kohë në internet gjatë fundjavës sesa në një ditë jave, me adoleshentët (15–17 vjeç) që kalojnë më gjatë në internet, mes 2.5 dhe 5.3 orë mesatarisht, në varësi të vendit.

Përdorimi i internetit

Midis fëmijëve dhe të rinjve, pajisja më e popullarizuar për të hyrë në internet është telefoni celular, i ndjekur nga kompjuterat desktop dhe laptopët. Fëmijët dhe të rinjtë kalojnë mesatarisht rreth dy orë në ditë gjatë javës dhe përafërsisht dyfishin e tyre çdo dite të fundjavës. Disa qëndrojnë të lidhur gjithë kohën në internet ndërsa shumë të tjerë ende nuk kanë qasje në internet në shtëpi.

---

1 Livingstone, S., Carr, J., and Byrne, J. (2015) *One in three: The task for global internet governance in addressing children's rights*. Global Commission on Internet Governance: Paper Series. London: CIGI and Chatham House, https:// www .cigionline .org/ publications/ one -three -internet -governance -and -childrens -rights.

2 Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)," *Broadband Commission for Sustainable Development,* October 2019, 84, https:// broadbandcommission .org/ Documents/ working -groups/ ChildOnlineSafety _Report .pdf.

3 Livingstone, Carr, and Byrne, "One in Three: Internet Governance and Children's Rights."

Në praktikë, shumica e fëmijëve dhe të rinjve që përdorin Internetin, e përdorin atë përmes më shumë se një pajisje: Fëmijët dhe të rinjtë që lidhen të paktën çdo javë ndonjëherë përdorin deri në tre pajisje të ndryshme për ta bërë këtë. Fëmijët më të rritur dhe fëmijët në vendet më të pasura zakonisht përdorin më shumë pajisje dhe djemtë përdorin pak më shumë pajisje sesa vajzat në çdo vend të anketuar.

Aktiviteti më i popullarizuar - për vajzat dhe djemtë - është shikimi i videoklipeve. Më shumë se tre të katërtat e fëmijëve dhe të rinjve që përdorin internet thonë se ata shikojnë video në internet të paktën çdo javë, ose vetëm ose me anëtarët e tjerë të familjes së tyre. Shumë fëmijë dhe të rinj mund të konsiderohen 'aktivë 'duke përdorur disa platforma të mediave sociale si Facebook, Twitter, TikTok ose Instagram.

Fëmijët dhe të rinjtë gjithashtu merren me politikë në internet dhe i bëjnë të dëgjohen zërat e tyre përmes blogjeve.

Niveli i përgjithshëm i pjesëmarrjes në lojërat në internet ndryshon nga vendi përafërsisht në përputhje me disponueshmërinë e fëmijëve dhe të rinjve për të hyrë në internet, ndërsa 10 deri në 30 për qind e fëmijëve dhe të rinjve që përdorin internetin merren me aktivitete krijuese në internet në baza javore.

Për qëllime edukative, shumë fëmijë dhe të rinj të të gjitha moshave përdorin internetin për detyrat e shtëpisë, apo edhe për të arritur pas humbjes së orëve të mësimit ose për të kërkuar informacion shëndetësor në internet në baza javore. Fëmijët më të rritur duket se kanë një dëshirë më të madhe për informacion sesa fëmijët më të vegjël.

2.3 Ndikimi i teknologjisë në përvojën dixhitale të fëmijëve

Interneti dhe teknologjia dixhitale mund të ofrojnë mundësi dhe të paraqesin rreziqe për fëmijët dhe të rinjtë. Për shembull, kur fëmijët përdorin mediat sociale, ata përfitojnë nga shumë mundësi për të eksploruar, mësuar, komunikuar dhe zhvilluar aftësitë kryesore. Për shembull, rrjetet sociale shihen nga fëmijët si platforma që i lejojnë ata të eksplorojnë identitetin personal në një mjedis të sigurt. Të kesh aftësitë përkatëse dhe të dish si të merresh me çështje që lidhen me privatësinë dhe reputacionin është e rëndësishme për të rinjtë.

"Unë e di se gjithçka që postoni në internet qëndron përgjithmonë dhe kjo mund të ndikojë në jetën tuaj në të ardhmen", Djalë, 14 vjeç, Kili.

Sidoqoftë, me konsultat që tregojnë se shumica e fëmijëve që përdorin media sociale para moshës minimale trembëdhjetë vjeç, dhe shërbimet e verifikimit të moshës janë përgjithësisht të dobëta ose që mungojnë, rreziqet me të cilat përballen fëmijët mund të intensifikohen. Dhe ndërsa fëmijët duan të mësojnë aftësi dixhitale dhe të bëhen qytetarë dixhitalë, veçanërisht duke u kujdesur për privatësinë e tyre, ata priren të mendojnë për privatësinë në lidhje me miqtë dhe të njohurit e tyre - "Çfarë mund të shohin miqtë e mi?" - dhe më pak në lidhje me të huajt dhe palët e treta. Kombinuar me kureshtjen natyrore të fëmijëve dhe pragun përgjithësisht më të ulët të rrezikut, kjo mund t'i bëjë ata të prekshëm nga rregullimi, shfrytëzimi, ngacmimi ose lloje të tjera të përmbajtjes së dëmshme ose kontakti.

Popullariteti i përhapur i ndarjes së imazheve dhe videove përmes aplikacioneve mobile, dhe veçanërisht përdorimi i platformave të drejtpërdrejta të transmetimit nga fëmijët paraqet shqetësime të mëtejshme të privatësisë dhe rrezikut. Disa fëmijë po prodhojnë imazhe seksuale të tyre, miqve dhe të afërmëve dhe po i ndajnë ato në internet. Për disa, veçanërisht për fëmijët e moshuar, kjo mund të shihet si eksplorim natyror i seksualitetit dhe identitetit seksual, ndërsa për të tjerët, veçanërisht për fëmijët më të vegjël shpesh ka detyrim nga një i rritur ose një fëmijë tjetër. Sido që të jetë rasti, përmbajtja që rezulton është në shumë vende ilegale dhe mund t'i ekspozojë fëmijët ndaj rrezikut të ndjekjes penale, ose mund të përdoret për të shfrytëzuar më tej fëmijën.

Në mënyrë të ngjashme, lojërat në internet u mundësojnë fëmijëve të përmbushin të drejtën e tyre themelore për të luajtur, si dhe të ndërtojnë rrjete, të kalojnë kohë me të dhe të takojnë miq të rinj dhe të zhvillojnë aftësi të rëndësishme. Në shumicën e rasteve, kjo mund të jetë pozitive. Sidoqoftë, ka gjithnjë e më shumë prova për të treguar se të lënë pa vëzhgim dhe të pambështetur nga një i rritur i përgjegjshëm, platformat e lojërave në internet mund të paraqesin rreziqe për fëmijët, nga çrregullimet e lojrave, rreziqet financiare, mbledhja dhe monetarizimi i të dhënave personale të fëmijëve, te ngacmimi në internet, gjuha e urrejtjes, dhuna , dhe ekspozimi ndaj sjelljes ose përmbajtjes së

papërshtatshme, dhe pastrimi duke përdorur imazhe dhe video reale, të krijuara nga kompjuteri apo edhe realitet virtual që përshkruajnë dhe normalizojnë abuzimin seksual dhe shfrytëzimin e fëmijëve.

Për më tepër, zhvillimet në teknologji kanë çuar në shfaqjen e Internetit të gjërave, ku një numër në rritje e pajisjeve janë në gjendje të lidhen, komunikojnë dhe rrjetëzohen përmes Internetit. Kjo përfshin lodrat, vëzhguesit e foshnjave dhe pajisjet e mundësuara nga inteligjenca artificiale që mund të paraqesin rreziqe në lidhje me privatësinë dhe kontaktet e padëshiruara.

2.4 Kërcënimet kryesore për fëmijët në internet

Të rriturit dhe fëmijët janë të ekspozuar ndaj një sërë rreziqesh në internet. Sidoqoftë, fëmijët janë një popullsi shumë më e prekshme. Disa fëmijë janë gjithashtu më të prekshëm se grupet e tjera të fëmijëve, për shembull fëmijë me aftësi të kufizuara ose fëmijë në lëvizje. Bërësit e politikave duhet të garantojnë që të gjithë fëmijët mund të zhvillohen dhe arsimohen në një mjedis dixhital të sigurt. Ideja që fëmijët janë të prekshëm dhe duhet të mbrohen nga të gjitha format e shfrytëzimit përshkruhet në Konventën e KB për të Drejtat e Fëmijëve.

Disa zona në mjedisin dixhital ofrojnë mundësi të mëdha për fëmijët, por në të njëjtën kohë mund të përbëjnë rreziqe që mund të dëmtojnë thellësisht fëmijët dhe të dëmtojnë mirëqenien e tyre. Ekzistojnë shqetësime, për të rriturit dhe fëmijët ashtu që për shembull interneti mund të përdoret për të pushtuar privatësinë personale, dezinformimin e lundrimit në internet ose më keq, për të lejuar hyrjen në pornografi.

Është thelbësore të bëhet dallimi midis rreziqeve dhe dëmtimeve për fëmijët. Jo çdo aktivitet që mund të ketë elementë të rrezikut është i rrezikshëm dhe jo të gjitha rreziqet bëhen domosdoshmërisht të dëmshme për fëmijët, për shembull, Sexting, e cila është një mënyrë që të rinjtë mund të eksplorojnë seksualitetin dhe marrëdhëniet, dhe që nuk është domosdoshmërisht e dëmshme.

	Permbajtja Femija si marres (e prodhimit ne mase)	**Kontakti** Femija si pjesmarres (te rriturit-iniciator)	**Sjellja** Femija si aktor (viktim)
Agresive	**Permbajtje e dhunshme/e rende**	**Ngacmimet, perndjekjet**	**Bullizim nga moshataret e tij**
Seksuale	**Permbajtje pornografike**	**Abuzime seksuale ne takime me te huaj**	**Ngacmime seksuale me mesasazhe**
Vlersuese	**Permbajtje raciste/urrejtje**	**Bindje Ideologjike**	**Permbajtje te rrezikshme**
Reklamues	**Reklamime**	**Keqperdorim i te dhenave personale**	**Bixhoz,plagjature, shkelje**

Figure 2. Klasifikimi i kërcënimeve në internet për fëmijët

Burime: EU Kids Online (Livingstone, Haddon, Görzig, and Ólafsson (2011)

Ardhja e epokës dixhitale ka paraqitur sfida të reja për mbrojtjen e fëmijëve. Fëmijët duhet të fuqizohen të lundrojnë në mënyrë të sigurt në botën online dhe të korrin shpërblimet e saj të shumta.

Krijuesit e politikave duhet të sigurojnë që legjislacioni përkatës, masat mbrojtëse dhe mjetet janë në dispozicion për t'i lejuar fëmijët të zhvillohen dhe të mësojnë në mënyrë të sigurt. Eshtë e rëndësishme që fëmijët të jenë të pajisur me aftësitë e nevojshme për të identifikuar kërcënimet dhe për të kuptuar plotësisht implikimet dhe nuancat e sjelljes së tyre në internet.

Ndërsa janë në internet, fëmijët mund të hasin në një mori kërcënimesh nga organizatat, të rriturit dhe bashkëmoshatarët e tyre.

Përmbajtja dhe manipulimi

• Ekspozimi ndaj përmbajtjes së papërshtatshme apo edhe kriminale mund t'i çojë fëmijët në ekstreme si vetë-dëmtimi, sjelljet shkatërruese dhe të dhunshme. Ekspozimi ndaj një përmbajtje të tillë mund të çojë në mënyrë të barabartë në radikalizim ose pajtim në ide raciste ose diskriminuese. Recognizedshtë e njohur që shumë fëmijë nuk u përmbahen kufizimeve të moshës të vendosura në faqet e internetit.

• Ekspozimi ndaj informacionit të pasaktë ose jo të plotë kufizon kuptimin e fëmijëve për botën përreth tyre. Trendi i personalizimit të përmbajtjes bazuar në sjelljen e përdoruesit mund të çojë në bub flluska filtri ', duke kufizuar fëmijët nga zhvillimi dhe arritja e një game të gjerë të përmbajtjes.

• Ekspozimi ndaj përmbajtjes që filtrohet algoritmikisht me synimin për të manipuluar mund të ndikojë shumë në zhvillimin, mendimet, vlerat dhe zakonet e një fëmije. Izolimi i fëmijëve në m dhomat e ekos 'ose bub flluska filtri' i pengon ata të kenë qasje në një larmi mendimesh dhe idesh.

Kontakti me të rriturit ose moshatarët

Fëmijët mund të hasin një gamë të gjerë kërcënimesh kontakti nga moshatarët e tyre ose të rriturit.

• Ngacmimi në internet mund të përhapet më gjerësisht, me një shkallë më të madhe shpejtësie sesa jashtë linje. Mund të ndodhë në çdo kohë të ditës ose natës, duke pushtuar kështu 'hapësirat e sigurta' më parë, dhe mund të jetë anonime.

• Fëmijët që janë viktimizuar jashtë linje ka të ngjarë të viktimizohen në internet. Kjo i vendos fëmijët me aftësi të kufizuara në rrezik më të lartë në internet, pasi hulumtimet tregojnë se fëmijët me aftësi të kufizuara kanë më shumë të ngjarë të përjetojnë abuzime të çdo lloji, dhe posaçërisht kanë më shumë gjasa të përjetojnë viktimizim seksual. Viktimizimi mund të përfshijë ngacmimin, përjashtimin dhe diskriminimin bazuar në paaftësinë aktuale ose të perceptuar të një fëmije, ose në aspektet që lidhen me paaftësinë e tij, siç janë mënyra se si ata sillen ose flasin, ose pajisjet ose shërbimet që ata përdorin.

• Shpifja dhe dëmtimi i reputacionit: imazhet dhe videot mund të ndryshohen dhe t'u ndahen miliarda njerëzve. Komentet e gjykuara keq mund të jenë në dispozicion për dekada, falas për këdo për t'i parë.

• Fëmijët mund të vihen në shënjestër, të pastrohen dhe të keqtrajtohen përmes Internetit nga një shkelës lokal ose në anën tjetër të botës, shpesh duke pretenduar të jenë dikush që nuk janë. Kjo mund të marrë disa forma, përfshirë radikalizimin ose detyrimin për të dërguar përmbajtje të qartë seksuale të vetvetes.

• Të qenit nën presion, mashtrim ose detyrim për të bërë blerje me ose pa lejen e paguesit të faturës.

• Reklamimi i padëshiruar ngre çështje të pëlqimit dhe shitjes së të dhënave.

Sjellja e fëmijës, duke sjellë potencialisht pasoja

• Ngacmimi në internet mund të jetë veçanërisht i mërzitshëm dhe i dëmshëm sepse mund të përhapet më gjerësisht, me një shkallë më të madhe të reklamimit, dhe përmbajtja e qarkulluar në mënyrë elektronike mund të rishfaqet në çdo kohë, gjë që mund ta bëjë më të vështirë për viktimën e ngacmimit që të mbyllet për incidentin ; mund të përmbajë imazhe vizuale të dëmshme ose fjalë lënduese; përmbajtja është në dispozicion 24 orë në ditë; ngacmimi me mjete elektronike mund të ndodhë 24/7 kështu që mund të pushtojë privatësinë e viktimës edhe në vende ndryshe 'të sigurta' siç është shtëpia e tyre; dhe informacioni personal mund të manipulohet, imazhet vizuale të ndryshohen dhe këto të kalohen te të tjerët. Për më tepër, mund të kryhet në mënyrë anonime. Zbulimi i informacionit personal që çon në rrezik të dëmtimit fizik, duke përfshirë takime në jetën reale me të njohurit në internet, me mundësinë e abuzimit fizik dhe / ose seksual.

• Shkelja e tyre ose e të drejtave të të tjerëve përmes plagjiaturës dhe ngarkimit të përmbajtjes pa leje, përfshirë marrjen dhe ngarkimin e fotove të papërshtatshme pa leje.

• Shkelja e të drejtës së autorit të personave të tjerë, p.sh., duke shkarkuar muzikë, filma ose programe televizive që duhet të paguhen pasi kjo mund të jetë e dëmshme për viktimën e vjedhjes.

• Përdorimi i detyrueshëm dhe i tepruar i internetit dhe / ose lojërave në internet, në dëm të aktiviteteve sociale dhe / ose të jashtme të rëndësishme për shëndetin, ndërtimin e besimit, zhvillimin shoqëror dhe mirëqenien e përgjithshme.

• Përpjekje për të dëmtuar, ngacmuar ose ngacmuar dikë tjetër, duke përfshirë pretendimin se jeni dikush tjetër, shpesh një fëmijë tjetër.

• Një sjellje gjithnjë e më e zakonshme nga adoleshentët është 'sexting' (ndarja e imazheve ose teksteve të seksualizuara përmes celularëve). Këto imazhe dhe tekst shpesh ndahen midis partnerëve në një marrëdhënie ose me partnerë të mundshëm, por ndonjëherë përfundojnë duke u ndarë me audienca shumë më të gjera. Nuk ka gjasa që adoleshentët e rinj të kenë një kuptim adekuat të implikimeve të këtyre sjelljeve dhe rreziqeve të mundshme që ato sjellin.

2.5 Dëmet kryesore për fëmijët në internet

Seksioni i mëparshëm i referohet kërcënimeve që fëmijët mund të hasin në internet. Kjo pjesë nënvizon dëmet që mund të ndodhin nga ato kërcënime.

Dëmtimi

Sipas studimeve të UNICEF mbi përdorimin e internetit, kategoritë e mëposhtme konsiderohen rreziqe dhe dëmtime:

- Abuzimi me vetveten dhe vetë-dëmtimi:

• përmbajtje vetëvrasjeje

• diskriminim

- Ekspozimi ndaj materialeve të papërshtatshme:

• ekspozimi ndaj përmbajtjes ekstremiste / të dhunshme / të ashpër

• marketing i ngulitur

• bixhoz në internet

- Rreth 20 për qind e fëmijëve të anketuar mbi këtë çështje thanë se kishin parë, gjatë vitit të kaluar, faqe në internet ose diskutime në internet rreth njerëzve që dëmtonin fizikisht ose dëmtonin veten e tyre. - Radikalizimi:

• bindje ideologjike

• gjuhë urrejtjeje

- Fëmijët kishin më shumë të ngjarë të raportonin se ishin të mërzitur nga gjuha e urrejtjes ose përmbajtja seksuale në internet, duke u trajtuar në një mënyrë të dëmshme në internet ose jashtë linje, ose duke takuar dikë ballë për ballë që ata kishin njohur më parë në internet. - Abuzimi dhe shfrytëzimi seksual:

• përmbajtje të vetë-gjeneruar

• Pastrimi seksual

• material për abuzim seksual të fëmijëve (CSAM)

• trafikimi

• shfrytëzimi seksual i fëmijëve në udhëtime dhe turizëm

Një studim i vitit 2017 për fëmijët në Danimarkë, Hungari dhe Mbretërinë e Bashkuar zbuloi se 6 për qind e fëmijëve kishin shpërndarë fotografi të tyre pa lejen e tyre.

Në vitin 2019, Fondacioni i Shikimit të Internetit (IWF) identifikoi më shumë se 132,000 faqe në internet të konfirmuara se përmbajnë imazhe dhe video të abuzimit seksual të fëmijëve. Çdo faqe në internet mund të përmbajë gjithçka nga një deri në mijëra imazhe të këtij abuzimi.

Rreziqet që lidhen me dhunën në internet, të tilla si shpërndarja e fotove nudo pa pëlqim dhe ngacmimi kibernetik seksual, shënohen nga dinamika të pabarabarta gjinore, me vajzat që zakonisht preken më shumë nga presionet gjinore ndaj sjelljes seksuale, duke përjetuar pasoja më negative dhe shkaktare dëmtimi

- Shkelja dhe keqpërdorimi i të dhënave personale:

• pirateri

• mashtrim dhe vjedhje

Shumë njerëz janë të njohur me mashtrimet dhe piraterinë, por cënimi i privatësisë në lidhje me aktivitetet në internet të një fëmije shihet si një shkelje tjetër. Të rriturit shpesh minojnë të rinjtë duke kontrolluar me kujdes telefonat e tyre celularë dhe duke vëzhguar aktivitetet e tyre në internet, për shembull, raportet nga fëmijët në Brazil tregojnë se djemtë dhe vajzat, nga mosha të ndryshme, i perceptojnë prindërit si më kontrollues të përdorimit të vajzave nga interneti. Përpjekjet për të shpjeguar këtë shpesh sugjerojnë që vajzat mund të jenë në disa raste më të prekshme për shkak të strukturave shoqërore brenda të cilave ata jetojnë, veçanërisht në lidhje me sigurinë e tyre, në një kontekst ku kufiri midis ndërveprimit online dhe offline bëhet gjithnjë e më i paqartë.

- Ngacmimi në internet, ndjekja dhe ngacmimi: Aktivitet armiqësor dhe i dhunshëm i kolegëve

Dhomat e bisedave dhe faqet e rrjeteve sociale mund të hapin derën e dhunës dhe ngacmimit, pasi përdoruesit anonimë, përfshirë të rinjtë, përfshihen në një komunikim agresiv ose abuziv. Në të gjithë shtatë vendet në Evropë - Belgjika, Danimarka, Irlanda, Italia, Portugalia, Rumania dhe Mbretëria e Bashkuar - Livingstone, Mascheroni, Ólafsson dhe Haddon1 zbuluan se mesatarisht, në 2010, 8 për qind e fëmijëve ishin ngacmuar në internet, ndërsa 12 për qind e fëmijëve ishin viktima të ngacmimit në internet në 2014.

Essentialshtë thelbësore të theksohet se fëmijët e prekshëm shpesh janë në një rrezik më të lartë të viktimizimit të ngacmimit në internet.

[1] Livingstone, S., Mascheroni, G., Ólafsson, K., and Haddon, L., (2014) Rreziqet dhe mundësitë në internet të fëmijëve: gjetjet krahasuese nga EU Kids Online dhe Net Children Go Mobile. Londër: Shkolla e Ekonomisë në Londër dhe Shkenca Politike, www .eukidsonline .net dhe hYp:// www .netchildrengomobile .eu/ .

Në fokus: Rritja e pabarazive

I në 2017, rreth 60 për qind e fëmijëve nuk ishin në internet në rajonin e Afrikës, krahasuar me vetëm 4 për qind në Evropë. Përdoruesit meshkuj të internetit tejkalojnë numrin e përdoruesve të grave në çdo rajon botëror dhe përdorimi i internetit nga vajzat shpesh monitorohet dhe kufizohet. Me zgjerimin e brezit të gjerë në pjesët e palidhura të botës kjo pabarazi do të rritet ndjeshëm.

Fëmijët që mbështeten në celularë sesa në kompjuter mund të marrin vetëm një përvojë të dytë më të mirë në internet. Fëmijët që flasin gjuhë të pakicave shpesh nuk mund të gjejnë përmbajtje përkatëse në internet, dhe fëmijët nga zonat rurale kanë më shumë të ngjarë të përjetojnë vjedhje të fjalëkalimeve ose parave.

Komisioni Broadband, “Siguria Online e Fëmijëve: Minimizimi i Rrezikut të Dhunës, Abuzimit dhe Shfrytëzimit

Kërkimet tregojnë, se shumë adoleshentë në të gjithë botën duhet të lundrojnë në pengesa të rëndësishme për pjesëmarrjen e tyre në internet. Për shumë, sfidat e aksesit - lidhja e dobët, kostot ndaluese të të dhënave dhe pajisjeve dhe mungesa e pajisjeve të përshtatshme - mbeten pengesat kryesore.

Me zgjerimin e brezit të gjerë të përballueshëm në botën në zhvillim, ekziston një nevojë urgjente për të vendosur masa për të minimizuar rreziqet dhe kërcënimet ndaj këtyre fëmijëve, duke lejuar gjithashtu që të përfitojnë nga të gjitha përfitimet e botës dixhitale.In Focus: Child Sexual Abuse Material (CSAM)

Shkalla e problemit

Interneti ka transformuar shkallën dhe natyrën e prodhimit, shpërndarjes dhe disponueshmërisë së CSAM. Në vitin 2018, kompanitë e teknologjisë me qendër në Shtetet e Bashkuara të Amerikës raportuan mbi 45 milion imazhe dhe video në internet që dyshohet se tregojnë abuzime seksuale të fëmijëve nga e gjithë bota. Kjo është një industri globale dhe shkalla dhe ashpërsia e abuzimit po rritet megjithë përpjekjet për ta ndaluar atë.

Historikisht, në një botë jashtë linje, gjetja e CSAM kërkoi që shkelësit të marrin rreziqe të konsiderueshme, me shpenzime të konsiderueshme, për të hyrë në material. Me internet, shkelësit e ligjit tani mund të hyjnë në këtë material relativisht lehtë dhe të përfshihen në sjellje gjithnjë e më të rrezikshme. Kamerat janë më të vogla, gjithnjë e më të integruara në çdo aspekt të jetës sonë, duke e bërë më të lehtë procesin e prodhimit të CSAM dhe marrjen e përmbajtjes nga abuzimi pa kontakt.

15 Online (2019).”

Është e pamundur të përcaktohet madhësia ose forma e saktë e kësaj ndërmarrje klandestine dhe ilegale. Sidoqoftë, është e qartë se numri i imazheve të paligjshme tani në qarkullim mund të llogaritet në miliona. Pothuajse të gjithë fëmijët e përfshirë në imazhe kanë imazhin e tyre të dyfishuar. Në vitin 2018, IWF gjurmoi se sa shpesh shfaqeshin imazhe të një fëmije i cili dihej se ishte shpëtuar në 2013. Gjatë tre muajve, analistët e IWF gjurmuan imazhet 347 herë - 5 herë çdo ditë pune.

Peisazhi aktual

Sa herë që një imazh i një abuzimi të një fëmije shfaqet dhe rishfaqet në internet, ose shkarkohet nga një shkelës, ai fëmijë po abuzohet përsëri. Viktimat janë të detyruara të jetojnë me jetëgjatësinë dhe qarkullimin e këtyre imazheve për pjesën tjetër të jetës së tyre.

Sapo të zbulohet abuzimi seksual i fëmijëve me materialin që përshkruan ose një faqe në internet, është e rëndësishme të hiqni ose bllokoni përmbajtjen sa më shpejt që të jetë e mundur. Natyra globale e internetit e bën këtë të vështirë: shkelësit e ligjit mund të prodhojnë materiale në një vend dhe ta presin atë në një tjetër për konsumatorët në një të tretën. Është pothuajse e pamundur që urdhrat ose njoftimet kombëtare të miratohen pa një bashkëpunim të sofistikuar ndërkombëtar.

Ritmi i inovacionit brenda botës dixhitale do të thotë që peisazhi i shkelësit po zhvendoset vazhdimisht. Kërcënimet kryesore që janë shfaqur kohët e fundit përfshijnë:

• Rritja e kriptimit lejon pa dashje shkelësit të veprojnë dhe ndajnë materialin me kanale të fshehura, ndërsa në mënyrë të barabartë e bën më sfiduese zbulimin dhe zbatimin e ligjit.

• Forumet kushtuar rregullimit të fëmijëve po rriten në cepat e mbrojtur të Internetit, duke normalizuar dhe inkurajuar këtë sjellje, shpesh duke kërkuar që content përmbajtja e re ’të bashkohet.

• Zgjerimi i shpejtë i internetit po u mundëson përdoruesve të hyjnë në internet në zona që ende nuk duhet të zhvillojnë / implementojnë një strategji gjithëpërfshirëse të mbrojtjes ose infrastrukturën përkatëse.

• Fëmijët po përdorin pajisje pa mbikëqyrje në moshat më të reja dhe sjellja seksuale në internet po normalizohet. Numri i imazheve të krijuara nga vetë-abuzimi po rritet çdo vit.

Në Fokus: Përmbajtja e gjeneruar nga vetvetja

Fëmijët dhe adoleshentët mund të marrin fotografi ose video kompromet uese të tyre. Ndërsa kjo sjellje në vetvete nuk është domosdoshmërisht e paligjshme dhe mund të ndodhë si pjesë e zhvillimit normal, të shëndetshëm seksual, ekzistojnë rreziqe që çdo përmbajtje e tillë të mund të qarkullojë në internet ose jashtë linje për të dëmtuar fëmijët ose të përdoret si bazë për të zhvatur favore. Megjithëse disa fëmijë mund të bëhen nën presion ose të detyrohen të ndajnë imazhe seksuale, të tjerët, (në veçanti adoleshentët) mund të prodhojnë me dëshirë përmbajtje seksuale. Kjo nuk do të thotë që ata pranojnë ose janë përgjegjës për përdorimin shfrytëzues ose abuziv dhe / ose shpërndarjen e këtyre imazheve.

Sexting është përcaktuar si "vetë-prodhimi i imazheve seksuale", ose si "shkëmbimi i mesazheve ose imazheve seksuale" dhe "krijimi, ndarja dhe përcjellja e imazheve nudo ose gati nudo sugjeruese seksuale përmes telefonave celularë dhe / ose internetit ” Sexting është një formë e përmbajtjes së qartë seksuale të vetë-gjeneruar, dhe praktika është "shumë e larmishme në aspektin e kontekstit, kuptimit dhe qëllimit".

Ndërsa sexting është ndoshta forma më e zakonshme e përmbajtjes së qartë seksuale të vetë-gjeneruar që përfshin fëmijë, dhe shpesh bëhet nga dhe midis adoleshentëve që japin pëlqim nga përvoja, ka edhe shumë forma të sexting të padëshiruar. Kjo i referohet aspekteve jo-konsensuale të veprimtarisë, të tilla

si ndarja ose marrja e fotove, videove ose mesazheve të qarta seksuale të padëshiruara, për shembull nga persona të njohur ose të panjohur që përpiqen të krijojnë kontakt, të ushtrojnë presion ose të rregullojnë fëmijën. Sexting mund të jetë gjithashtu një formë e ngacmimit seksual, ku një fëmijë është nën presion për të dërguar një foto tek një i dashur / e dashura / bashkëmoshatari i cili më pas e shpërndan atë në një rrjet kolegësh pa pëlqimin e tyre.

Në fokus: Bulizimi në internet

Ndërsa ngacmimi si një fenomen i para daton Internetit, shkalla e shtuar, fushëveprimi dhe vazhdimësia e ngacmimit të kryer në internet mund të përkeqësojë më tej atë që tashmë është një përvojë shqetësuese dhe shpesh e dëmshme për viktimat e tij. Ngacmimi në internet përcaktohet si dëm i qëllimshëm dhe i përsëritur i shkaktuar nga përdorimi i kompjuterëve, telefonave celularë dhe pajisjeve të tjera elektronike. Shpesh zhvillohet paralelisht me ngacmimin jashtë linje që zhvillohet në shkollë ose diku tjetër, ai mund të ketë dimensione shtesë raciste, fetare ose seksiste dhe mund të përbëjë një zgjatim të dëmit të shkaktuar jashtë linje, të tilla si përmes piraterisë së llogarisë, përhapjes së fotove dhe videove në internet dhe natyra 24/7 e mesazheve lënduese dhe disponueshmëria e përmbajtjes. Në përgjithësi, një çështje shoqërore dhe jo penale në natyrë, politikat për të adresuar ngacmimin kibernetik kërkojnë një qasje gjithëpërfshirëse që përfshin vetë shkollat, familjet dhe shumë të rëndësishëm fëmijët.

Në fokus: Ngacmimi online dhe Shantazh

Me përparimet e shpejta në teknologji dhe rritjen e aksesit në Internet dhe komunikimet dixhitale të përjetuara në vitet e fundit, një rrezik i rritur i veprimeve kriminale në internet që synojnë fëmijët ka ndjekur në mënyrë të pashmangshme. Midis këtyre formave të reja të shfrytëzimit seksual të fëmijëve në internet janë pastrimi në internet dhe sextortion i fëmijëve. Grooming online i referohet gjerësisht procesit të miqësimit dhe ndikimit të një të rrituri me një fëmijë (nën moshën 18 vjeç), përmes përdorimit të internetit ose teknologjive të tjera dixhitale, për të lehtësuar ndërveprimin seksual të kontaktit ose jo-kontaktit me atë fëmijë. Përmes procesit të pastrimit, një shkelës i ligjit përpiqet të fitojë pajtueshmërinë e fëmijës për të ruajtur sekretin dhe për të shmangur zbulimin dhe ndëshkimin. Importantshtë e rëndësishme të pranohet se ka edhe raste të abuzimit nga kolegët.

INTERPOL raporton se interneti lehtëson rregullimin e fëmijëve duke pasur një numër të madh të synimeve potenciale lehtësisht të arritshme dhe duke bërë të mundur që dhëndrit të paraqiten në një mënyrë tërheqëse për fëmijën. Shkelësit seksualë të fëmijëve në internet përdorin manipulimin, detyrimin dhe joshjen për të ulur ndalimet dhe për t'i joshur fëmijët të merren me veprimtari seksuale. Ngacmuesi ndërmerr një proces të qëllimshëm të identifikimit të një viktime të mundshme të prekshme, mbledhjen e inteligjencës në mbështetjen e familjes së fëmijës dhe përdor presionin ose turpin / frikën për të abuzuar seksualisht me një fëmijë. Ngacmuesit mund të përdorin pornografinë e të rriturve dhe abuzimin e fëmijëve ose materialin e shfrytëzimit për të disinhibuar synimet e tyre të mundshme, duke paraqitur aktivitetin seksual të fëmijëve si natyral dhe normal. Interneti ka ndryshuar mënyrën në të cilën njerëzit ndërveprojnë dhe ka ripërcaktuar konceptin e 'mikut'. Një pastrues mund të krijojë një miqësi me një fëmijë në internet shumë lehtë dhe shpejt, gjë që detyron një rivlerësim të mesazheve tradicionale të edukimit "rrezik i huaj".

Ruajtja në internet u njoh për herë të parë zyrtarisht në një instrument juridik ndërkombëtar në vitin 2007 nga Konventa e Këshillit të Evropës për Mbrojtjen e Fëmijëve nga Shfrytëzimi Seksual dhe Abuzimi Seksual (Konventa e Lanzarote). Neni 23 penalizon "thirrjen e fëmijëve për qëllime seksuale", që kërkon që të ketë një propozim të qëllimshëm për të takuar fëmijën me qëllim të kryerjes së një vepre seksuale e cila pasohet nga "akte materiale që çojnë në një takim të tillë". Në shumë raste të pastrimit, fëmijët abuzohen dhe shfrytëzohen seksualisht në internet - 'takimi' i kërkuar nga Konventa e Lanzarote dhe shumë ligje ekzistuese kombëtare është plotësisht virtual - por sidoqoftë është po aq i dëmshëm për

fëmijën sa një takim fizik. Crucshtë e rëndësishme që kriminalizimi i pastrimit të shtrihet "në rastet kur abuzimi seksual nuk është rezultat i një takimi personal por është kryer në internet".

Shantazhi mund të ndodhë si një tipar i pastrimit në internet ose si një vepër e pavarur. Ndërsa ngancmimi mund të ndodhë pa procesin e pastrimit në internet, në disa raste pastrimi online mund të çojë në shantazh. Shantazhi mund të ndodhë në kontekstin e pastrimit në internet ndërsa një pastrues manipulon dhe ushtron ndikim mbi fëmijën gjatë procesit të pastrimit përmes kërcënimeve, kërcënimeve dhe detyrimeve për të dërguar imazhe seksuale të vetvetes (përmbajtje të vetë-gjeneruar). Nëse viktima dështon të ofrojë favoret e kërkuara seksuale, imazhe shtesë intime, para ose përfitime të tjera, imazhet e tij ose të saj mund të postohen në internet me qëllim të shkaktimit të poshtërimit ose shqetësimit ose shtrëngimit të fëmijës në gjenerimin e materialit shtesë seksual të qartë. Sextortioni është referuar si "sulm seksual virtual" për shkak të efekteve të ngjashme emocionale dhe psikologjike mbi viktimat. Në disa raste, abuzimi është aq traumatik sa që viktimat janë përpjekur të vetë-dëmtojnë ose të bëjnë vetëvrasje si një mjet për t'i shpëtuar abuzimit.

Europol vuri në dukje se mbledhja e informacionit për të vlerësuar fushën e shantazhit që prek fëmijët është sfiduese dhe mund të raportohet shumë më pak. Për më tepër, mungesa e terminologjisë dhe përkufizimeve të zakonshme për rregullimin dhe shantazhit në internet janë pengesa për mbledhjen e të dhënave të sakta dhe të kuptuarit e fushës së vërtetë të çështjeve në të gjithë botën.

2.6 Fëmijët me aftësi të kufizuara

Fëmijët dhe të rinjtë mund të jenë të prekshëm për një larmi arsyesh të ndryshme. Hulumtimi i kryer në vitin 2019 deklaroi se "jeta dixhitale e fëmijëve të pambrojtur rrallë merr të njëjtën vëmendje të nuancuar dhe të ndjeshme që fatkeqësia e" jetës reale "tenton të tërheqë". Për më tepër, raporti vazhdon të thotë se "në rastin më të mirë ata [fëmijët dhe të rinjtë] marrin të njëjtën këshillë gjenerike për sigurinë në internet si të gjithë fëmijët dhe të rinjtë e tjerë, ndërsa kërkohet ndërhyrja e specialistëve".

Tre shembuj të dobësive specifike janë: fëmijët migrantë, fëmijët me çrregullime të spektrit autik dhe fëmijët me aftësi të kufizuara), por natyrisht ka edhe shumë të tjerë.

Fëmijë migrantë

Fëmijët dhe të rinjtë me prejardhje migrante vijnë shpesh në një vend (ose tashmë jetojnë atje) me një grup të veçantë të përvojave dhe pritjeve socio-kulturore. Ndërsa teknologjia zakonisht mendohet të jetë një lehtësuese për të lidhur dhe marrë pjesë, rreziqet dhe mundësitë në internet mund të ndryshojnë shumë në kontekste. Për më tepër, gjetjet dhe hulumtimet empirike tregojnë një funksion jetësor të mediave dixhitale në përgjithësi:

• është e rëndësishme për orientim (kur udhëtoni në një vend të ri).

• isshtë një funksion qendror për përvetësimin dhe njohjen me shoqërinë / kulturën e vendit pritës.

• Mediat sociale mund të luajnë një rol kryesor në mbajtjen e kontakteve me familjen dhe bashkëmoshatarët, dhe në qasjen në informacione të përgjithshme.

Krahas shumë aspekteve pozitive, media dixhitale mund të sjellë sfida për migrantët duke përfshirë:

• Infrastruktura - është e rëndësishme të mendoni për hapësira të sigurta në internet në mënyrë që fëmijët dhe të rinjtë migrantë të mund të përfitojnë nga privatësia dhe siguria.

• Burimet - migrantët shpenzojnë shumicën e parave të tyre në kartat e parapaguara të telefonit.

• Integrimi - së bashku me aksesin në teknologji, fëmijët dhe të rinjtë migrantë gjithashtu duhet të marrin një arsimim të mirë dixhital.

Fëmijët me Çrregullim të Spektrit të Autizmit (ASD)

Spektri i autizmit përmbledh dy fusha thelbësore në procesin e diagnostikimit të sjelljes DSM-5:

• sjellje e kufizuar dhe e përsëritur ("nevoja për njëllojshmëri");

• vështirësi me sjelljet shoqërore dhe komunikuese;

• bashkë-ndodhje e shpeshtë me paaftësi intelektuale, çështje gjuhësore dhe të ngjashme.

Teknologjia dhe interneti ofrojnë mundësi të pafund për fëmijët dhe të rinjtë kur mësojnë, komunikojnë dhe luajnë. Megjithatë, krahas këtyre përfitimeve ka shumë rreziqe ndaj të cilave fëmijët dhe të rinjtë me ASD mund të jenë më të prekshëm:

• Interneti mund t'u japë fëmijëve dhe të rinjve me autizëm mundësi shoqërimi dhe interesash të veçanta që ata mund të mos kenë në jetën reale.

• Sfidat shoqërore, të tilla si një vështirësi për të kuptuar qëllimet e të tjerëve, mund ta lënë këtë grup të pambrojtur ndaj "miqve" me qëllime të këqija.

• Sfidat në internet shpesh janë të lidhura me karakteristikat thelbësore të autizmit: udhëzime konkrete, specifike mund të përmirësojnë përvojat në internet të individëve, por sfidat themelore mbeten.

Fëmijët me aftësi të kufizuara

Fëmijët me aftësi të kufizuara përballen me rreziqe në internet në të njëjtën mënyrë si fëmijët pa aftësi të kufizuara, por ata gjithashtu mund të përballen me rreziqe specifike të lidhura me aftësitë e tyre.

Fëmijët me aftësi të kufizuara shpesh përballen me përjashtim, stigmatizim dhe pengesa (fizike, ekonomike, shoqërore dhe qëndrimi) për të marrë pjesë në komunitetet e tyre. Këto përvoja mund t'i kontribuojnë një fëmije me aftësi të kufizuara që kërkon ndërveprime shoqërore dhe miqësi në hapësirat në internet, të cilat mund të jenë pozitive, të ndërtojnë vetëvlerësim dhe të krijojnë rrjete mbështetëse. Sidoqoftë, kjo gjithashtu mund t'i vendosë ata në rrezik më të madh për incidente pastrimi, kërkesë në internet dhe / ose ngacmim seksual - hulumtimi tregon se fëmijët që përjetojnë vështirësi jashtë linje dhe ata që preken nga vështirësi psikosociale janë në rrezik të rritur për incidente të tilla.

Në përgjithësi, fëmijët që janë bullizohen jashtë linje ka të ngjarë të bullizohen në internet. Kjo i vendos fëmijët me aftësi të kufizuara në rrezik më të lartë në internet, megjithatë ata kanë një nevojë më të madhe për të qenë në internet. Hulumtimet tregojnë se fëmijët me aftësi të kufizuara kanë më shumë të ngjarë të përjetojnë abuzime të çdo lloji, dhe posaçërisht kanë më shumë gjasa të përjetojnë viktimizim seksual. Viktimizimi mund të përfshijë ngacmimin, ngacmimin, përjashtimin dhe diskriminimin bazuar në paaftësinë aktuale ose të perceptuar të një fëmije, ose në aspektet që lidhen me paaftësinë e tij, siç janë mënyra se si ata sillen ose flasin, pajisjet ose shërbimet që ata përdorin.

Kryerësit e pastrimit, kërkimit në internet dhe / ose ngacmimit seksual ndaj fëmijëve me aftësi të kufizuara mund të përfshijnë jo vetëm shkelësit e ligjit që synojnë fëmijët, por edhe ata që synojnë fëmijët me aftësi të kufizuara. Kundërvajtësit e tillë mund të përfshijnë 'adhurues' - persona të paaftë

për persona të tërhequr seksualisht nga persona me aftësi të kufizuara (më së shpeshti personat e gjymtuar dhe personat që përdorin ndihmat e lëvizjes), disa prej të cilëve madje pretendojnë të jenë me aftësi të kufizuara vetë. Veprimet nga njerëz të tillë mund të përfshijnë shkarkimin e fotove dhe videove të fëmijëve me aftësi të kufizuara (me natyrë të padëmshme) dhe / ose ndarjen e tyre përmes forumeve të dedikuara ose llogarive të mediave sociale. Mjetet e raportimit në forume dhe media sociale shpesh nuk kanë një rrugë të synuar ose të përshtatshme për t'u marrë me veprime të tilla.

Ekzistojnë shqetësime se 'ndarja' (prindërit që ndajnë informacione dhe fotografi të fëmijëve të tyre në internet) mund të shkelin privatësinë e një fëmije, të çojnë në ngacmim, të shkaktojnë siklet ose të sjellin pasoja negative më vonë në jetë32. Prindërit e fëmijëve me aftësi të kufizuara mund të ndajnë një informacion të tillë në kërkim të mbështetjes ose këshillës, duke i vendosur fëmijët me aftësi të kufizuara në rrezik më të lartë për rezultate anësore.

Disa fëmijë me aftësi të kufizuara mund të përballen me vështirësi në përdorim, apo edhe përjashtim nga mjediset në internet për shkak të dizajnit të paarritshëm (p.sh. aplikacione që nuk lejojnë të rritet madhësia e tekstit), mohimit të akomodimeve të kërkuara (p.sh. softuer i lexuesit të ekranit ose kontrolle adaptive të kompjuterit), ose nevoja për mbështetje të përshtatshme (p.sh. trajnimi në mënyrën e përdorimit të pajisjeve, një mbështetje për një në ndërveprimet shoqërore).

Në lidhje me rrezikun e kontratës ose nënshkrimin e termave dhe kushteve, fëmijët me aftësi të kufizuara janë në rrezik më të lartë të pranimit të kushteve ligjore që ndonjëherë as të rriturit nuk mund t'i kuptojnë.

2.7 Perceptimet e fëmijëve për rreziqet në internet

Ekspozimi në të gjithë botën ndaj dhunës, qasja në përmbajtje të papërshtatshme, mallra dhe shërbime; shqetësimet në lidhje me përdorimin e tepruar; çështjet e mbrojtjes së të dhënave dhe privatësisë janë ato rreziqe të theksuara nga fëmijët.

Adoleshentët raportojnë një sërë shqetësimesh në lidhje me angazhimin e tyre me teknologjitë dixhitale. Këto përfshijnë shqetësime të diskutuara zakonisht për sigurinë në internet siç janë frika e bashkëveprimit me të huajt në internet, hyrja në përmbajtje të papërshtatshme ose ekspozimi ndaj malware ose viruseve - ndërsa të tjerët lidhen me besueshmërinë e qasjes së tyre në teknologji; ndërhyrja e prindërve në jetën e tyre 'private' në internet; dhe aftësitë e tyre të shkrim-leximit dixhital.

Kërkimet e BE Kids Online tregojnë se pornografia dhe përmbajtja e dhunshme janë shqetësimet kryesore të fëmijëve në internet në Evropë. Në përgjithësi, djemtë duken më të shqetësuar nga dhuna, ndërsa vajzat janë më të shqetësuara me rreziqet që lidhen me kontaktin. Shqetësimi për rreziqet është më i lartë në mesin e fëmijëve nga vendet 'me përdorim të lartë, me rrezik të lartë'.

Në Amerikën Latine, konsultimet me fëmijë kanë treguar se humbja e privatësisë, dhuna dhe ngacmimi janë shqetësimet kryesore. Fëmijët raportojnë se janë kontaktuar nga njerëz që nuk i njohin - ky është veçanërisht rasti kur luajnë lojëra në internet. Në situata të tilla, strategjia kryesore duket se nuk angazhohet dhe / ose bllokon personin. Vajzat ballafaqohen me ngacmime në rrjetet sociale që në moshë të vogël. Ata arrijnë të lundrojnë vetë në këto forma të dhunës, duke bllokuar përdoruesit dhe duke ndryshuar cilësimet e privatësisë. Ngacmimi vjen nga përdoruesit që ndonjëherë nuk flasin spanjisht, por arrijnë t'u dërgojnë imazhe, të kërkojnë miqësi dhe të komentojnë në postimet e tyre. Disa djem gjithashtu raportojnë se kanë marrë kërkesa të tilla.

Në shumë pjesë të botës, fëmijët kanë një kuptim të mirë të disa prej rreziqeve me të cilat përballen në internet. Hulumtimet kanë treguar se shumica e fëmijëve janë në gjendje të dallojnë ngacmimin në internet nga shaka ose ngacmimet në internet, duke njohur që ngacmimi në internet ka një dimension publik dhe është krijuar për të dëmtuar.

3. Përgatitja për një strategji kombëtare për mbrojtjen e fëmijëve online

Për të zhvilluar një strategji kombëtare për mbrojtjen e fëmijëve online për të promovuar sigurinë online të fëmijëve dhe të rinjve, qeveritë kombëtare dhe institucionet ligjbërëse duhet të identifikojnë praktikën më të mirë dhe të angazhohen palët e interesuara.

Seksionet e mëtejshme nënvizojnë palët e interesuara dhe vepruesit dhe rolet dhe përgjegjësite e tyre në lidhje me mbrojtjen e fëmijëve online.

3.1 Vepruesit dhe palët e interesuara

Ligjbërësit mund të identifikojnë individë, grupe dhe organizata të përshtatshëm të cilët mund të përfaqësojnë palët e interesuara brenda juridiksionit të tyre. Vlerësimi i aktiviteteve te tyre të tanishme, të planifikuara dhe potenciale është i rëndësishëm në çdo koordinim dhe orkestrim kombëtar për strategjitë e mbrotjes online të fëmijëve.

Fëmijët dhe të rinjtë

Nëpër botë fëmijët dhe të rinjtë kanë treguar se mund të përshtaten dhe përdorin teknologjitë e reja me lehtësi të madhe. Interneti po bëhet gjithmonë e më i rëndësishëm në shkolla dhe si arenë ku fëmijët mund të punojnë, luajnë dhe komunikojnë.

Sipas raportit të fundit të ChildFund Alliance, vetëm 18.1% e fëmijëve të intervistuar mendojnë se liderët e vendit të tyre bëjnë përpjekje për t'i mbrojtur. Është e rëndësishme që ligjbërësit të punojnë me fëmijët për këtë problem, që t'i nënkuptojnë se e respektojnë të drejtën e tyre për t'u dëgjuar.

Për të qenë të aftë t'i mbrojnë fëmijët, ligjbërësit duhet të standardizojnë definicionin e fëmijëve në të gjitha dokumentet ligjore. Një fëmijë duhet të definohet si çdo individ nën 18 vjeç. Ky definicion është konsistent me Artikullin 1 të Konventës së të Drejtave të Fëmijëve të Kombeve të Bashkuara, e cila shpjegon se "fëmijë është çdo njeri nën moshën 18 vjeç". Kompanitë nuk duhet të lejohen të trajtojnë si të rritur askënd nën 18 vjeç që është ligjërisht i rritur mjaftueshëm për t'u marrë me procesim të dhënash. Ky definicion i ngushtë nuk justifikohet nga asnjë provë e zhvillimit të fëmijëve. Gjithashtu nënvlerëson të drejtat dhe rrezikon sigurinë e fëmijëve.

Ndërkohë që shume fëmijë mund të duken konfidentë në përdorimin e teknologjisë, shumë prej tyre ndihen të pasigurtë[2] online dhe kanë shumë shqetësime[3] përsa i përket Internetit.

Mungesa e eksperiencës së fëmijëve dhe të rinjve në lidhje me botën e gjerë mund t'i bëjë vulnerabël ndaj një rangu rreziqesh. Ata kanë të drejtën të presin ndihmë dhe mbrojtje. Është gjithashtu e rëndësishme të kujtohet se jo të gjithë fëmijët dhe të rinjtë përballen njëlloj me Internetin dhe teknologjitë e reja. Disa fëmijë me nevoja të veçanta, të shkaktuara nga kufizime fizike ose të tjera, mund të jenë veçanërisht vulnerabël në mjedisin online dhe të kenë nevojë për më tepër mbështetje.

Sondazhet kanë treguar vazhdimisht se çfarë të rriturit mendojnë se fëmijët dhe të rinjtë bëjnë online, dhe çfarë ata bëjnë në të vërtetë mund të jenë shumë ndryshe nga njëra tjetra. Gjysma e fëmijëve të

[2] ChildFund Alliance, "VIOLENCE AGAINST CHILDREN AS EXPLAINED BY CHILDREN," Save Voices Big Dreams, 2019, https:// childfundalliance .org/ zdocs/a 9357061 -749f -4ebf -a1e9 -b1aee81cb216/ SVBD -THE _REPORT -digital .pdf.

[3] Council of Europe, "It's Our World: Children's Views on How to Protect Their Rights in the Digital World," Report on child consultations (Council of Europe, Children's Right Division, October 2017), https:// rm .coe .int/ it -s -our -world -children -s -views -on -how- to -protect -their -rights -in -the -/ 1680765dff.

pyetur thonë se në vendet e tyre të rriturit nuk i dëgjojnë opinionet e tyre për problematikat që kanë rëndësi për ta[4]. Për këtë arsye, është e rëndësishme të sigurohet që të gjehen mekanizmat e duhura që të dëgjohen zërat e fëmijëve dhe të rinjve dhe që eksperiencat e tyre në përdorimin e teknologjisë të merren parasysh.

Prindër, kujdestarë dhe edukatorë

Prindërit, kujdestarët dhe edukatorët shpenzojnë më shumë kohë me fëmijët. Ata duhet të edukohen në shkrim-lexim digjital që të kuptojnë mjedisin online dhe të mund të kujdesen për fëmijët dhe t'u mësojne atyre të mbrojnë veten e tyre.

Institucionet e edukimit kanë një përgjegjësi të veçantë t'i mësojnë fëmijëve të jenë të sigurt online, qoftë kur e përdorin Internetin në shkollë, në shtëpi ose kudo tjetër. Ligjbërësit duhet të përfshijnë njohjen e mirë të instrumenteve digjitale që në moshë të hershme (3 deri 18 vjeç). Kjo do t'i lejojë fëmijët të kujdesen për veten, të dinë të drejtat e tyre, dhe si pasojë të përdorin Internetin si një mundësues njohurish[5].

Ligjbërësit duhet të kujtojnë se prindërit dhe kujdestarët do të jenë pothuajse gjithmonë linja e parë, e fundit dhe më e mira për mbrojtjen dhe mbështetjen e fëmijëve të tyre. Ama kur diskutohet Interneti, ata mund të ndihen pak të humbur. Përsëri, shkollat mund të jenë një kanal i mirë që i vë në dije prindërit dhe kujdestarët për rreziqet si dhe gjithe mundësite e mora që ofrojnë teknologjitë e reja. Megjithatë, shkollat nuk duhet të jenë e vetmja mënyrë për t'i njoftuar prindërit dhe kujdestarët. Është e rëndësishme që të ketë më shumë se nje mënyrë për t'i arritur prindërit dhe kujdestrët, në mënyrë që të arrihen sa më shumë prej tyre. Industria ka një rol të rëndësishëm në mbështetjen e përdoruesve dhe klientëve. Prindërit dhe kujdestarët mund të zgjedhin të menaxhojnë vetë aksesin dhe aktivitetin e femijëve ne Internet, të flasin me ta për përdorimin korrekt të Internetit dhe të teknologjive, të kuptojnë çfarë fëmijët e tyre bëjnë online në mënyrë që bisedat familjare t'i trajtojnë eksperiencat online dhe në jetën reale si një e vetme.

Prindërit dhe kujdestarët duhet të jenë shembuj të mirë për fëmijët e tyre për përdorimin e pajisjeve të tyre dhe sjelljen korrekte në Internet.

Ligjbërësit duhet të kujtojnë se prindërit dhe kujdestarët duhet të konsultohen për të kuptuar pikëpamjet, eksperiencat dhe mirëkuptimin e tyre në mbrojtjen e fëmijëve online.

Si përfundim, ligjbërësit së bashku me institucionet publike mund të zhvillojnë fushata ndergjegjësimi publike, duke përfshirë prindërit, kujdestarët dhe edukatorët. Libraritë publike, qendrat shëndetësore dhe qendrat tregtare mund të mundësojnë salla për prezantimin e sigurisë online dhe informimit për aftësitë digjitale. Kur kjo të implementohet, qeveritë duhet të sigurojnë neutralitet në dhënien e këshillave, të jenë të pastër nga interesat private dhe të mbulojnë një varietet problematikash brenda hapësirave digjitale.

Industria

Industria është një nga palët kryesore të interesuara në ekosistem si sektor që përmban njohuritë teknologjike që duhen adresuar dhe kuptuar nga ligjbërësit. Kështu që është e

[4] ChildFund Alliance, "Violence against children as explained by children."

[5] UNICEF, "Policy Guide on Children and Digital Connectivity" (Policy Lab, Data, Research and Policy, United Nations Children's Fund, June 2018), https://w ww.unicef. org /esa/m edia /3141 /fi le/PolicyLab- Guid e -DigitalConnectivity -Nov .6 .18 -lowres .pdf.

nevojshme që ligjbërësit të përfshijnë industrinë në procesin e krijimit të ligjeve për mbrojtjen e fëmijëve online.

Gjithashtu është e rëndësishme të inkurajohet industria që të inkorporojnë në bizneset e tyre sigurinë në zhvillimin e teknologjive të reja. Sigurisht që kompanitë që po krijojnë ose ofrojnë produkte teknologjike të reja duhet t'i ndihmojnë përdoruesit të kuptojnë si punojnë dhe si t'i përdorin në mënyrë të saktë dhe korrekte.

Industria gjithashtu ka një përgjegjësi të madhe për promovimin e ndërgjegjësimit për axhendën e sigurisë online, sidomos te fëmijët dhe prindërit dhe kujdestarët e tyre, por edhe te publiku i gjerë. Duke i angazhuar në këtë mënyrë, të interesuarit e industrisë do të mësojnë më shumë për problematikat, rreziqet dhe dëmet ndaj të cilave ekspozohen përdoruesit. Me këtë njohuri, industria mund të korrigjojë produkte dhe shërbime ekzistuese, dhe të identifikojë rreziqe në krijim.

Në disa vende po konsiderohet një framework ligjor dhe rregullator që i kërkon kompanive të gjejnë, bllokojnë ose heqin rrezikun ndaj fëmijëve në platforma ose shërbime, dhe të ofrojnë mënyra raportimi dhe akses ndaj mbështetjes.

Komuniteti kërkimor dhe organizatat joqeveritare

Brenda universiteteve dhe komunitetit kërkimor ka një rang akademikësh të cilët kanë një interes profesional dhe njohuri të detajuara në impaktin social dhe teknik të Internetit. Ata janë një burim shumë i besueshëm që ndihmon qeveritë kombëtare dhe ligjbërësit në krijimin e strategjive të bazuara në fakte dhe prova.

Në mënyrë të ngjashme, në komunitetin e organizatave joqeveritare ka një sërë ekspertizash dhe informacionesh që mund të jenë një burim i paçmuar në ofrimin e shërbimeve ndaj fëmijëve, prindërve, kujdestarëve dhe edukuesve për të ndihmuar në promovimin e axhendës së sigurisë online dhe më përgjithësisht, mbrojtjen e interesit publik.

Zbatimi i ligjit

Është një fakt i trishtueshëm që sa e mrekullueshme është teknologjia, po aq ka tërhequr vëmendjen e elementeve kriminale dhe anti-shoqërore. Interneti ka rritur shumë qarkullimin e materialeve të abuzmit seksual të fëmijëve dhe rreziqe të tjera online. Predatorët seksualë kanë përdorur Internetin për të bërë kontaktin fillestar me fëmijët dhe për t'i tërhequr ata në forma shumë të dëmshme të kontaktit, online dhe në jetën reale. Bullizmi dhe forma të tjera ngacmimi mund të dëmtojnë jetët e fëmijëve dhe Interneti ka mundësuar rrugë të reja në të cilat mund të ndodhi.

Për këto arsye, është themelore që komuniteti i zbatimit të ligjit të angazhohet plotësisht në çdo strategji që ndihmon në bërjen e Internetit më të sigurt për fëmijët dhe të rinjtë. Oficerët e zbatimit të ligjit duhet të trajnohen për të bërë investigime në krimet e lidhura me Internetin kundrejt fëmijëve dhe të rinjve. Atyre iu nevojiten njohuritë e duhura teknologjike dhe aksesi në mjetet lehtësuese të investigimit, në mënyrë që të nxjerrin dhe interpretojnë të dhënat e siguruara nga kompjuterat ose Interneti në një kohë të shkurtër.

Veç kësaj, është shumë e rëndësishme që zbatuesit e ligjit të përcaktojnë mekanizma të qarta që iu mundësojnë fëmijëve dhe të rinjve, ose çdo pjesëtari të publikut, raportimin e çdo incidenti ose shqetësimi që mund të kenë për sigurinë online të të rinjve dhe fëmijëve. Shumë vende, për shembull, kanë caktuar linja telefonike që lehtësojnë raportimet e materialeve të abuzmit seksual të fëmijëve dhe mekanizma të ngjashme të dedikuara ekzistojnë për të lehtësuar raportimet e problematikave të tjera, si psh bullizmi. Ligjbërësit duhet të punojnë me Shoqatën Ndërkombëtare të Linjave Telefonike në

Internet (INHOPE), t'i mbështesin në vlerësimin dhe procesimin e raporteve të materialeve të abuzmit seksual të fëmijëve dhe të përfitojnë nga ndihma e INHOPE ndaj organizatave nëpër botë për ngritjen e këtyre linjave telefonike në vendet ku nuk ka. Ligjbërësit duhet të sigurojnë që nuk ka kanale komunikim të hapura mes ligj-zbatuesve dhe palëve të tjera. Zbatuesit e ligjit janë burimi kryesor për kapjen e materialeve të abuzimit seksual të fëmijëve brenda kufijve shtetërorë. Duhet të ngrihet një proces që ekzaminon çdo material në mënyrë që të vërtetohet nëse mund të identifikohen viktima lokale. Në vendet ku kjo nuk është e mundur, materiali duhet t'i kalohet INTERPOLIT që të përfshihet në databazën e ICSE. Duke qenë se është kërcënim global, ligjbërësit duhet të sigurojnë bashkëpunim global midis agjensive të zbatimit të ligjit nëpër botë. Kjo do të pakësonte kohën e proceseve formale dhe lejonte një përgjigje më të shpejtë nga agjentët.

Shërbimet sociale

Në raste kur fëmijët ose të rinjtë janë abuzuar online, për shembull duke pasur një foto të papërshtatshme të tyre online, ata kanë nevojë për suport dhe këshillim të gjatë dhe të specializuar. Janë të nevojshme edhe shërbime dhe praktika rregulluese ndaj autorëve të rinj qe mund të kenë qenë viktima gjithashtu. Profesionistët duhet të jenë të trajnuar që të suportojnë fëmijët në këto raste. Ky suport duhet të jetë si online ashtu dhe në jetën e përditshme.

Shërbimet shëndetësore

Shërbimet shëndetësore të nevojitura pas çdo dhunimi ndaj një fëmije duhet të jenë pjesë e paketave shëndetësore në nivel kombëtar. Institucionet shëndetësore duhet të kryejnë raportime të detyrueshme të abuzimit. Profesionistët shëndetësorë duhet të jenë të pajisur dhe të kenë njohuri në mënyrë që të suportojnë fëmijët në këto raste. Këto paketa shëndetësore duhet të përfshijnë suportin për mirëqenien mendore të tyre.

Ministritë shtetërore

Politikat e Mbrojtjes së Fëmijëve Online mund të bjeri nën juridiksionin e disa Ministrive Shtetërore dhe është i rëndësishëm bashkëpunimi i tyre për një plan të suksesshëm kombëtar. Këto mund të përfshijnë:

- Ministrinë e Punëve të Brendshme

- Ministrinë e Shëndetësisë

- Ministrinë e Arsimit

- Ministrinë e Mbrojtjes

- Agjensi digjitale/ informacioni

- Rregullatorë

Rregullatorët kontribuojnë në rolin e kontrolluesit dhe llogaritarëve në bashkëpunim me institucionet shtetërore. Këtu mund të përfshihet media dhe rregulluesit e mbrojtjes së të dhënave.

Operatorët telefonikë dhe lidhjet Wifi

Operatorët mund të zbulojnë, bllokojnë dhe raportojnë përmbajtjen ilegale brenda lidhjes së tyre dhe të sigurojnë mjete familjare, shërbime dhe konfigurime për përdorimin e prindërve në zgjedhjen e përdorimit të aksesit nga fëmijët e tyre. Është e rëndësishme që ata të sigurojnë që të drejtat e tyre civile dhe privatësia të respektohen.

Të drejtat e fëmijëve

Institucionet e pavarura e të drejtave të njerëzve për fëmijë mund të luajnë rol kryesor në sigurimin e fëmijëve online. Megjithëse detyrat e tyre varjojnë, këto institucione shpesh kanë këto funksione:

- monitorimi i ndikimit të ligjeve, politikave dhe praktikave mbi sigurimin e të drejtave të fëmijëve;

- promovimi i implementimit të standardeve ndërkombëtare të të drejtave njerëzore në nivel kombëtar;

- hetimi i shkeljeve të të drejtave të fëmijëve;

- sigurimi i ekspertizës mbi të drejtat e fëmijëve në gjykatë;

- të sigurojnë që këndvështrimi i fëmijëve ka peshë mbi tema që shtjellojnë të drejtat e tyre, përshirë krijimin e ligjeve dhe politikave të përshtatshme;

- promovimi i mirëkuptimit publik dhe ndërgjegjësimi i të drejtave të fëmijëve; dhe

- sipërmarrja e edukimit dhe trajnimit mbi të drejtat e njeriut.

Është e rëndësishme të përshihet konsultimi direkt me fëmijët duke qenë se është e drejta e tyre nën artikullin 12 të UNCRC. Funksionet këshilluese, investigatore, ndërgjegjësuese dhe edukuese janë të rëndësishme për parandalimin dhe përgjigjen ndaj rrezikut që fëmijët mund të hasin online. Institucione të tilla duhet të zhvillojnë një qasje gjithëpërshirëse drejt forcimit të politikave që drejtojnë mbrojtjen e fëmijëve online, përshirë konsultimin direkt me fëmijët duke qenë se është e drejta e tyre.

Në kohët e sotme, ka pasur raste të juridiksioneve njohëse të agjensive shtetërore me mandat specifik mbi suportin e të drejtave të fëmijëve online, përshirë sigurinë ndaj rreziqeve ose dhunës. Këto agjensi, duhet të asociohen me përpjekjen për të forcuar përgjigjen në nivel kombëtar mbi mbrojtjen e fëmijëve online.

3.2 Përgjigjet ekzistuese për mbrojtjen në internet të fëmijëve

Disa iniciativa janë zhvilluar në mënyrë që të veprojnë në nivele kombëtare dhe ndërkombëtare përballë rritjes së rëndësisë së TIK në jetën e fëmijëve në të gjithë botën dhe rreziqeve të qenësishme për më të rinjtë në shoqëritë tona.

National models

Në nivelin kombëtar, disa legjislacione duhet të theksohen duke mbuluar aspekte të rëndësishme të një kornize gjithëpërfshirëse për Mbrojtjen Online të Fëmijëve. Këto përfshijnë, por nuk kufizohen në:

• Direktiva e Shërbimeve të Mediave Audiovizive (AVMSD) (rishikuar 2018, BE)

• Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave (GDPR) (2018, BE)

Ka pasur zhvillime inovative në përgjigjen rregullatore dhe institucionale të Shteteve anëtare ndaj kërcënimeve për sigurinë dhe mirëqenien e fëmijëve në internet. Nuk ka një mënyrë të vetme për t'iu përgjigjur CSAM, ngacmimit në internet dhe dëmtimeve të tjera që fëmijët hasin në internet, por është e dukshme që ka pasur qasje të reja të provuara në vitet e fundit:

The Age-Appropriate Design Code (2019, UK)

Në fillim të vitit 2019, Zyra e Komisionerëve të Informacionit publikoi propozime për 'kodin e saj të përshtatshëm të moshës' për të mbrojtur më tej fëmijët në internet. Kodi i propozuar përqendronte interesat më të mira të fëmijës, siç përcaktohet në UNCRC, dhe përcakton disa pritje për industrinë.

Këto përfshijnë masa të forta të verifikimit të moshës, shërbimet e vendndodhjes që do të çaktivizohen për fëmijët, për industrinë që të mbledhë dhe të mbajë vetëm sasinë minimale të të dhënave personale të fëmijëve, që produktet të jenë të sigurta sipas modelit dhe shpjegimet të jenë të përshtatshme për moshën dhe të arritshme .

The Harmful Digital Communications Act (reviewed 2017, New Zealand)

Legjislacioni i vitit 2015 e bëri abuzimin në internet një krim specifik dhe përqendrohet në një dëm të gjerë, nga ngacmimi kibernetik te pornografia hakmarrëse. Ai synon të parandalojë, parandalojë dhe pakësojë komunikimin dixhital të dëmshëm, duke e bërë të paligjshme postimin e një komunikimi dixhital me qëllim që të shkaktojë shqetësime serioze emocionale tek dikush tjetër dhe përcakton një seri prej 10 parimesh të komunikimit. Ai i fuqizon përdoruesit të ankohen në një organizatë të pavarur nëse këto parime janë thyer ose aplikojnë për urdhra gjykate kundër autorit ose nikoqirit të komunikimit nëse çështja nuk zgjidhet.

The eSafety Commissioner (2015, Australia)

Komisioneri eSafety është agjencia e parë qeveritare në botë e përkushtuar posaçërisht për sigurinë në internet. Themeluar në vitin 2015, eSafety ka një rol të ligjshëm për të udhëhequr, koordinuar, edukuar dhe këshilluar për çështjet e sigurisë në internet për të siguruar që të gjithë Australianët të kenë përvoja të sigurta, pozitive dhe fuqizuese në internet. eSafety administron skema hetimore që përqendrohen në një sërë dëmesh përfshirë ngacmimin serioz kibernetik të fëmijëve, abuzimin e bazuar në imazhe dhe përmbajtjen e ndaluar. Ai ka fuqinë të hetojë dhe të marrë masa për të adresuar ankesat ose raportet që përfshijnë këto lloj dëmtimesh - përfshirë, në disa raste, fuqinë për të lëshuar njoftime për individë dhe për shërbime online për heqjen e materialit. Krahas kompetencave të tij hetimore, eSafety miraton një tërësi të qasjes së komunitetit, e cila mbështetet në iniciativa dhe ndërhyrje sociale, kulturore dhe teknologjike. Parandalimi, mbrojtja dhe përpjekjet e tij proaktive ofrojnë një qasje gjithëpërfshirëse për sigurinë në internet.

International models

Në nivel ndërkombëtar dhe ndërkombëtar, rekomandime dhe standarde janë lëshuar nga aktorë të ndryshëm. Këto udhëzime bazohen në punën e përpjekjeve të mëposhtme:

Udhëzime në lidhje me zbatimin e Protokollit Opsional të Konventës për të Drejtat e Fëmijëve mbi shitjen e fëmijëve, prostitucionin e fëmijëve dhe pornografinë e fëmijëve.

Udhëzimet e Këshillit të Evropës për të respektuar, mbrojtur dhe përmbushur të drejtat e fëmijës në mjedisin dixhital.

Udhëzimet u drejtohen të gjithë vendeve anëtare të Këshillit të Evropës, me qëllim që të ndihmojnë shtetet anëtare dhe palët e tjera të interesit në përpjekjet e tyre për të miratuar një qasje gjithëpërfshirëse, strategjike në maksimizimin e gamës së plotë të të drejtave të fëmijëve në mjedisin dixhital. Midis shumë temave të mbuluara janë mbrojtja e të dhënave të personave, sigurimi i përmbajtjes miqësore për fëmijë të përshtatur për kapacitetet e tyre në zhvillim, linjat e ndihmës dhe linjat e nxehta, cenueshmëria dhe qëndrueshmëria, si dhe roli dhe përgjegjësitë e ndërmarrjeve të biznesit. Për më tepër, udhëzimet u bëjnë thirrje shteteve që të angazhohen me fëmijë, përfshirë proceset e vendimmarrjes, për të siguruar që politikat kombëtare adresojnë në mënyrë adekuate zhvillimet në mjedisin dixhital. Udhëzimet aktualisht janë në dispozicion në 19 gjuhë. Ata do të shoqërohen nga një version miqësor për fëmijë i dokumentit, si dhe një Manual për politikë-bërësit, i cili do të sigurojë masa konkrete se si të zbatohen udhëzimet.

Council of Europe – Lanzarote Convention

Konventa e Këshillit të Evropës për Mbrojtjen e Fëmijëve nga Shfrytëzimi Seksual dhe Abuzimi Seksual (Konventa e Lanzarote), e cila u kërkon shteteve të ofrojnë një përgjigje holistike ndaj dhunës seksuale ndaj fëmijëve, përmes metodës "4ps": Parandalimi, Mbrojtja, Ndjekja Penale dhe Promovimi i bashkëpunimi ndërkombëtar. Operacioni i Konventës në lidhje me mjedisin dixhital është sqaruar nga Komiteti i Palëve në Konventën për Mbrojtjen e Fëmijëve kundër Shfrytëzimit Seksual dhe Abuzimit Seksual ("Komiteti Lanzarote"), përmes miratimit të një numri dokumentesh. Këto janë: një Opinion mbi imazhet dhe / ose videot e qarta ose sugjeruese seksuale të fëmijëve të krijuara, të ndara dhe të marra nga fëmijët (6 qershor 2019); një Opinion Interpretues mbi zbatueshmërinë e Konventës Lanzarote ndaj veprave seksuale kundër fëmijëve të lehtësuar përmes përdorimit të TIK (12 maj 2017); një Deklaratë në adresat e internetit që reklamon materiale abuzimi seksual të fëmijëve ose imazhe ose ndonjë shkelje tjetër të krijuar në përputhje me Konventën e Lanzarote (16 Qershor 2016); dhe një Opinion mbi Nenin 23 të Konventës së Lanzarote - Kërkimi i fëmijëve për qëllime seksuale përmes teknologjive të informacionit dhe komunikimit (Grooming). Komiteti i Lanzarote kryen monitorim mbi zbatimin e Konventës: raundi i tij i dytë i monitorimit tematik i Komitetit përqendrohet në mbrojtjen e fëmijëve nga shfrytëzimi seksual dhe abuzimi seksual i lehtësuar nga TIK: një raport do të publikohet mbi raundin e monitorimit në vitin 2020. të vitit 2019, ka 46 Shtete Palë në Konventë, përfshirë Tunizinë - shteti i parë jo-anëtar që aderon.

Further Council of Europe guidelines

Standardet dhe mjetet e mëtejshme të Këshillit të Evropës kontribuojnë në një acquis kolektive për një kornizë gjithëpërfshirëse që synon të gjithë palët e interesuara. Konventa e Këshillit të Evropës për Krimin Kibernetik përmban detyrime për Palët për të kriminalizuar një sërë veprash në lidhje me materialin e abuzimit seksual të fëmijëve: aktualisht është ratifikuar nga 64 Shtete Palë. Këshilli i Evropës përqendrohet, ndër të tjera, në fuqizimin e fëmijëve dhe atyre përreth tyre për të lundruar në sferën dixhitale në mënyrë të sigurt. Kjo promovohet përmes mjeteve arsimore, duke përfshirë një Manual për Rishikimin e Librave të Internetit (2017), një Doracak për Edukimin e Qytetarisë Dixhitale (2019) dhe manuale që synojnë prindërit (Prindërimi në epokën dixhitale - Udhëzime prindërore për mbrojtjen në internet të fëmijëve nga shfrytëzimi seksual dhe abuzimi seksual (2017); Qytetaria dixhitale… dhe fëmija juaj - Çfarë duhet të dijë dhe të bëjë çdo prind (2019). Më në fund, Këshilli i Evropës ka ndërmarrë kërkime konsultative me fëmijët në lidhje me të drejtat e tyre në mjedisin dixhital - worldshtë bota jonë : Pikëpamjet e fëmijëve se si të mbrojnë të drejtat e tyre në mjedisin dixhital (2017) dhe zhvilluan disa nga hulumtimet e para konsultative që përqendrohen në përvojat e fëmijëve me aftësi të kufizuara në mjedisin dixhital - Dy klikime përpara dhe një klikim prapa: Raporti për fëmijët me aftësi të kufizuara në mjedisi dixhital (2019).

Child Online Safety Report

Siguria në internet e Fëmijëve: Minimizimi i Rrezikut të Dhunës, Abuzimit dhe Shfrytëzimit Online + Deklarata Universale e Sigurisë në Fëmijë.

Rekomandimet e OECD mbi Mbrojtjen e Fëmijëve Online (2012 / Rishikim 2019-2020) Nisma të tjera kombëtare dhe transnacionale duhet të theksohen më tej si mbështetje e bashkëpunimit ndërkombëtar, si dhe përpjekje kombëtare për të vendosur strategji për mbrojtjen në internet të fëmijëve. Këto janë për shembull:

Baza e të dhënave ndërkombëtare për imazhin e Shfrytëzimit Seksual të Fëmijëve

Menaxhuar nga INTERPOL, baza e të dhënave ndërkombëtare për imazhe të Shfrytëzimit Seksual të Fëmijëve (ICSE DB) është një mjet i fuqishëm inteligjence dhe hetimi që lejon hetuesit e specializuar të ndajnë të dhëna me kolegët në të gjithë botën. I disponueshëm përmes sistemit të sigurt global të komunikimit policor INTERPOL (i njohur si I-247), ICSE DB përdor një softuer të sofistikuar të krahasimit të imazheve për të bërë lidhje midis viktimave, abuzuesve dhe vendeve. ICSE DB u mundëson përdoruesve të certifikuar në vendet anëtare të kenë qasje në bazën e të dhënave në kohë reale - të marrin në pyetje pronat ekzistuese, të ngarkojnë të dhëna të reja, materialin e triazhit dhe të llojit, të dekonfliktojnë, të kryejnë analiza dhe të komunikojnë me ekspertë të tjerë në botë në përgjigje të pyetjeve që lidhen me seksin e fëmijëve hetimet e shfrytëzimit.

The WePROTECT Global Alliance

Aleanca Globale WePROTECT (WPGA) është një lëvizje globale që bashkon ndikimin, ekspertizën dhe burimet e kërkuara për të transformuar mënyrën se si trajtohet shfrytëzimi seksual i fëmijëve online (OSBE) në të gjithë botën. Shtë një partneritet i qeverive, kompanive globale të teknologjisë dhe organizatave të shoqërisë civile. Natyra e tij me shumë aktorë është unike në këtë fushë. Vizioni i Aleancës Globale WePROTECT është identifikimi dhe mbrojtja e më shumë viktimave, kapja e më shumë autorëve dhe përfundimi i shfrytëzimit seksual të fëmijëve në internet. Aleanca Globale e WeProtect përbëhet nga një numër përbërësish, specifikisht një Model i Përgjigjes Kombëtare dhe një Përgjigje Strategjike Globale. Detaje të mëtejshme mund të gjenden në Shtojcën 3.

The 2020 Child Online Safety Index

Indeksi i Sigurisë Online të Fëmijëve DQ Institute 2020 (COSI) është platforma e parë analitike në kohë reale për të ndihmuar kombet të monitorojnë më mirë statusin e sigurisë në internet të fëmijëve të tyre.

COSI bazohet në gjashtë shtylla që formojnë kornizën COSI. Shtyllat një dhe dy, Rreziqet Kibernetike dhe Përdorimi i Disiplinuar Dixhital, lidhen me përdorimin e mençur të teknologjisë dixhitale. Shtyllat tre dhe katër, Kompetenca dhe udhëzimi dixhital dhe edukimi, kanë të bëjnë me fuqizimin. Dy shtyllat e fundit kanë të bëjnë me infrastrukturën, këto janë shtyllat e Infrastrukturës Sociale dhe Lidhshmërisë.

3.3 Shembuj të përgjigjeve ndaj dëmeve në internet

Ekzistojnë një numër shembujsh të përgjigjeve ndaj dëmeve në internet në Shtojcën 4. Këto shembuj përfshijnë përgjigjet arsimore, legjislative dhe identifikimin e dëmeve në internet.

3.4 Përfitimet e një strategjie kombëtare për mbrojtjen e fëmijëve online

Harmonizimi i ligjeve

Miratimi nga të gjitha vëndet i nje legjislacioni të duhur kundër keqpërdorimit të ICTs për qëllime kriminale është thelbësore për arritjen e sigurisë globale kibernetike. Meqënëse këto kërcënime mund të ndodhinl kudo përreth globit, sfidat janë në thelb të tyre me karakter ndërkombëtar dhe si të tilla kërkojnë bashkëpunim ndërkombëtar, ndihmë hetimore dhe dispozita të përbashkëta materiale dhe procedurale. Kështu që është e rëndësishme që vendet të harmonizojnë kuadrot e tyre ligjore për të

luftuar krimin kibernetik, për të mbrojtur fëmijët në internet dhe për të lehtësuar bashkëpunimin ndërkombëtar[6].

Zhvillimi i një legjislacioni të përshtatshëm kombëtar dhe i një kuadri ligjor të lidhur me krimin kibernetik apo harmonizimi në nivel ndërkombëtar është një hap kryesor drejt suksesit të cdo strategjie kombëtare për mbrojtjen e fëmijëve në internet. Kjo kërkon në rradhë të parë krijimin e disa dispozitave të domosdoshme të ligjit penal, me qëllim penalizimin e veprimeve të tilla si mashtrimi kompjuterik, akseset e paligjshme, ndërhyrjet në të dhëna, shkeljet e së drejtës së autorit dhe CSAM, ndërsa gjithashtu duhet pasur kujdes për mos kriminalizimin e fëmijëve padrejtësisht. Ekzistenca e dia dispozitave në kodin penal që janë të zbatueshme për veprime të ngjashme të kryera në jetën e përditshme nuk nenkupton zbatimin e tyre dhe në rastet e ndodhura online. Prandaj, është thelbësore një analizë e plotë e ligjeve aktuale kombëtare në mënyrë që të identifikohet cdo boshllëk i mundshëm në këto dispozita. Hapi tjetër do të qe identifikimi dhe përcaktimi i gjuhës legjislative si dhe materialit referues që mund të ndihmojë vendet në krijimin e ligjeve të harmonizuara të krimit kibernetik dhe të rregullave procedurale. Instrumente të tillë praktikë mund të përdoren nga vëndet me qëllime përpunimin e një krize ligjore të sigurisë kibernetike apo të ligjeve të ngjashme me to. ITU në bashkëpunim me Shtetet Anëtare dhe palët e interesuara, është duke punuar në këtë drejtim dhe po kontribuon shumë në avancimin e harmonizimit global të ligjeve të krimit kibernetik.

Nëse marrim në konsideratë rritjen e shpejtë të inovacionit teknologjik, vetërregullimi dhe bashkë-rregullimi janë paraqitur si zgjidhje të mundshme për eleminimin e rregullores ekzistuese dhe për zhvillimin e procesit legjislativ. Sidoqoftë, për të qenë efektiv, rregullatorët (politikë-bërësit) duhet të përcaktojnë qartë objektivat dhe sfidat në këtë fushë lidhur me mbrojtjen e fëmijëve, duke vendosur kështu një proces të qartë rishikimi dhe një metodologji për vlerësimin e efektivitetit të proceseve të vetërregullimit dhe bashkë-rregullimit. Duke qënë se bashkërregullimi nuk arrin të adresojë sfidat e identifikuara, kështillohet fillimi i një procesi zyrtar legjislativ për adrsimin e këtyre sfidave. Suksesi i arritur nga këto masa vetërregulluese mund të sjellë miratimin e tyre në ligjin zyrtar brënda procesit legjislativ, duke u bërë në këtë mënyrë një prapavijë ligjore për të parandaluar anulimin ose përfundimin e aderimit në disa nga këto iniciativa .

Koordinimi

Në të gjithë rrethin e aktorëve dhe palëve të interesuara ekzistojnë një sërë aktivitetesh dhe veprimesh të cilat kanë si qëllim mbrojtjen e fëmijëve në internet, por që të gjitha këto gjatë gjithë kësaj kohe kanë ndodhur në izolim. Të kuptuarit e tyre është i rëndësishëm në vlerësimin e përpjekjeve në zhvillimin e strategjisë kombëtare të mbrojtjes së fëmijëve. Strategjia synon të koordinoj dhe të drejtoj përpjekjet përmes orkestrimit të aktiviteteve ekzistuese dhe atyre të reja.

[6] Broadband Commission for Sustainable Development (2019)

4. Rekomandimet për kuadrot dhe implementimin

Qeveritë duhet të adresojnë të gjitha situatat që tregojnë shfaqjen e dhunës ndaj fëmijëve në mjedisin digjital. E megjithatë, masat e marra për të mbrojtur fëmijët në mjedisin digjital nuk duhet të kufizojnë padrejtësisht ushtrimin e të drejtave të tjera si; e drejta e shprehjes, e drejta për të pasur akses në informacion ose e drejta për lirinë e asocimit. Në vend që të kufizojë kuriozitetin që vjen natyrshëm nga fëmijët dhe ndjenjën e inovacionit nga frika e përballjes me rreziqet në internet, është i rëndësishëm shfrytëzimi i shkathtësive të fëmijëve dhe rritja e qëndrueshmerisë së tyre ndërsa eksplorohet potenciali i mjedisit digjital.

Në shumë raste vërehet se aktet e dhunës ndaj fëmijëve kryhen nga vetë fëmijë të tjerë. Në situata të tilla qeveritë duhet të ndjekin sa më shumë të jetë e mundur qasjet restauruese të cilat kanë për qëllim riparimin e dëmeve të bëra, duke paralizuar kështu kriminalizimin e fëmijëve. Qeveritë duhet të promovojnë përdorimin e ICTs në parandalimin dhe adresimin e dhunës, të tilla sic janë zhvillimi i teknologjive dhe burimeve, që fëmijët të kenë informacion për të bllokuar materiale të dëmshme dhe të jenë në gjëndje për të raportuar raste dhune kur ato janë të pranishme.[7].

Për të përballuar këtë situatë globale që lidhet me sigurinë në internet të fëmijëve, qeveritë duhet të lehtësojnë komunikimin midis etniteteve të tjera përkatëse dhe të bashkëpunojnë hapur për të eleminuar dëmtimin e fëmijëve në internet.

4.1 Kuadret e rekomanduara

4.1.1 Kuadri ligjor

Kur është e nevojshme, qeveritë duhet të rishikojnë dhe të azhornojnë kuadrin ligjore të saj, duke u mbështetur në plotësimin e të drejtave të fëmijëve në mjedisin digjital. Një kornizë gjithëpërfshirëse ligjore duhet të bëjë të mundur adresimin e masave parandaluese si mund të jetë ndalimi i të gjitha formave të dhunës ndaj fëmijëve në mjedisin digjital, sigurimi i mjeteve juridike efektive, rikuperimi dhe riintegrimi për të adresuar shkeljet e të drejtave të fëmijëve, vendosja e mekanizmave të këshillimit dhe raportimit të ankesave të fëmijëve si dhe mekanizmave përgjegjëse për të luftuar pandëshkueshmërinë[8].

Kurdoherë që është e mundur, legjislacioni duhet të jetë neutral ndaj teknologjisë, në mënyrë që zbatueshmëria e tij të mos të cënohet nga zhvillimet e ardhshme të saj[9].

Zbatimi efektiv i legjislacionit kërkon vendosjen e disa masave plotësuese nga qeveritë, duke marrë në konsideratë gjithashtu përfshirjen e ndërgjegjësimit dhe iniciativave të mobilizimit social, përpjekjet dhe fushatat arsimore, si dhe ndërtimin e kapaciteteve të profesionistëve qe punojne me dhe për fëmijët.

Gjatë zhvillimit të një ligji të përshtatshëm, është e rëndësishme të kuptohet se fëmijët nuk janë një grup homogjen. Duke pasur një situatë të tillë duhet të kërkohen përgjigje të ndryshme për fëmijë të

[7] Special Representative of the Secretary-General on Violence against Children, *Annual Report of the Special Representative of the Secretary-General on Violence against Children to the Human Rights Council,* A/ HRC/31/20 (January 2016), para. 103 and 104.

[8] Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), p. 55.

[9] Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), p. 64.

moshave të ndryshme si dhe për fëmijët me nevoja specifike të cilët rrezikojnë të dëmtohen përmes mjedisit digjital të krijuar.

Qeveritë duhet të krijojnë një mjedis të qartë dhe të parashikueshëm ligjor dhe rregullator i cili ka si synim të mbështes bizneset dhe palët e tjera të treta, për të përmbushur përgjegjësitë e tyre lidhur me mbrojtjen e këtyre të drejtave përgjatë gjithë veprimtarisë së tyre, brenda dhe jashtë vëndit[10].

Aspektet e mëposhtme do të ishin të rëndësishme për politikë-bërësit në rishikimin e fushës së cdo kuadri ligjor lidhur me parashikimet e mëposhtme :

- Manipulimi seksual ose forma të tjera online të joshjes dhe detyrimit të fëmijëve drejt kontaktit ose aktivitetit të papërshtatshëm seksual.
- Arritja e zotërimit, prodhimit dhe shpërndarjes së CSAM, pavarësisht nga qëllimi për të shpërndarë;
- ngacmimi, bullizmi, abuzimi ose gjuha e urrejtjes në internet;
- materiale terroriste në internet;
- Siguria kibernetike;
- reflektimi se çfarë është e paligjshme offline është po aq e paligjshme në botën e Internetit

4.1.2 Kuadri politik dhe institucional

Garancia e realizimit të të drejtave të fëmijëve në mjedisin digjital kërkon nga qeveritë që të vendosin një ekujlibër midis maksimizimit të përfitimeve nga përdorimi i ICTs nga fëmijët dhe minimizimit të rreziqeve që lidhen me to. Kjo mund të arrihet vetëm duke përfshirë në planet kombëtare masat për mbrojtjen e fëmijëve nga interneti[11], si dhe duke zhvilluar strategji të vecanta shumëpalëshe për mbrojtjen e tyre online. Një axhendë e tillë duhet të jetë plotësisht e integruar me cdo kuadër ekzistues të politikave në lidhje me të drejtat e fëmijëve apo mbrojtjen e tyre, si dhe duhet të plotësojë politikat kombëtare të mbrojtjes së fëmijëve duke ofruar një kuadër specifik për të gjitha rreziqet dhe dëmet e mundshme për ta, duke synuar kështu krijimin e një mjedisi të sigurt dhe gjithëpërfshirës digjital[12].

Qeveritë duhet të vendosin një kuadër koordinues kombëtar me një mandat të qartë dhe autoritet të mjaftueshëm për të koordinuar të gjitha aktivitetet që lidhen me të drejtat e fëmijëve , median digjitale dhe ICTs në nivele ndër-sektoriale, kombëtare, rajonale dhe lokale. Ato duhet të vendosin qëllime eficente në kohë dhe një proces transparent për vlerësimin dhe monitorimin e procesit. Eshtë i rëndësishëm sigurimi i burimeve të nevojshme njerëzore, teknike dhe financiare dhe vendosja e tyre në dispozicion të funksionimit efektiv të kësaj politike[13].

Qeveritë duhet të krijojnë një platformë me shumë aktorë për të drejtuar zhvillimin, zbatimin dhe monitorimin e agjendës digjitale kombëtare për fëmijët. Një platformë e tillë duhet të mbledhë së bashku përfaqësues të grupeve të ndryshme si fëmijët, të rinjtë, shoqatat e prindërve/kujdestarëve, sektorët përkatës të qeverisë si ajo e arsimit,drejtësisë, shëndetësisë, kujdesit shoqëror, institucionet

[10] UN Committee on the Rights of the Child, *General Comment No. 16*, para. 53.

[11] The State of the Broadband 2019, Recommendation 5.6, page 78. https:// www .itu .int/ dms _pub/ itu -s/ opb/ pol/ S -POL -BROADBAND .20 -2019 -PDF -E .pdf.

[12] For model provisions on child protection for national broadband plans see chapter 10 of the Child Online Safety Report.

[13] Special Representative of the Secretary-General on Violence against Children, *Annual Report of the Special Representative of the Secretary-General on Violence against Children* (December 2014) A/HRC/28/55 and *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), para. 88.

kombëtare të të drejtave të njeriut dhe organet përkatëse rregullatore si industria, akademia dhe shoqatat përkatëse profesionale.

4.1.3 Kuadri rregullator

Qeveritë janë përgjegjëse për shkeljen e të drejtave të fëmijëve të shkaktuara apo të kontribuara nga ndërmarrjet e biznesit ku nuk është arritur marrja e masave të nevojshme dhe të përshtatshme për të parandaluar apo korrigjuar shkelje të tilla, duke bashkëpunuar në këtë mënyrë me këto shkelje ose duke i toleruar ato[14].

Guiding Principles on Business and Human Rights parashikon që koorporatat duhet të sigurojnë mekanizma përmirësues që janë të arritshme legjitimisht , të barabarta, të pajtueshme me të drejtat dhe të bazuara në dialog dhe angazhim duke u kthyer ne një burim të vazhdueshëm të të mësuarit të vazhdueshëm. Këto mekanizma për ankesat, të krijuara nga ndërrmarjet e biznesit mund të ofrojnë zgjidhje alternative fleksible në kohë dhe ndonjëherë mund të qëndrojnë në interesin e mirë të një fëmijë për shqetësimet e ngritura duke ndryshuar sjelljet e kompanive lidhur me vetëpërmirësimin e tyre. Në të gjitha rastet duhet të jetë i disponueshëm rishikimi gjygjësor i mjeteve juridike, administrative dhe procedurave të tjera[15]. Duhen marrë në konsideratë mekanizma të tillë që krijojnë shërbime të sigurta, të përshtatshme për moshën e fëmijëve dhe ku përdoruesit të mund të raportojnë shqetësimet e tyre.

Pavarësisht nga ekzistenca e mekanizmave të brendshëm për paraqitjen e këtyre ankesave, qeveritë duhet të krijojnë mekanizma monitorimi për hetimin dhe korrigjimin e shkeljeve të të drejtave të fëmijëve, me qëllim përmirësimin e përgjegjësisë së ICT dhe kompanive të tjera përkatëse si dhe forcimin e përgjegjësisë së agjensive rregullatore për zhvillimin e standarteve të rëndësishme për të drejtat e fëmijëve dhe ICTs[16]. Kjo është vecanërisht e rëndësishme sepse mjetet juridike të tjera në dispozicion të atyre që preken nga veprimi i koorporatave – të tilla si procedurat civile dhe dëmshpërblimet e tjera gjyqësore, janë shpesh të vështira dhe të kushtueshme[17].

UN Committee on the Rights of the Child ka theksuar potencialin që kanë institucionet kombëtare të të drejtave të njeriut në këtë fushë, duke përshkruar se si ata mund të kenë rolin e marrjes, hetimit dhe ndërmjetësimit të ankesave të shkeljeve nga njësitë e industrisë; kryerjen e hetimeve publike për abuzimet në shkallë të gjerë dhe ndërmarrjen e rishikimeve legjislative për të siguruar përputhshmërinë me Konventen për të Drejtat e Fëmijëve. Komiteti ka treguar që, kur është e nevojshme, "Shtetet duhet të zgjerojnë mandatin legjislativ të institucioneve kombëtare të të drejtave të njeriut për të akomodur të drejtat e biznesit dhe të fëmijëve". Eshtë e rëndësishme që cdo mekanizëm në të cilin paraqiten ankesat, të ketë ndjeshmërinë ndaj fëmijëve duke siguruar privatësinë dhe mbrojtjen e ''viktimave'' . Kjo realizohet duke ndërrmarrë aktivitete monitorimi ndjekjeje dhe verifikimi për fëmijët e dëmtuar nga mjedisi digjital.

Një shembull i një fushe në të cilën një institucion kombëtar i të drejtave të njeriut ose një organ tjetër rregullator mund të sigurojë një zgjidhje efektive për fëmijët janë rastet e bullizmit në internet. Mekanizmat e brendshëm të korrigjimit ndonjëherë nuk janë efektivë sepse edhe në rastet kur përmbajtja është shqetësuese apo e dëmshme, ajo nuk adresohet nga legjislacioni kombëtar dhe nuk ka një bazë të qartë për të kërkuar largimin e saj nga përmbajtja. Fuqizimi i nje autoriteti publik, duke i

[14] UN Committee on the Rights of the Child, *General Comment No.* 16, para. 28.

[15] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, A/HRC/17/31 (2011), para. 71.

[16] UN Committee on the Rights of the Child, *Report of the 2014 Day of General Discussion*, para. 96.

[17] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (2016), para. 71.

dhënë atij autoritetin për të marrë ankesa në lidhje me rastet e bullizimit dhe për të kryer ndërmjetësimin me mbajtësit e përmbajtjes për ta hequr atë do të ishte një mbrojtje e rëndësihme për fëmijët[18]. Kjo do të kishte avantazhet e sigurimit të një përgjigjeje të shpejtë, e cila është e një rëndësie thelbësore në kontekstin e bullizmit në internet dhe gjithashtu do të funksiononte si një bazë e qartë ligjore për adresimin e heqjes së materialit nga mjedisi digjital.

Sa i takon qasjes së qeverive në rregullimin e mjedisit digjital, ato duhet të kenë njohuri për ndikimin e një rregulloreje të tillë e cila do të sillte zbatimin e të gjitha të drejtave të njeriut përfshirë dhe lirinë e shprehjes[19].

Qeveritë duhet të vendosin një detyrim mbi bizneset duke i ndërgjegjësuar mbi kujdesin që duhet të tregojnë për të drejtat e fëmijëve. Kjo do t'u siguronte ndërrmarjeve të biznesit parandalimin dhe zbutjen e ndikimit të tyre në këto të drejta përfshirë dhe marrëdheniet e tyre të biznesit[20].

Përvec kesaj, qeveritë duhet të marrin në konsideratë masa plotësuese të tilla si sigurimi i njësive të industrisë, aktivitetet e së cilës mund të kenë një ndikim në të drejtat e fëmijëve në mjedisin digjital, që duhet të jenë në perputhje me standartet më të larta në drejtim të parandalimit dhe reagimit ndaj shkeljeve të mundshme të të drejtave.

4.2 Rekomandimet për implementimin

Qeveritë duhet të sigurojnë aksesin e mjeteve efektive për fëmijët e prekur nga sulmet në internet, përfshirë dhe kërkesën e dëmshpërblimit të shpejtë dhe të nevojshme për dëmin e pësuar, në rastet kur është i nevojshëm. Ato duhet të sigurojnë gjithashtu mbështetjen dhe ndihmën e duhur për fëmijët e prekur nga shkeljet të cilat lidhen me mediat digjitale dhe ICTs, duke siguruar shërbime gjithëpërfshirëse për rikuperimin dhe riintegrimin e plotë të fëmijës dhe parandalimin e riviktimizimit të këtyre fëmijëve të prekur më parë[21].

Mekanizmat e këshillimit, raportimit dhe ankesave duhet të jenë të sigurta, lehtësisht të arritshme dhe duhet të jenë pjesë e sistemit kombëtar të mbrojtjes së fëmijëve. Sigurimi i këtyre shërbimeve të lidhura me funksionin rregullator është e rëndësishme për të ndihmuar në thjeshtëzimin e ndërveprimit të fëmijëve me organet institucionale gjatë një kohe ku ata mund të kenë përjetuar shqetësime. Linjat ndihmëse janë vecanërisht të vlefshme në lidhje me cështje shumë të rëndësishme si për shembull abuzimi seksual, diskutimi i të cilave paraqet vështirësi nga fëmijët sa i takon bashkëmoshatarëve, prindërve, kujdestarëve, ose mësuesve. Këto linja ndihmëse luajnë një rol vendimtar në qasjen e fëmijëve drejt shërbimeve të tilla si shërbimet ligjore, shtëpitë e sigurta, zbatimin e ligjit ose rehabilitimit[22].

Qeveritë duhet të jenë në gjendje të identifikojnë dhe të ndjekin sjelljet e këtyre shkelësve për të rritur shkallën e zbulimit të abuzuesve dhe për të zvogëluar rrezikun e abuzuesve për të rivepruar. Krijimi i linjave ndihmëse të cilat ofrojnë ndihmë falas, këshillime anonime apo mbeshtetje të bazuara në biseda të cilat provokojnë ndjesi ose mendime me interes seksual te fëmijët mund të kthehen në shkelës të

[18] Bertrand de Crombrugghe, "Report of the Human Rights Council on Its Thirty-First Session" (UN Human Rights Council, 2016).

[19] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (2016), para. 45.

[20] UN Committee on the Rights of the Child, *General Comment No. 16*, para. 62.

[21] UN Committee on the Rights of the Child, *Report of the 2014 Day of General Discussion*, para. 106.

[22] Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks*, p. 51 and p. 65.

mundshëm. Të ndihmuarit e personave shkelës për të ndryshuar sjelljen e tyre mund të minimizojë rrezikun e shkeljes së ligjit.

Mekanizmat statike të trajtimit të ankesave gjithashtu përbëjnë një pjesë thelbësore të kuadrit juridik efektiv.

Këto mekanizma të cilat funksionojnë si rregullatorë duhet të kryejnë matje dhe studime të pavarura për të vlerësuar sesi platëformat ekzistuese raportojnë apo trajtojnë ceshtjet në lidhje me mbrojtjen e fëmijëve. Ekzistenca e teknologjisë i lejon këto mekanizma të realizojnë një monitorim në mënyrë të pavarur.

Qeveritë, së bashku me bashkësinë ndërkombëtare dhe industrinë duhet të zhvillojnë një grup universal matjeje, në mënyrë që palët e interesuara të mund t'i përdorin për të gjitha aspektet e rëndësishme të sigurisë në internet lidhur me fëmijët.

4.2.1 Shfrytëzimi seksual

- Konsiderata konkrete për politikë-bërësit kur marrin në konsideratë kërcënimet për dëmtime ndaj fëmijëve, posaçërisht materialin e abuzimit seksual të fëmijëve, përmbajtjen e vetë-gjeneruar, rregullimin dhe shfrytëzimit nëpërmjet materiale seksuale dhe rreziqeve të tjera në internet. Këto mund të përfshijnë:
- Hapat për të ndërprerë ose zvogëluar trafikun në CSAM, për shembull duke krijuar një linjë telefonike kombëtare ose një Portal Raportues të IWF dhe duke vendosur masa që do të bllokojnë qasjen në përmbajtjen në internet që dihet se përmban ose reklamon disponueshmërinë e CSAM.
- Sigurimi që ekzistojnë procese kombëtare për të siguruar që të gjitha CSAM të gjetura në një vend të kanalizohen drejt një burimi kombëtar të centralizuar, që ka kompetenca legjislative për të drejtuar kompanitë të heqin përmbajtjen.
- Strategjitë për të adresuar kërkesën për CSAM veçanërisht midis atyre që kanë dënime për vepra të tilla. eshtë e rëndësishme të kihet kujdes për faktin se ky nuk është një krim pa viktima: fëmijët abuzohen për të prodhuar materialin që shihet dhe shohin ose shkarkojnë me qëllim CSAM, dikush kontribuon drejtpërdrejt në abuzimin e fëmijës dhe një gjithashtu inkurajon abuzimin e më shumë fëmijëve për të prodhuar më shumë fotografi.
- Ndërtimi i kujdesit për faktin se fëmijët nuk mund të pranojnë kurrë që të abuzohen seksualisht, qoftë për prodhimin e CSAM apo në ndonjë mënyrë tjetër. Inkurajoni njerëzit që përdorin CSAM për të kërkuar ndihmë, e kështu në të njëjtën kohë, i bëni të vetëdijshëm se ata do të konsiderohen si përgjegjës për veprimtaritë e paligjshme në të cilën ata angazhohen/merren.
- Strategji të tjera për të adresuar kërkesën për CSAM. Për shembull, disa vende mbajnë një regjistër të shkelësve seksualë të dënuar. Gjykatat kanë lëshuar urdhra gjykate që ndalojnë shkelësit e tillë të përdorin internetin plotësisht ose të përdorin pjesë të internetit që frekuentohen nga fëmijë dhe të rinj. Problemi me këto urdhra deri më tani ka qenë zbatimi. Sidoqoftë, në disa vende, po merret parasysh integrimi i listës së shkelësve seksualë që vizitojnë ose bashkohen në uebfaqe të caktuara, për shembull faqet e internetit që dihen që vizitohen nga një numër i madh fëmijësh dhe të rinjsh. Sigurisht, nëse kryesi i veprës hyn në një faqe në internet duke përdorur një emër tjetër ose log-in të rremë, efektiviteti i masave të tilla mund të reduktohet shumë, por duke kriminalizuar këtë sjellje mund të krijohet një pengesë e mëtejshme.
- Sigurimi i mbështetjes së duhur afatgjatë për viktimat. Kur fëmijët ose të rinjtë bërë viktima në internet, ku për shembull një imazh i paligjshëm i tyre është publikuar në Internet, ata natyrisht do të ndihen shumë të shqetësuar për faktin se kush mund ta ketë parë atë dhe çfarë ndikimi do të ketë kjo mbi ta. Kjo mund ti bëjë fëmijët ose të rinjtë të ndjehen të dobët ndaj ngacmimeve ose shfrytëzimit të mëtejshëm seksual dhe abuzimit. Në këtë kontekst do të ishte e rëndësishme

që të ketë shërbime profesionale mbështetëse në dispozicion të mbështetjes së fëmijëve dhe të rinjtë që gjenden në këto rrethana. Një mbështetje e tillë mund të jetë e nevojshme të ofrohet në baza afatgjata.

- Sigurimi që një mekanizëm është krijuar dhe promovohet gjerësisht për të siguruar një mjet të kuptueshëm dhe të shpejtë për raportimin e përmbajtjes së paligjshme ose sjelljes së paligjshme ose shqetësuese në internet, p.sh. një sistem i ngjashëm me atë që është krijuar nga Task Forca Virtuale Globale dhe INHOPE. Duhet të inkurajohet përdorimi i sistemit INTERPOL i24 / 7.

- Sigurimi që një numër i mjaftueshëm i zyrtarëve të zbatimit të ligjit janë trajnuar në mënyrë të përshtatshme për hetimin e krimeve në Internet dhe krimeve të kompjuterizuara dhe të kenë qasje në pajisjet/lehtësirat e duhura mjeko-ligjore për t'i mundësuar atyre nxjerrjen dhe interpretimin e të dhënave përkatëse dixhitale.

- Investimi në trajnime për autoritetet e zbatimit të ligjit, prokurorisë dhe gjykatave në metodat e përdorura nga kriminelët në internet për të kryer këto krime. Investimi do të jetë gjithashtu i nevojshëm në blerjen dhe mirëmbajtjen e lehtësive të nevojshme për të marrë dhe interpretuar provat mjeko-ligjore nga pajisjet dixhitale. Për më tepër, do të jetë e rëndësishme të vendoset bashkëpunim dypalësh dhe shumëpalësh dhe shkëmbime informacioni me autoritetet përkatëse të zbatimit të ligjit dhe organet hetimore në vendet e tjera.

4.2.2 Edukimi

Thelbësor është edukimi i fëmijëve mbi njohurinë digjitale, si pjesë e një strategjie për t'u siguruar atyre përdorimin e kësaj teknologjie pa u dëmtuar. Kjo do t'u lejonte fëmijëve të zhvillonin aftësi të të menduarit kritik, gjë e cila do t'i ndihmonte në identifikimin e anëve pozitive dhe negative të lundrimit të tyre në hapësirën digjitale. Duke marrë në konsideratë rëndësinë që ka për fëmijët ilustrimi me shembuj konkret i aspekteve negative që lundrimi në internet ka, duhet të kuptojmë se kjo do të kishte efektivitet vetëm në rastet e hartimit të disa programeve specifike lidhur me njohurinë digjitale, e cila do të ishte e përshtatshme për moshën e tyre dhe do të kishte në fokus aftësimin dhe përqëndrimin e tyre. Rëndësi të vecantë paraqesin mësime të koncepteve të tilla si ato sociale apo emocionale mbi sigurinë në internet, pasi kjo do të sillte të kuptuarit dhe të menaxhuarit e emocioneve, për të pasur në këtë mënyrë marrëdhënie të shëndetshme si në internet ashtu edhe në marrëdhëniet e përditshme

Mënyra më e mirë për të mbajtur fëmijët e sigurtë gjatë lundrimit në internet është pajisja e tyre me mjetet dhe informacionet e duhura lidhur me këtë mjedis. Përfshirja e njohurive digjitale në programet mësimore është njëra mënyrë. Mënyra tjetër është krijimi i burimeve edukative jashtë kurrikulës shkollore.

Individët të cilët punojnë me fëmijët duhet të kenë njohuritë dhe aftësitë e përshtatshme për t'i mbështetur ata me përgjigjet lidhur me mbrojtjen online, apo zgjidhjen e cështjeve të ndryshme që lidhen me mbrojtjen e tyre në internet. Një rast tjetër mund të jetë ajo e pajisjes së fëmijëve me nevoja të vecanta, me njohuritë e duhura digjitale për të nxjerrë përfitim prej tyre.

4.2.3 Industria

Industritë kombëtare dhe ndërkombëtare duhet të zgjojnë ndjeshmërinë e tyre lidhur me cështjet që lidhen me sigurinë e fëmijëve në internet dhe të ndihmojnë të rriturit të cilët janë përgjegjës për mirëqenien e një fëmije si; prindërit, kujdestarët, shkollat, komunitetet apo organizatat për të rinjtë te zhvillojne njohuritë dhe aftësitë e tyre për t'i mbajtur fëmijët e sigurt. Këto industri duhet të kenë një

qasje shumë më të sigurt sa i takon produkteve, shërbimeve apo platformave të tyre, duke vendosur sigurinë si qëllimin e tyre kryesor.

- Sigurimi i mjeteve të përshtatshme për moshën e gjithësecilit për të ndihmuar në menaxhimin sa më të mirë të mbrojtjes së familjeve gjatë lundrimit në internet;
- Sigurimi i mekanizmave të përshtatshëm për raportimin e cështjeve apo shqetësimeve në internet. Përdoruesit duhet të kenë përgjigje të menjëhershme lidhur me këto raportime lidhur me veprimet që janë ndërmarrë ose në rastet kur është e mundur orientimi drejt hapave ku përdoruesit mund te marrin mbeshtetje te metejshme;
- Rëndesi perben sigurimi i nje raportimi proaktiv i abuzimit ndaj femijeve per te identifikuar dhe adresuar cdo lloj abuzimi (i klasifikuar si veprimtari kriminale) ndaj femijeve. Kjo lloj praktike ka treguar se nese te gjitha palet jane te interesuara per te zbuluar, bllokuar dhe raportuar vetem atehere mund te pretendojme te kemi nje hapesire me te paster, dhe te sigurte ne internet per te gjithe.Te gjitha industrite duhet te marrin ne konsiderate mjete te cilat pengojne shfrytezimin e platformave te tyre sic janeIWF Services.

Eshte tejet thelbesore angazhimi i te gjithe aktoreve ne nje ekosistem i cili duhet te jete i vetedijshem lidhur me reziqet apo demet ne internet dhe keshtu dueht te jete ne gjendje te parandaloje situatat ku femijet te gjenden te ekspozuar ndaj rreziqeve te tilla te panevojshme.

Zhvillimi i njësive matëse të cilat lidhen me sigurinë e fëmijëve në internet mundëson matjen e të gjitha aspekteve që kanë ndikim në këtë cështje. Standartet e përbashkëta matëse janë e vetmja mënyrë për të ndjekur progresin në vende të ndryshme apo për të përcaktuar suksesin e projekteve apo aktiviteteve të ndryshme të zhvilluara për të eleminuar kështu cdo dhunë ndaj fëmijëve, duke njohur kështu forcën e eksistemit mbrojtës për fëmijët në internet.

5. Zhvillimi i një strategjie për mbrojtjen e fëmijëve online

5.1 Një listë kombëtare

Për të formuluar një strategji kombëtare që përqendrohet në sigurinë e fëmijëve në Internet, politikëbërësit duhet të marrin në konsideratë një varg strategjish. Tabela 1 përcakton fushat kryesore për tu marrë në konsideratë.

Tabela 1: Fushat kryesore për t'u marrë në konsideratë

	#	Aspektet kryesore për t'u konsideruar	Detaje të mëtejshme
Korniza ligjore	1	Rishikoni kornizën ligjore ekzistuese për të përcaktuar ekzistencën e të gjitha kompetencave të nevojshme ligjore që mundësojnë zbatimin e ligjit dhe agjencitë e tjera përkatëse për të mbrojtur personat nën moshën 18 vjeç në të gjitha platformat e mundësuara nga interneti.	Në përgjithësi do të jetë e nevojshme që të ekzistojë një tërësi ligjore që bën të qartë se ndonjë dhe çdo krim që mund të kryhet kundrejt një fëmije në botën reale mund të kryhet në mënyrë të ngjashme edhe në internet ose në ndonjë tjetër rrjet elektronik.
	2	Vendosni, në mënyrë të njejtë, që çdo veprim i paligjshëm në botën reale kundrejt një fëmije, është i paligjshëm në internet dhe se rregullat e mbrojtjes së të dhënave online dhe rregullave të privatësisë për fëmijët janë gjithashtu adekuate.	Mund të jetë gjithashtu e nevojshme të zhvillohen ligje të reja ose të përshtaten ato ekzistueset për t'i bërë të jashtëligjshme disa lloje të caktuara sjelljesh që mund të ndodhin vetëm në internet, për shembull joshja e fëmijëve për të kryer ose parë akte seksuale nga larg, ose shfrytëzimi i fëmijëve për t'u takuar në realitet për qëllime seksuale. Ndihmuese për këto qëllime do të jetë ekzistenca e një kornize ligjore që nxjerr të si të jashtëligjshme keqpërdorimin e kompjuterëve për qëllime kriminale, hakimin ose përdorimin e dëmshëm ose jo-konsensual të kodit kompjuterik dhe përcakton se interneti është një vendndodhje brenda të cilit mund të kryhen krime.

	#	Aspektet kryesore për t'u konsideruar	Detaje të mëtejshme
Korniza regullatore	3	Merrni parasysh zhvillimin e politikës rregullatore. Kjo mund të përfshijë një zhvillim të politikës vetë ose bashkë-rregulluese, si dhe një kornizë të plotë rregullatore. Modeli vetë ose bashkë-rregullues mund të përfshijë formulimin dhe botimin e kodeve të praktikave të mira ose pritshmërive themelore të sigurisë në internet, si në terma të ndihmës për të angazhuar, koordinuar ose orkestruar dhe mbështetur përfshirjen e të gjithë aktorëve të përshtatshëm dhe në terma të rritjes së shpejtësisë me të cilën mund të formulohen dhe vihen në veprim përgjigjet e duhura ndaj ndryshimeve teknologjike. Një model rregullator mund të përcaktojë pritjet dhe detyrimet ndërmjet palëve të interesuara dhe të vendosen brenda një konteksti ligjor. Dënimet për shkelje të politikave gjithashtu mund të merren parasysh.	Disa vende kanë krijuar një model vetë ose bashkë rregullator në lidhje me zhvillimin e politikave në këtë fushë dhe përmes modeleve të tilla ata kanë, për shembull, kodet e botuara të praktikave të duhura për të drejtuar industrinë e internetit në lidhje me masat që mund të funksionojnë më mirë kur bëhet fjalë për t'i mbajtur fëmijët dhe të rinjtë më të sigurt në internet. Për shembull brenda Bashkimit Evropian ku kodet në të gjithë BE-në janë botuar si për faqet e rrjeteve sociale dhe rrjetet e telefonisë mobile në lidhje me sigurimin e përmbajtjes dhe shërbimeve për fëmijët dhe të rinjtë përmes rrjeteve të tyre. Vetë dhe bashkë-rregullimi mund të jetë mënyra e duhur në drejtim të rritjes së shpejtësisë me të cilën përgjigjet e duhura ndaj ndryshimeve teknologjike mund të formulohen dhe të vihen në veprim. Kohët e fundit disa vende kanë zhvilluar dhe/ose zbatuar një kornizë rregullatore. Në këta shembuj, korniza rregullatore është zhvilluar nga modelet vetë-rregulluese dhe përcakton kërkesat dhe pritshmëritë për palët e interesit, veçanërisht ofruesit e industrisë, për të mbrojtur më mirë përdoruesit e tyre.

	#	Aspektet kryesore për t'u konsideruar	Detaje të mëtejshme
Raportimi i përmbajtjeve ligjore	4	Sigurohuni që një mekanizëm është krijuar dhe promovohet gjerësisht për të siguruar mjete lehtësisht të kuptueshme për raportimin e shumëllojshmërisë së përmbajtjes së paligjshme të gjetura në internet. Për shembull, një linjë telefonike kombëtare, e cila ka aftësinë të përgjigjet shpejt dhe të heqë materiale të paligjshme ose të bëhen të paaksesueshme. Industria duhet të ketë mekanizma për të identifikuar, bllokuar dhe hequr abuzimin ndaj fëmijëve në internet, duke marrë të gjitha shërbimet e rëndësishme për organizatat e tyre.	Mekanizmat për raportimin e abuzimit të një shërbimi online ose për raportimin e një sjelljeje të gabuar ose të paligjshme në internet, për shembull në një linjë telefonike kombëtare, duhet të reklamohen gjerësisht dhe të promovohen si në Internet dhe në media të tjera. Nëse një linjë telefonike kombëtare nuk është në dispozicion, IWF ofron zgjidhjen nëpërmjet Portaleve të Raportimit. Lidhjet për të raportuar mekanizmat e abuzimit duhet të shfaqen dukshëm në pjesët përkatëse të çdo faqe në internet që lejon shfaqjen e përmbajtjes së krijuar nga përdoruesit. Duhet gjithashtu të jetë e mundur që njerëzit që ndihen të kërcënuar në ndonjë mënyrë, ose për njerëzit që kanë parë ndonjë aktivitet shqetësues në internet, të jenë në gjendje ta raportojnë atë sa më shpejt që të jetë e mundur në agjencitë përkatëse të zbatimit të ligjit që duhet të trajnohen dhe të jenë të gatshëm të përgjigjen. Task Forca Virtuale Globale është një organ i zbatimit të ligjit i cili siguron një mekanizëm 24/7 për të marrë raporte në lidhje me sjelljen e paligjshme ose përmbajtjen nga persona në SHBA, Kanada, Australi dhe Itali, me vendet e tjera që pritet të bashkohen së shpejti. Shikoni www .virtualglobaltaskforce .com. Shikoni gjithashtu INHOPE.
Raportimi i problemeve të përdoruesit	5	Industritë duhet t'i ofrojnë përdoruesve mundësinë për të raportuar shqetësimet dhe problematikat dhe t'u përgjigjen në bazë të rrethanave.	Ofruesit duhet **t**ë jenë të detyruar të ofrojnë dhe sinjalizojnë në mënyrë të qartë, përdoruesve të tyre mundësinë e raportimit të problemeve dhe shqetësimeve brenda shërbimit që ata ofrojnë. Ata duhet të jenë miqësor dhe lehtësisht të disponueshëm.

	#	Aspektet kryesore për t'u konsideruar	Informacion i detajuar
Aktorët dhe palët e interesit	6	Angazhoni të gjithë aktorët e përshtatshëm me interes në mbrojtjen e fëmijëve në internet, në veçanti: • Agjensitë qeveritare • Zbatuesit e ligjit (ekzekutivët) • Organizatat e shërbimeve sociale • Ofruesit e Shërbimeve të Internetit (ISP) dhe ofruesit e tjerë të shërbimeve elektronike (ESP) • Ofruesit e rrjetit të telefonit celular • Ofruesit publik të Wi-Fi • Kompani të tjera relevante të teknologjisë së lartë • Organizatat e mësuesve • Organizatat prindërore • Fëmijë dhe të rinj • Mbrojtja e fëmijëve dhe OJQ-të e tjera përkatëse • Komuniteti akademik dhe kërkimor Pronarët e kafeneve në Internet dhe ofruesit e tjerë të aksesit publik p.sh. bibliotekat, telecentrat, PC Bangs63 dhe qendrat e lojrave në internet etj.	Disa qeveri kombëtare e shohin të dobishme të bashkojnë të gjithë aktorët kryesorë të interesit dhe pjesmarrësit për t'u përqëndruar në zhvillimin dhe zbatimin e një iniciative kombëtare për ta bërë internetin një vend më të sigurt për fëmijët dhe të rinjtë, dhe rritjen e ndërgjegjësimit për çështjet dhe mënyrën e trajtimit në një mënyrë shumë praktike. Do të jetë e rëndësishme brenda kësaj strategjie të vlerësojmë që shumë janë të lidhur në mënyrë universale dhe vazhdimisht me internetin përmes një larmie pajisjesh. Operatorët e rrjetit, celular dhe Wi-Fi duhet të përfshihen. Për më tepër, në shumë vende rrjeti i bibliotekave publike, telecentrave dhe kafeneve në Internet mund të jenë burime të rëndësishme të aksesit në Internet, veçanërisht për fëmijët dhe të rinjtë.
Kërkimet	7	Ndërmerrni kërkime në lidhje me spektrin e aktorëve dhe palëve kombëtare të interesit për të përcaktuar mendimet, përvojat, shqetësimet dhe mundësitë e tyre në lidhje me mbrojtjen e fëmijëve në Internet. Kjo gjithashtu duhet të vlerësojë shkallën e çdo përgjegjësie së bashku me aktivitetet ekzistuese ose të planifikuara për të mbrojtur fëmijët në internet.	

A “PC Bang” is term commonly used in the Republic of Korea and in some other countries to describe a large room where a LAN facilitates large scale game playing, either online or between players in the

63

room.

	#	Aspektet kryesore për t'u konsideruar	Detaje të mëtejshme
Literatura e edukimit dixhital dhe kompetencat	8	Zhvilloni karakteristikat e literaturës dixhitale si pjesë të çdo programi shkollor kombëtar që është i përshtatshëm për moshën dhe i zbatueshëm për të gjithë fëmijët.	Shkollat dhe sistemi arsimor në përgjithësi do të përfaqësojnë bazën e komponentit të edukimit dhe literaturës dixhitale të një strategjie kombëtare mbi mbrojtjen e fëmijëve në internet. Çdo kurrikul shkollore kombëtare duhet të përfshijë aspekte të mbrojtjes së fëmijëve në Internet dhe të synojë t'u sigurojë fëmijëve të të gjitha moshave aftësi të përshtatshme për të përfituar dhe përdorur me sukses teknologjinë dhe për të qenë të ndjeshëm ndaj kërcënimeve dhe dëmeve që duhet të shmangen me sukses. Këto kurrikula duhet të njohin dhe shpërblejnë sjelljet pozitive dhe konstruktive në internet. Brenda çdo fushate edukimi dhe ndërgjegjësimi është e rëndësishme të jepet toni i duhur. Mesazhet e bazuara në frikë duhet të shmangen dhe vëmendja e duhur duhet t'i jepet tipareve dhe karakteristikave pozitive dhe argëtuese të teknologjisë së re. Interneti ka një potencial të madh si një mjet për të fuqizuar fëmijët dhe të rinjtë që të zbulojnë botë të reja. Mësimi i formave pozitive dhe të përgjegjshme të mënyrës së të sjellurit në internet është objektivi kryesor i programeve të edukimit dhe ndërgjegjësimit. Ata që punojnë me fëmijë, veçanërisht mësuesit, duhet të aftësohen dhe pajisen në mënyrë të përshtatshme për të edukuar me sukses dhe për t'u siguruar fëmijëve këto aftësi. Ata duhet të kuptojnë kërcënimet dhe dëmet në internet dhe së bashku m to, të kenë aftësinë për të njohur shenjat e abuzimit dhe dëmtimit dhe për t'iu përgjigjur dhe raportuar këto shqetësime në mënyrë që të mbrojnë fëmijët e tyre.

	#	Aspektet kryesore për t'u konsideruar	Detaje të mëtejshme
Resurset edukative	9	Përfitoni nga njohuritë dhe përvoja e të gjithë palëve të interesuara dhe zhvilloni mesazhe dhe materiale të sigurisë në Internet që pasqyrojnë normat dhe ligjet kulturore lokale dhe sigurohuni që këto të shpërndahen në mënyrë efikase dhe të shpërndahen në mënyrë të përshtatshme për të gjithë audiencat kryesore të synuara. Merrni parasysh mundësinë që të marrni ndihmë nga mass media në promovimin e mesazheve të ndërgjegjësimit. Zhvilloni materiale që theksojnë aspektet pozitive dhe fuqizuese të internetit për fëmijët dhe të rinjtë dhe shmangin mesazhet e bazuara në frikë. Promovoni forma pozitive dhe të përgjegjshme të sjelljes në internet. Merrni parasysh zhvillimin e burimeve për të ndihmuar prindërit të vlerësojnë sigurinë e fëmijëve të tyre në internet dhe të mësojnë se si të minimizojnë rreziqet dhe të maksimizojnë potencialin për familjen e tyre përmes arsimit të synuar.	Kur prodhoni materiale edukuese, është e rëndësishme të keni parasysh se shumë njerëz që janë të rinj në teknologji nuk do të ndihen rehat kur ta përdorin atë. Për këtë arsye, është e rëndësishme të sigurohet që materialet e sigurisë të vihen në dispozicion ose në formë të shkruar ose të prodhohen duke përdorur media të tjera me të cilat të sapoardhurit do të ndihen më të njohur, për shembull, me video. Shumë nga kompanitë e mëdha të Internetit prodhojnë faqe në internet të cilat përmbajnë një marrëveshje informacioni rreth çështjeve në internet për fëmijët dhe të rinjtë. Megjithatë, shumë herë ky material mund të jetë i disponueshëm vetëm në anglisht ose në një grup shumë të ngushtë gjuhësh. Është shumë e rëndësishme, pra, që materialet të prodhohen lokalisht, që reflektojnë ligjet lokale, si dhe normat kulturore lokale. Kjo do të jetë thelbësore për çdo fushatë të sigurisë në Internet ose çdo material trajnimi që zhvillohet.
Mbrojtja e fëmijëve	10	Sigurohuni që ekzistojnë mekanizma universalë dhe sistematikë të mbrojtjes së fëmijëve që detyrojnë të gjithë ata që punojnë me fëmijë (kujdesi social, shëndetësia, shkollat etj.) të identifikojnë, përgjigjen dhe raportojnë incidentet e abuzimit dhe problematikave që ndodhin në internet.	Duhet të ekzistojë një sistem universal dhe i zbatueshëm për mbrojtjen e fëmijëve për të gjithë ata që punojnë me fëmijët, duke i detyruar ata të raportojnë mbi abuzimet ndaj tyre në mënyrë që hetimet tmos pengohen dhe situatat të zgjidhen.

	#	Fushat kryesore për t'u konsideruar	Detaje të mëtejshme
Ndërgjegjësimi kombëtar	11	Organizoni fushata kombëtare për ndërgjegjësim që të krijojmë mundësi për të nxjerrë në pah çështjet e mbrojtjes së fëmijëve në Internet. Mund të jetë e dobishme të shfrytëzohen fushata globale siç është Dita e Internetit më të Sigurt për të ndërtuar një fushatë.	Prindërit, kujdestarët dhe profesionistët, të tillë si mësuesit, kanë një rol vendimtar për të mbajtur fëmijët dhe të rinjtë më të sigurt në internet. Duhet të zhvillohen programe mbështetëse të cilat ndihmojnë në rritjen e ndërgjegjësimit për çështje të caktuara dhe gjithashtu ofrojnë strategji për trajtimin e tyre. Duhet të merret gjithashtu parasysh marrja e ndihmës së mass mediave në promovimin e mesazheve dhe fushatave të ndërgjegjësimit. Mundësi të tilla si Dita e Internetit më të Sigurt do të jenë të dobishme në stimulimin dhe inkurajimin e një dialogu kombëtar për mbrojtjen e fëmijëve në internet. Shumë vende kanë ndërmarrë me sukses fushata të ndërgjegjësimit kombëtar rreth "Ditës së Internetit më të Sigurt" dhe përfshijnë grupin e plotë të aktorëve dhe palëve të interesit në amplifikimin e mesazheve universale nëpër media dhe media sociale

	#	Aspektet kryesore për t'u konsideruar	Detaje të mëtejshme
Mjete, shërbime dhe cilësimet	12	Merrni parasysh rolin e cilësimeve të pajisjes, mjeteve teknike (të tilla si programet e filtrimit) dhe aplikacioneve dhe cilësimeve që mund të ndihmojnë për mbrojtjen e fëmijëve. Inkurajoni përdoruesit të marrin përgjegjësi për pajisjet e tyre duke inkurajuar përditësime të sistemit operativ së bashku me përdorimin e softuerëve dhe aplikacioneve më të përshtatshme për sigurinë e fëmijëve.	Ka disa shërbime të disponueshme që mund të ndihmojnë në shfaqjen e materialit të padëshiruar ose bllokimin e kontakteve të padëshiruara. Disa prej këtyre programeve të sigurisë dhe filtrimit mund të jenë në thelb falas sepse ato janë pjesë e një sistemi operativ ose ato ofrohen si pjesë e një pakete të disponueshme nga një ISP ose ESP. Prodhuesit e disa lojërave gjithashtu ofrojnë mjete të ngjashme nëse pajisja është e aktivizuar në Internet. Këto programe nuk janë të padobishme, por ato mund të ofrojnë një nivel fillestar të mbështetjes, veçanërisht në familje me fëmijë të vegjël. Shumica e pajisjeve përmbajnë cilësime që ndihmojnë në mbrojtjen e fëmijëve dhe gjithashtu promovojnë përdorim të shëndetshëm dhe të ekuilibruar. Kjo shtrihet dhe në mekanizmat që lejojnë prindërit të menaxhojnë pajisjet e fëmijëve të tyre, duke alokuar kohën, aplikacionet dhe shërbimet që ata janë në gjendje të përdorin dhe të menaxhojnë një blerje. Kohët e fundit raportet dhe cilësimet janë zhvilluar për të mundësuar përdoruesit dhe prindërit të kuptojnë dhe menaxhojnë më mirë kohën dhe qasjen në ekran. Këto mjete teknike duhet të përdoren si pjesë e një arsenali më të gjerë. Përfshirja e prindërve dhe/ose kujdestarit është kritike. Ndërsa fëmijët fillojnë të rriten, ata do të duan më shumë privatësi dhe gjithashtu do të ndiejnë një dëshirë të fortë që të eksplorojnë vetë. Përveç kësaj, kur ekziston një marrëdhënie faturimi midis shitësit dhe klientit, proceset e verifikimit të moshës mund të luajnë një rol shumë të vlefshëm për të ndihmuar shitësit e mallrave dhe shërbimeve të kufizuara në moshë ose botuesve të materialit i cili është menduar vetëm për audiencat në ose mbi një moshë të caktuar, për të arritur tek ato audienca specifike. Kur nuk ka marrëdhënie faturimi, përdorimi i teknologjisë së verifikimit të moshës mund të jetë problematik ose në shumë vende mund të jetë i pamundur për shkak të mungesës së burimeve të besueshme të të dhënave.

5.2 Shembuj pyetjesh

Me identifikimin e palëve të interesit dhe aktorëve, pyetjet e mëposhtme mund të shpërndahen tek ta dhe ata t'u përgjigjen. Përgjigjet e tyre do të ndihmojnë në përcaktimin e shkallës së mbulimit që bëjnë politikave, pikat e forta, si dhe fushat për t'u përqëndruar në të gjithë listën kombëtare të kontrollit.

• Deri në cilën masë ofrohen siguria në internet dhe të drejtat e fëmijëve?

• Si integrohen siguria në internet dhe të drejtat e fëmijëve në politikat dhe proceset tuaja ekzistuese?

• Në çfarë mase është mbulohet siguria në internet brenda legjislacionit ekzistues?

• Cilat janë përparësitë tuaja të sigurisë në internet?

• Çfarë aktivitetesh keni për të mbështetur sigurinë në internet?

• Si punoni me agjencitë dhe organizatat e tjera për të përmirësuar/ përparuar sigurinë në internet?

• A mund t'ju raportojnë fëmijët/prindërit shqetësime ose çështje të sigurisë në internet?

• Cilat janë tre sfidat tuaja kryesore në botën online?

• Cilat janë tre mundësitë tuaja kryesore në botën online?

Do të ishte gjithashtu e dobishme të ndërmerren kërkime dhe të kuptohen perceptimi dhe përvojat e fëmijëve, si dhe prindërve të tyre në lidhje me mbrojtjen e fëmijëve në internet.

6. Reference material

Child online safety: Key documents and publications

2020

- ECPAT International, Sexual Exploitation Of Children In The Middle East And North Africa, 2020
- DQ Institute, 2020 Child Online Safety Report, 2020
- EU Kids Online, EU Kids Online 2020: Survey results from 19 countries, 2020

2019

- Internet Watch Foundation (IWF), Annual Report, 2019
- WeProtect Global Alliance, Global Threat Assessment, 2019
- Broadband Commission / ITU, Child Online Safety. Universal Declaration, 2019
- Broadband Commission / ITU, Child Safety Online: Minimizing the Risk of Violence, Abuse and Exploitation Online, 2019
- Global Kids Online, Growing up in a connected world, 2019
- Rethinking the Detection of Child Sexual Abuse Imagery on the Internet, in Proceedings of the 2019 World Wide Web Conference, May 13–17, 2019, San Francisco, USA, 2019
- UK Home Office, Online Harms White Paper (UK only), 2019
- PA Consulting, A tangled web: rethinking the approach to online CSEA, 2019
- UK Information Commissioner Office, Consultation on Code of Practice to help protect children online (UK only), 2019
- Global Fund to End Violence against Children, Disrupting Harm: evidence to understand online child sexual exploitation and abuse, 2019
- Global Partnership to End Violence against Children, Safe to Learn Call for Action, Youth Manifesto, 2019
- UNESCO, Behind the numbers: Ending school violence and bullying, 2019 (includes data on online hurtful behaviour and cyber-bullying)
- United Nations Human Rights, children's rights in relation to the digital environment, 2019
- Australian eSafety Commissioner, Safety by Design Overview, 2019
- UNICEF, Why businesses should invest in digital child safety brief, 2019
- U.S. Department of State, Trafficking in Persons report, 2019

2018

- WeProtect Global Alliance, Global Threat Assessment, 2018
- Child Dignity on the Digital World, Technical Working Group Report, 2018 Council of Europe, Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 2018
- Global Fund to End Violence against Children, Two years of supporting solutions: results from the Fund's investments, 2018
- WeProtect Global Alliance, Country examples of Model of National Response capabilities and implementation, 2018
- INTERPOL and ECPAT International, Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material, 2018
- EUROPOL, Internet Organized Crime Threat Assessment (IOCTA), 2018
- NetClean, Report about Child Sexual Abuse Cybercrime, 2018
- International Centre for Missing & Exploited Children (ICMEC), Child Sexual Abuse Material: Model Legislation & Global Review, 9th Edition, 2018

- International Centre for Missing & Exploited Children (ICMEC), Studies in Child Protection: Sexual Extortion and Non-Consensual Pornography, 2018
- International Association of Internet Hotlines, INHOPE Report, 2018
- Internet Watch Foundation (IWF), Annual Report, 2018
- Thorn, Production and Active Trading of Child Sexual Exploitation Images, 2018
- ITU, Global Cybersecurity Index, 2018
- CSA Centre of Expertise, Interventions for perpetrators of online child sexual exploitation - a scoping review and gap analysis, 2018
- NatCen, Behaviour and Characteristics of Perpetrators of Online-facilitated CSEA - a rapid evidence assessment, 2018
- UNICEF, Policy guide on children and digital connectivity, 2018

2017

- The National Center for Missing & Exploited Children (NCMEC), The online enticement of children: an in-depth analysis of CyberTipline Reports, 2017
- 5Rights Foundation, Digital Childhood, development milestones in digital environment, 2017
- Childnet, DeShame Report, 2017
- Canadian Centre for Child Protection, Survivors' survey, 2017
- Internet Watch Foundation (IWF), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review, 2017
- Thorn, Sextortion online survey with 2,097 victims of sextortion ages 13 to 25, 2017
- UNICEF, Children in a Digital World, 2017
- Western Sydney University, Young and Online: Children's Perspectives on Life in Digital Age, 2017
- ECPAT International, Sexual Exploitation of Children in South East Asia, 2017

2016

- UNICEF, Perils and possibilities: growing up online, 2016
- UNICEF, Child protection in the digital age: National responses to online CSEA in ASEAN, 2016
- Centre for Justice and Crime Prevention, Child Online Protection in the MENA Region, 2016
- ECPAT International, Interagency Working Group on Sexual Exploitation of Children, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (The Luxembourg Guidelines), 2016

2015

- WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, 2015
- NCMEC, A Global Landscape of Hotlines Combating CSAM, 2015
- ITU and UNICEF, Guidelines for Industry on Child Online Protection, 2015

Related to human rights in a digital world

- Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 2018
- UNESCO, Internet Universality Indicators, 2019
- Ranking Digital Rights (RDR), 2019 RDR Corporate Accountability Index, 2019
- Broadband Commission for Sustainable Development, The State of the Broadband, 2019

- ITU, Measuring Digital Development, 2019
- ITU, Measuring Information Society Report, 2018
- UNICEF, Children and Digital Marketing Industry Toolkit, 2018
- Broadband Commission for Sustainable Development, Digital health, 2017
- Broadband Commission for Sustainable Development, Digital Skills for life and work, 2017
- Broadband Commission for Sustainable Development, Digital gender divide, 2017
- UNICEF, Privacy, protection of personal information and reputation, 2017
- UNICEF, Freedom of expression, association, access to information and participation, 2017
- UNICEF, Access to the Internet and digital literacy, 2017
- UN CRC, Guidelines on effective protection of children from sexual exploitation, 2019

For further resources, please refer to the additional resource list on www .itu - cop -guidelines .com

Aneksi 1: Terminologjia

Fëmijë

Në përputhje me nenin 1 të Konventës për të Drejtat e Fëmijëve, një fëmijë është çdo person nën 18 vjeç sipas ligjit kombëtar.[23]

Shfrytëzimi dhe abuzimi seksual i fëmijëve (CSEA)

Përshkruan të gjitha format e shfrytëzimit seksual dhe abuzimit seksual (CRC, 1989, art. 34), p.sh. "(a) nxitja ose detyrimi i një fëmije për t'u përfshirë në ndonjë veprimtari të paligjshme seksuale; (b) Shfrytëzimi i fëmijëve në prostitucion ose praktika të tjera të paligjshme seksuale; (c) Shfrytëzimi i fëmijëve në shfaqje dhe materiale pornografike", si dhe një "kontakt seksual që zakonisht përfshin forcë ndaj një personi pa pëlqim". Shfrytëzimi dhe abuzimi seksual i fëmijëve bëhet gjithnjë e më shumë përmes internetit ose me ndonjë lidhje me mjedisin në internet[24].

Material seksual (shfrytëzimi dhe abuzimi) i fëmijëve (CSAM)

Evolucioni i shpejtë i TIK ka krijuar forma të reja të shfrytëzimit dhe abuzimit seksual të fëmijëve në internet, të cilat mund të ndodhin praktikisht dhe jo domosdoshmërisht përfshijnë takime fizike ballë për ballë me fëmijën[25]. Megjithëse shumë juridiksione ende etiketojnë imazhe dhe video të abuzimit seksual të fëmijëve 'pornografi fëmijësh' ose 'imazhe të pahijshme të fëmijëve', këto udhëzime do t'u referohen subjekteve kolektivisht si material i abuzimit seksual të fëmijëve (tani e tutje, CSAM). Kjo është në përputhje me Udhëzimet e Komisionit të Broadband dhe Përgjigjen Kombëtare të Aleancës Globale ËePROTECT[26]. Ky term përshkruan më saktë përmbajtjen. Pornografia i referohet një industrie të ligjshme, të komercializuar dhe siç përcaktojnë Udhëzimet e Luksemburgut përdorimin e termit:

"Mund (pa dashje ose jo) të kontribuojë në zvogëlimin e gravitetit, banalizimin, apo edhe legjitimin e asaj që në të vërtetë është abuzimi seksual dhe / ose shfrytëzimi seksual i fëmijëve […] termi" pornografi e fëmijëve "rrezikon të nënkuptojë se veprimet janë kryer me pëlqimin e fëmijës dhe paraqesin material legjitim seksual "[27].

Termi CSAM i referohet materialit që përfaqëson veprime që janë abuzive seksuale dhe / ose shfrytëzuese për një fëmijë. Kjo përfshin, por nuk kufizohet në, material që regjistron abuzimin seksual të fëmijëve nga të rriturit; imazhe të fëmijëve të përfshirë në sjellje të qarta seksuale; organet seksuale të fëmijëve kur imazhet prodhohen ose përdoren kryesisht për qëllime seksuale.

[23] OHCHR; UNICEF and ITU, *Guidelines for Industry on Child Online Protection*.

[24] "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

[25] "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse"; UNICEF, "Global Kids Online Comparative Report (2019)."

[26] WePROTECT Global Alliance, "Preventing and Tackling Child Sexual Exploitation and Absue (CSEA): A Model National Response.," 2016, https:// static1 .squarespace .com/ static/ 5630f48de4b00a75476ecf0a/ t/ 582ba50bc534a51764e8a4ec/ 1479255310190/ WePROTECT+G lobal+Alliance+Mode l+National+Response+Guidance .pdf; Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)."

[27] "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

Fëmijët dhe të rinjtë

Përshkruan të gjithë personat nën moshën 18 vjeç, ku fëmijët, të referuar edhe si fëmijë më të vegjël në udhëzime, përfshin të gjithë personat nën moshën 15 vjeç dhe të rinjtë përbëhen nga grupmosha 15 deri në 18 vjeç.

Connected toys Lodrat e lidhura

Lodrat e lidhura

Lodrat e lidhura lidhen me internetin duke përdorur teknologji të tilla si Ëi-Fi dhe Bluetooth dhe zakonisht funksionojnë së bashku me aplikacionet shoqëruese për të mundësuar lojë interaktive për fëmijët. Sipas Juniper Research, në vitin 2015 tregu për lodrat e lidhura arriti në 2.8 miliardë dollarë dhe parashikohet të rritet në 11 miliardë dollarë deri në vitin 2020. Këto lodra mbledhin dhe ruajnë informacione personale nga fëmijët, përfshirë emrat, vendndodhjet gjeografike, adresat, fotografitë, audio dhe video regjistrimet. [28].

Bullizmi në internet, referuar gjithashtu si ngacmim në internet

E drejta ndërkombëtare nuk e përcakton ngacmimin në internet. Për qëllimet e këtij dokumenti, ngacmimi në internet përshkruhet një veprim i qëllimshëm agresiv i kryer në mënyrë të përsëritur ose nga një grup ose nga një individ duke përdorur teknologjinë dixhitale dhe që synon një viktimë që nuk mund të mbrohet lehtë[29]. Zakonisht përfshin "përdorimin e teknologjisë dixhitale dhe internetit për të postuar informacione të dëmshme për dikë, duke shpërndarë qëllimisht informacione private, foto ose video në një mënyrë të dëmshme, dërgimin e mesazheve kërcënuese ose fyese (përmes postës elektronike, mesazheve të çastit, bisedës, teksteve), përhapjen e thashethemeve dhe informacion i rremë për viktimën ose përjashtimin e tij me qëllim nga komunikimet në internet ". Mund të përfshijë komunikime të drejtpërdrejta[30] (të tilla si biseda ose mesazhe me tekst), gjysmë publike (të tilla si postimi i një mesazhi ngacmues në një listë e-mail) ose komunikime publike (të tilla si krijimi i një faqe në internet kushtuar talljes me viktimën).

Cyberhate, diskriminimi dhe ekstremizmi i dhunshëm

"Cyberhate, diskriminimi dhe ekstremizmi i dhunshëm janë një formë e veçantë e dhunës kibernetike pasi synon një identitet kolektiv, sesa individë […] shpesh që kanë të bëjnë me racën, orientimin seksual, fenë, kombësinë ose statusin e imigracionit, seksin / gjininë dhe politikën"[31].

Shtetësia dixhitale

Qytetaria dixhitale i referohet aftësisë për t'u angazhuar pozitivisht, në mënyrë kritike dhe me kompetencë në mjedisin dixhital, duke u mbështetur në aftësitë e komunikimit dhe krijimit efektiv, për

[28] Jeremy Greenberg, "Dangerous Games: Connected Toys, COPPA, and Bad Security," Georgetown Law Technology Review, December 4, 2017, https:// georgetownlawtechreview .org/ dangerous -games -connected -toys -coppa -and -bad -security/ GLTR -12 -2017/ .

[29] Anna Costanza Baldry, Anna Sorrentino, and David P. Farrington, "Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities," Children and Youth Services Review 96 (January 2019): 302–7, https:// doi .org/ 10 .1016/ j .childyouth .2018 .11 .058.

[30] UNICEF, "Global Kids Online Comparative Report (2019)"; "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

[31] UNICEF, "Global Kids Online Comparative Report (2019)."

të praktikuar forma të pjesëmarrjes sociale që respektojnë të drejtat dhe dinjitetin e njeriut përmes përdorimit të përgjegjshëm të teknologjisë[32].

Shkrim-leximi dixhital

Njohuri dixhitale do të thotë të kesh aftësitë që i duhen dikujt për të jetuar, mësuar dhe punuar në një shoqëri ku komunikimi dhe qasja në informacion është gjithnjë e më shumë përmes teknologjive dixhitale si interneti, rrjetet sociale dhe pajisjet mobile [33]. Përfshihet komunikimi i pastër, aftësitë teknike dhe mendimi kritik.

Elasticiteti dixhital

Ky term përshkruan aftësinë e një fëmije për të përballuar emocionalisht dëmet në internet. Elasticiteti dixhital përfshinte pasurimin e burimeve emocionale të nevojshme për të kuptuar kur fëmija rrezikon në internet, të dijë çfarë të bëjë për të kërkuar ndihmë, për të mësuar nga përvoja dhe për tu rikuperuar kur gjërat shkojnë keq [34].

Edukatorët

Një edukator është një person i cili punon në mënyrë sistematike për të përmirësuar kuptimin e një personi tjetër për një temë të caktuar. Roli i arsimtarëve përfshin si ata që japin mësim në klasa ashtu edhe edukatorët më informalë të cilët, për shembull, ata që përdorin platforma dhe shërbime të faqeve të rrjeteve sociale për të siguruar informacion në internet të sigurisë ose për të drejtuar kurse të bazuara në komunitet ose shkollë për të mundësuar që fëmijët dhe të rinjtë të qëndrojnë të sigurt në internet.

Puna e arsimtarëve do të ndryshojë në varësi të kontekstit në të cilin ata punojnë dhe grupmoshës së fëmijëve dhe të rinjve (ose të rriturve) që ata kërkojnë të arsimojnë.

Joshja/Ngacmimi online

Grooming / grooming online siç përcaktohet në Udhëzimet e Luksemburgut, i referohet procesit të krijimit / ndërtimit të një marrëdhënieje me një fëmijë ose personalisht ose përmes përdorimit të Internetit ose teknologjive të tjera dixhitale për të lehtësuar kontaktin seksual në internet ose në internet me atë person për të bindur fëmija të ketë një marrëdhënie seksuale[35]. Një proces që synon të joshë fëmijët në sjellje seksuale ose biseda me ose pa dijeninë e tyre, ose një proces që përfshin komunikimin dhe shoqërizimin midis autorit të veprës dhe fëmijës në mënyrë që ta bëjë atë ose atë më të prekshëm ndaj abuzimit seksual. Termi pastrim nuk është përcaktuar në të drejtën ndërkombëtare; disa juridiksione, përfshirë Kanadanë, përdorin termin 'joshje'.

[32] Council of Europe, "Digital Citizenship and Digital Citizenship Education," Digital Citizenship Education, accessed January 16, 2020, https:// www .coe .int/ en/ web/ digital -citizenship -education/ home.

[33] Western Sydney University-Claire Urbach, "What Is Digital Literacy?," accessed January 16, 2020, https:// www .westernsydney .edu .au/ studysmart/ home/ digital _literacy/ what _is _digital _literacy.

[34] Dr. Andrew K. Przybylski, et al., "A Shared Responsibility. Building Children's' Online Resilience Report" (ParentZone, University of Oxford and Virgin Media, 2014), https:// parentzone .org. uk/sites/ default/ files/ Building %20Online %20Resilience %20Report .pdf.

[35] "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse."

Teknologjitë e informacionit dhe komunikimit (TIK)

Teknologjitë e informacionit dhe komunikimit përshkruajnë të gjitha teknologjitë e informacionit që theksojnë aspektin e komunikimit. Kjo përfshin të gjitha shërbimet dhe pajisjet që lidhin internetin, të tilla si kompjuteri, laptopët, tabletët, telefonat inteligjentë, konzollat e lojërave, televizorët dhe orët[36]. Më tej përfshin shërbime të tilla si radio, si dhe ndër të tjera bandë të gjerë, pajisje rrjetore dhe sisteme satelitore.Information and communication technologies (ICTs).

Interneti dhe teknologjitë shoqëruese

Tani është e mundur të lidheni me internet duke përdorur një larmi pajisjesh të ndryshme, p.sh., smartphone, tableta, konzola lojrash, TV dhe laptopë si dhe kompjutera më tradicionalë. Kështu, përveç rasteve kur konteksti sugjeron ndryshe, çdo referencë në internet duhet të kuptohet për të përfshirë të gjitha këto metoda të ndryshme. Për të përfshirë ofrimet e pasura dhe komplekse të Internetit, 'Interneti dhe teknologjitë shoqëruese', 'TIK dhe industritë në internet' dhe 'Shërbimet e bazuara në Internet' përdoren në vend të njëjtë.

Njoftim dhe heqje

Operatorët dhe ofruesit e shërbimeve ndonjëherë njoftohen për përmbajtjen e të dyshuarve në internet nga klientët, anëtarët e publikut, organizatat e zbatimit të ligjit ose linjat telefonike. Procedurat e njoftimit dhe heqjes i referohen proceseve të një kompanie për heqjen e shpejtë të përmbajtjes së paligjshme (përmbajtja e paligjshme përcaktohet sipas juridiksionit) sapo të jenë bërë të ditur ('njoftuar') për praninë e këtyre përmbajtjeve në shërbimet e tyre.

Lojëra online

'Lojërat në internet' përcaktohet si luajtja e çdo lloj loje dixhitale komerciale me një ose me shumë lojtarë përmes çdo pajisjeje të lidhur me Internet, duke përfshirë konsolat e dedikuara, kompjuterët desktop, laptopët, tabletët dhe telefonat mobile.

Ekosistemi i lojërave në internet përcakton përfshirjen e procesit të shikimit të të tjerve duke luajtur video lojëra përmes e-sporteve, transmetimeve ose platformave të shpërndarjeve së videove, të cilat zakonisht ofrojnë mundësi për shikuesit për të komentuar ose ndërvepruar me lojtarët dhe anëtarët e tjerë të audiencës[37].

Mjetet e kontrollit prindëror

Program kompjuterik që lejon përdoruesit, zakonisht një prind, të kontrollojë disa ose të gjitha funksionet e një kompjuteri ose pajisjeve të tjera që mund të lidhen me internetin. Në mënyrë tipike, programe të tilla mund të kufizojnë hyrjen në lloje ose klasa të veçanta të faqeve të internetit ose shërbimeve online. Disa gjithashtu ofrojnë hapësirë për menaxhimin e kohës, d.m.th., pajisja mund të vendoset të ketë qasje në internet vetëm midis orëve të caktuara. Versione më të përparuara mund të regjistrojnë të gjitha tekstet e dërguara ose të marra nga një pajisje. Programet normalisht do të mbrohen me fjalëkalim[86].

[36] UNICEF and ITU, *Guidelines for Industry on Child Online Protection.*

[37] UNICEF, "Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry," DISCUSSION PAPER SERIES: Children's Rights and Business in a Digital World, 2019, https:// www .unicef -irc .org/ files/ upload/ documents/ UNICEF _CRBDigitalWorldSeriesOnline _Gaming .pdf. [86] UNICEF and ITU, *Guidelines for Industry on Child Online Protection.*

Prindërit, kujdestarët

Disa faqe në internet u referohen prindërve në mënyrë të përgjithshme (të tilla si në "faqen e prindërve" dhe i referohen "kontrolleve prindërore.") Prandaj mund të jetë e dobishme të përcaktohen njerëzit që në mënyrë ideale duhet të fuqizojnë fëmijët për të maksimizuar mundësitë e disponueshme në internet, të sigurohet që fëmijët dhe të rinjtë të përdorin faqet e internetit në mënyrë të sigurt dhe me përgjegjësi dhe të japin aprovimin e tyre për të pasur akses në faqet specifike të Internetit. Në këtë dokument, termi "prind" i referohet kujtdo (me përjashtim të edukatorëve) që ka një përgjegjësi ligjore për një fëmijë. Përgjegjësia prindërore ndryshon nga vendi në vend, po në të njejtën mënyrë dhe të drejtat ligjore të prindërve.

Informacion personal

Termi përshkruan informacione të identifikueshme individualisht për një person, të cilat mblidhen në internet. Këtu përfshihen emri i plotë, detajet e kontaktit si shtëpia dhe adresa e postës elektronike, numrat e telefonit, gjurmët e gishtave ose materiali për njohjen e fytyrës, numrat e sigurimit ose ndonjë faktor tjetër, që lejon kontaktin fizik ose në internet ose lokalizimin e një personi. Në këtë kontekst, ai i referohet më tej çdo informacioni në lidhje me një fëmijë dhe shoqërimin e tij ose të saj, informacion që mblidhet në internet nga ofruesit e shërbimeve të internetit, përfshirë lodrat e lidhura me internet dhe IoT dhe çdo teknologji tjetër të lidhur me internet.Privacy

Privacy is often measured in terms of sharing personal information online, having a public social media profile, sharing information with people they got to know online, using privacy settings, sharing passwords with friends, being concerned about privacy[38].

Ngacmimi nëpërmjet mesazheve

Ngacmimi nëpërmjet mesazheve zakonisht përcaktohet si dërgimi, marrja ose shkëmbimi i mesazheve me përmbajtje seksuale të vetë-prodhuar, duke përfshirë imazhe, mesazhe ose video përmes telefonave celularë dhe/ose internetit. Krijimi, shpërndarja dhe posedimi i imazheve seksuale të fëmijëve është i paligjshëm në shumicën e vendeve. Nëse zbulohen imazhe seksuale të fëmijëve, të rriturit nuk duhet t'i shohin ato. Shpërndarja e imazheve seksuale të një të rrituri me një fëmijë është gjithmonë një veprim kriminal dhe se mund t'u shkaktojë dëme dhe mund të nevojiten raportime dhe veprime për të hequr imazhe të shpërndara.Sextortion or sexual extortion of children

Sextortion përshkruan ose zhvatje seksuale (referuar gjithashtu si "detyrim dhe zhvatje seksuale në internet") "shantazh i një personi me ndihmën e imazheve të gjeneruara nga ai person në mënyrë që të përfitojë favore seksuale, para ose përfitime të tjera prej saj/tij nën kërcënimin e shpërndarjes së materialit përtej pëlqimit të personit që është shfrytëzuar (p.sh., postimi i imazheve në mediat sociale)".

The Internet of Things (IoT)

Internet of Things përfaqëson hapat e ardhshme drejt dixhitalizimit të ekonomisë dhe shoqërisë, ku objektet dhe njerëzit janë të ndërlidhur nëpërmjet rrjeteve të komunikimit dhe raportojnë për statusin e tyre dhe/ose të ambjentit rrethues[39].

[38] "Children's Online Privacy Protection Act," Pub. L. No. 15 U.S.C. 6501-6505 (1998), https:// uscode .house .gov/ view .xhtml ?req = granuleid %3AUSC -prelim -title15 -section6501& edition = prelim.

[39] Ntantko, The Internet of Things, 1 October 2013, Digital Single Market - European Commission, https:// ec .europa .eu/ digital -single -market/ en/ internet -of -things.

URL

Shkurtimi nënkupton 'uniform resource locator', adresën e një faqeje në Internet[40].

Realiteti virtual

Realiteti virtual është përdorimi i teknologjisë kompjuterike për të krijuar efektin e një bote tredimensionale interaktive, në të cilën objektet kanë një sens të prezencës hapësinore[41].

Wi-Fi

Wi-Fi (Wireless Fidelity) është një grup standardesh teknike që mundësojnë transmetimin e të dhënave nëpërmjet rrjetit wireless[42].

[40] UNICEF and ITU, *Guidelines for Industry on Child Online Protection*.

[41] NASA, "Virtual Reality," nas.nasa.gov, accessed January 16, 2020, https://w ww.nas. nas a.gov/S oftware /VWT/ vr .html.

[42] Children's Online Privacy Protection Act.

Aneksi 2: Kontaktoni veprat kundër fëmijëve dhe të rinjve

Fëmijët dhe të rinjtë mund të ekspozohen ndaj një sërë kontaktesh të padëshiruara ose të papërshtatshme në Internet që mund të ketë pasoja të tmerrshme për ta. Disa nga këto kontakte mund të jenë të natyrës seksuale.

Studimet kanë treguar se 22 përqind janë ngacmuar, ngacmuar ose ndjekur në internet; 24 përqind kanë marrë komente të padëshiruara seksuale; 8 përqind kanë takuar njerëz në jetën reale të cilët më parë i kishin njohur vetëm në internet. Megjithëse normat ndryshojnë nga vendi dhe rajoni, këto shifra tregojnë se rreziqet janë reale. Një studim në Internet në Shtetet e Bashkuara të Amerikës zbuloi se 32 përqind e adoleshentëve në internet janë kontaktuar nga një i panjohur plotësisht, nga ata, 23 përqind thanë se ndiheshin të frikësuar dhe të pakëndshëm gjatë kontaktit; dhe 4 për qind kishin marrë kërkesë agresive seksuale.

Grabitqarët seksualë përdorin internetin për të kontaktuar fëmijë dhe të rinj për qëllime seksuale, shpesh duke përdorur një teknikë të njohur si pastrim, përmes së cilës ata fitojnë besimin e fëmijës duke iu drejtuar interesave të tij ose të saj. Ata shpesh prezantojnë tema seksuale, foto dhe gjuhë të qartë për të desensibilizuar, për të rritur ndërgjegjësimin seksual dhe për të zbutur vullnetin e viktimave të tyre të reja. Dhuratat, paratë dhe madje biletat për transport përdoren për të bindur dhe joshur fëmijën ose të riun në një vend ku grabitqari mund ta shfrytëzojë atë seksualisht. Këto takime madje mund të fotografohen ose regjistrohen. Fëmijëve dhe të rinjve shpesh u mungon pjekuria emocionale dhe vetëvlerësimi, gjë që i bën ata të ndjeshëm ndaj manipulimeve dhe frikësimeve. Ata gjithashtu hezitojnë t'u tregojnë të rriturve për takimet e tyre nga frika e sikletit ose humbjes së hyrjes në internet. Në disa raste, ata kërcënohen nga grabitqarët dhe u thuhet të mbajnë sekret marrëdhënien. Grabitqarët seksualë gjithashtu mësojnë nga njëri-tjetri përmes forumeve në Internet dhe dhomave të bisedës.

Aneksi 3: Aleanca Globale WeProtect

Modeli Kombëtar i Përgjigjes WePROTECT

Strategjia e Aleancës Gobale WePROTECT (WPGA) mbështet vendet që të zhvillojnë përgjigjen e shumë palëve të përfshira për të mposhtur shfrytëzimin seksual të fëmijëve online, të udhëzuar nga Modeli Kombëtar i Përgjigjes (MNR). Modeli Kombëtar i Përgjigjes i WPGA funksionon si një blueprint për veprim kombëtar. Ai vë në përdorim një framework mbi të cilin çdo shtet operon për të mposhtur shfrytëzimin seksual të fëmijëve online (OCSE). Ky model përdoret për të ndihmuar një vend:

- të vlerësojë përgjigjen aktuale ndaj shfrytëzimit seksual të fëmijëve online dhe të identifikojë mangësitë;
- t'i japë prioritet përpjekjes kombëtare në rregullimin e këtyre mangësive;
- të rrisë mirëkuptimin dhe bashkëpunimin ndërkombëtar.

Modeli nuk ka si qëllim përcaktimin e aktivititeteve apo vendosjen e një qasjeje unike. Qëllimi i tij është të përshkruajë aftësitë që duhen për një mbrojtje efektive të fëmijëve dhe për të mbështetur vendet që të zhvillojnë ose rrisin aftësitë e tyre ekzistente. Ai gjithashtu liston një numër mundësuesish të cilët nëse përdoren në mënyrë efektive do të rrisin dhe përmirësojnë rezultatet. MNR përfshin 22 aftësi, të ndara në 6 seksione: politikë dhe ligjvënie, drejtësi kriminale, viktimë, shoqëria, industria dhe media dhe komunikimi. WPGA beson se bashkëveprimi i të gjashtë fushave do të sjellë një përgjigje kombëtare të përmbushur ndaj këtij krimi.

Modeli do t'i lejojë një vendi - pavarësisht pikënisjes - të identifikojë çdo mangësi në aftësi dhe të nisë rregullimin e këtyre mangësive. Pavarësisht se vendet do të zhvillojnë qasjet e tyre individuale, fakti që çdo gjë do të bëhet bazuar në një framework të pranuar unanimisht do të sjellë bashkëpunim midis palëve në nivel si kombëtar ashtu edhe ndërkombëtar.

Përgjigjia strategjike globale e WePROTECT

Përgjigjia strategjike globale (GSR) e Aleancës Globale WePROTECT është një qasje e koordinuar për luftën ndaj shfrytëzimit seksual të fëmijëve online duke përfshirë një vështrim global, një harmonizim ndërkombëtar, dhe zgjidhje globale që tejkalojnë përgjigjen kombëtare. GSR në pak fjalë është pjesa shoqëruese e Modelit të Përgjigjes Kombëtare (MNR); ndërsa MNR është i fokusuar në aftësitë e nevojshme për mposhtjen e shfrytëzimit seksual të fëmijëve online, GSR fokusohet në fushat prioritare për bashkëpunim ndërkombëtar.
GSR përfshin 6 fusha tematike, me aftësi të kërkuara dhe rezultate të pritura për secilën prej tyre, si dhe partnerët përtej kufjve të cilët duhet të punojnë sëbashku për të sjellë këto 6 fusha.

Politika dhe legjislacion

Zhvillimi i vullnetit politik për të ndërmarrë veprime dhe zhvillimi i legjislacionit që të harmonizojë në mënyrë efektive me qasjen ndaj veprave penale do të rezultojë në përtëritjen e angazhimit të lartë kombëtar dhe ndërkombëtar për të luftuar shfrytëzimin seksual të fëmijëve online.

Drejtësia kriminalistike

Ndarja e informacionit, përfshirë aksesin ndaj databazave ndërkombëtare nëpërmjet frameworkeve formale për shpërndarjen e të dhënave kombinuar me oficerë të trajnuar, të dedikuar dhe prokurorë me ekspertizë mbi shfrytëzimin seksual të fëmijëve online janë mënyra më e mirë për të identifikuar, ndjekur dhe kapur agresorët, duke përfshirë investigime dhe dënim në mënyrë të suksesshme.

Shërbimi ndaj viktimave

Mbështetja efektive dhe në kohë për viktimat, duke përfshirë ruajtjen e identitetit dhe amplifikimin e zërit të tyre, ndihmon në suportimin që i nevojitet viktimave, në kohën e duhur.

Teknologjia

Përdorimi i zgjidhjeve teknologjike, përfshirë Inteligjencën Artificiale, për të zbuluar, bllokuar dhe parandaluar materiale të dëmshme, live streaming dhe shfrytëzimin nga të rriturit online do t'i lejojë këtyre platformave të mos përdoren si një pajisje për shrytëzimin seksual të fëmijëve.

Shoqëria

Ka disa aftësi që punojnë sëbashku në shoqërinë e gjerë për t'u dhënë forcë fëmijëve që të vetëmbrohen nga shfrytëzimi seksual online, pavarësisht vendit ku jetojnë. Duke u siguruar që zhvillimi kulturor digjital ka karakteristika që mundësojnë sigurinë, dhe që ka një qasje etike dhe konsistente ndaj raportimit në media, ekspozimi ndaj materialeve të papërshtatshme online do të kufizohet. Ndërkohë, edukimi, informimi i fëmijëve, prindërve, kujdestarëve, dhe profesionistëve, si dhe ndërhyrjet ndaj agresorëve, punojnë të gjitha sëbashku për të ndaluar dukurinë e shfrytëzimit seksual të fëmijëve online.

Kërkime dhe njohuri

Si përfundim, llogaritja e rrezikut (si psh Llogaritja Globale e Rrezikut 2019), kërkime ndaj agresorëve dhe puna për të kuptuar trauma aftagjata te viktimat do t'i japin qeverive, zbatuesve të ligjit, shoqërisë civile, akademikëve dhe industrisë një mirëkuptim ndaj rreziqeve më të fundit.

Aneksi 4: Shembuj të përgjigjeve ndaj dëmeve në internet

Shembujt e përfshirë këtu janë përpiluar nga autorët dhe kontribuesit e udhëzimeve të ITU.

Edukimi i fëmijëve kundër dëmtimeve në internet

BBC Own IT App - një aplikacion i mirëqenë i cili ka si synim fëmijët e moshës 8-13 të cilët marrin smartphone-in e tyre të parë. Kombinimi i teknologjisë më të fundit për të mësuar makinerinë për të gjurmuar aktivitetin e fëmijëve në smartphone-in e tyre me aftësinë që fëmijët të vetë-raportojnë gjendjen e tyre emocionale, përdor këtë informacion për të dhënë përmbajtje të përshtatur dhe për të ndihmuar fëmijët të qëndrojnë të lumtur dhe të sigurtë në internet .

Duke shfaqur përmbajtje posaçërisht nga e gjithë BBC, aplikacioni ofron materiale dhe burime të dobishme për të ndihmuar të rinjtë të përfitojnë sa më shumë nga koha e tyre në internet dhe të ndërtojnë sjellje dhe zakone të shëndetshme në internet, duke ndihmuar të rinjtë dhe prindërit të kenë biseda më konstruktive në lidhje me përvojat e tyre në internet. Aplikacioni nuk mbledh të dhëna personale ose përmbajtje të gjeneruar nga përdoruesi pasi i gjithë mësimi i gjuhës makinë funksionon brenda aplikacionit dhe brenda pajisjes së përdoruesit.

Zhvillimi i Projektit – Kuadër arsimor me aftësi dixhitale dhe me burime të plota, duke identifikuar aftësitë digjitale për çdo moshë të fëmijëvë duke ndihmuar prindërit dhe mësuesit të kuptojnë aftësitë që duhet të kenë fëmijët e tyre, së bashku me burimet dhe aktivitetet që do t'u sigurojnë atyre me aftësitë e veçanta.

Siguria 360 gradë – Një mjet vetë-rishikimi në internet për shkollat në shqyrtimin dhe vlerësimit të të gjithë dispozitës së tyre të sigurisë në internet duke siguruar udhëzime dhe mbështetje për të marrë standarde të përcaktuara.

Instituti DQ – Të dhënat u mblodhën nga 145’426 fëmijë dhe adoleshentë në 30 vende nga 2017-2019 si pjesë e #DQEveryChild, një lëvizje globale e qytetarisë digjitale e mbështetur nga Instituti DQ,që filloi në Singapor me mbështetjen e Singtel dhe është zgjeruar shpejt në bashkëpunim me Forumin Ekonomik Botëror që përfshin mbi 100 organizata partnere. Kjo lëvizje synonte të fuqizonte fëmijët me kompetenca gjithëpërfshirëse të qytetarisë digjitale që nga fillimi i jetës së tyre digjitale duke përdorur programin online të arsimit dhe vlerësimit DQ World. Të dhënat nga kjo lëvizje u përdorën për të krijuar Indeksin e Sigurisë Online të Fëmijëve 2020 (COSI). Kuadri për COSI vlerëson dhe rendit sigurinë e fëmijëve në internet në 30 vende bazuar në 24 fusha të grupuara në gjashtë shtylla që ndikojnë në sigurinë në internet të fëmijëve.

Paketa e Gatishmërisë Familjare DQ Pro dhe DQ World ofrojnë mundësi për prindërit për të vlerësuar gatishmërinë dixhitale të fëmijës së tyre dhe, përmes materialeve arsimore, të përmirësojnë kompetencat dixhitale si shtetësia dixhitale, menaxhimi i kohës së ekranit, menaxhimi i ngacmimit kibernetik, menaxhimi i sigurisë kibernetike, ndjeshmëria dixhitale, menaxhimi i gjurmës dixhitale, mendimi kritik dhe menaxhimi i privatësisë.

Paketa eSafety për Shkollat e Australisë është një grup burimesh të dizenjuara për të mbështetur shkollat dhe për të krijuar nje mjedis më të sigurt në internet. Paketa e Veglave pasqyron një qasje

shumëplanëshe të edukimit mbi sigurinë në internet dhe është kategorizuar në katër elemente, që:

- përgatitja e shkollave për të vlerësuar gatishmërinë e tyre për t'u marrë me çështjet e sigurisë në internet dhe për të dhënë sugjerime për të përmirësuar praktikat e tyre aktuale;
- angazhoni të gjithë komunitetin shkollor për tu angazhuar dhe përfshirë në krijimin e një ambienti të sigurt në internet;
- edukimi duke theksuar praktikat më të mira në edukimin për sigurinë në internet dhe duke mbështetur shkollat për të zhvilluar aftësitë e sigurisë në internet të komunitetit shkollor;
- përgjigja e incidenteve në mënyrë efektive duke mbështetur sigurinë dhe mirëqenien.

Zyra e Komunikimeve Elektronike të Polonisë-UKE I Click Fushata arsimore e ndjeshme edukon fëmijët dhe prindërit se si të jenë më të sigurt në internet dhe si të njohin dhe të menaxhojnë rreziqet.

ChildFund Viet Nam themeloi nismën Swipe Safe. Ky program edukon fëmijët për rreziqet e mundshme në internet, të tilla si mashtrimet kibernetike, ngacmime ose abuzimi seksual dhe paraqet këshilla për metodat për të qëndruar të sigurt.

Raporti i Komisionit Broadband mbi Raportin e Komisionit Broadband në *Teknologjia, Broadband dhe Edukimi: avancimi i arsimit për të gjitha axhendat, 2013*, 2013.

Përvoja e Fëmijëve në Internet: Ndërtimi i Kuptimit dhe Veprimit Global, UNICEF, 2019.

Hulumtimi Global Kids Online përfshin shumë informacione në lidhje me përgjigjet e praktikave të mira për dëmet në internet.

Shembuj të industrisë angazhuese

Komisioneri Australian eSafety ndërton partneritete të forta dhe punon me industrinë për të ndihmuar të gjithë Australianët që të kenë përvoja më të sigurta dhe më pozitive në internet. Një shembull është puna eSafety për sigurinë sipas modelit. Si pjesë e nismës, eSafety zhvilloi një proces të hollësishëm konsultimi me industrinë, organet tregtare dhe organizatat me përgjegjësi për të mbrojtur përdoruesit, si dhe prindërit, kujdestarët dhe të rinjtë. Iniciativa e Sigurisë nga Projektimi është krijuar për të inkurajuar dhe ndihmuar industrinë për të siguruar sigurinë e përdoruesit të ngulitur në hartimin, zhvillimin dhe vendosjen e shërbimeve dhe platformave në internet. eSafety administron gjithashtu tre skema raportimi dhe ankesash: skema e ngacmimit në internet, skemat e abuzimit të bazuara në imazhe dhe skema e përmbajtjes në internet. eSafety mund të drejtojë zyrtarisht disa ofrues të shërbimeve në internet që të heqin përmbajtjen nga shërbimet e tyre. Ndërsa skemat veprojn kryesisht edhe një model bashkëpunues midis qeverisë dhe industrisë, fuqitë në dispozicion të eSafety për të detyruar heqjen e materialit sigurojnë një rrjet sigurie kritike dhe e shtyn industrinë të jetë proaktive në adresimin e dëmeve në internet.

Zyra e Komunikimeve Elektronike të Polonisë-UKE po përfshin shoqërinë civile dhe fëmijët në fushatat e tyre të avokimit për t'i bërë ata të kuptojnë se çfarë po nënshkruajnë në internet.

Fondacioni i Shikimit të Internetit është një organizatë partneriteti që bashkon industrinë, qeverinë, zbatimin e ligjit dhe OJQ-të për të ndaluar abuzimin seksual të fëmijëve. Në vitin 2020, IWF kishte 152 Anëtarë nëpër platforma dhe shërbime të infrastrukturës dhe u ofron Anëtarëve një sërë shërbimesh për të parandaluar përhapjen e imazheve kriminale në platformat e tyre.

Mbulimi i legjislacionit

Shprehni vullnetin politik për t'i dhënë përparësi COP duke nënshkruar Deklarata Universale e Sigurisë Online e Fëmijëve (Komisioni i brezit të gjerë).

Regullorja

Jashtë Hijeve: Reagimi ndaj abuzimit seksual dhe shfrytëzimit të fëmijëve (2019) nga The Economist Intelligence Unit është i vetmi mjet për shënjimin e stolit që analizon reagimin e vendeve ndaj abuzimit dhe shfrytëzimit seksual të fëmijëve, përfshirë hapësirën digjitale dhe përgjigjen e industrisë TIK tek ajo.

Identifikimi i abuzimit të fëmijëve në internet

Më poshtë janë shembuj të praktikave të mira në identifikimin e abuzimit të fëmijëve në internet.

INHOPE: Rrjeti INHOPE u formua në 1999 për të luftuar CSAM në internet dhe në përgjigje të një vizioni të përbashkët të një Interneti që nuk përmban materiale të abuzimit seksual të fëmijëve. Në 20 vitet e ndërhyrjes, INHOPE është rritur për të luftuar me sukses rritjen, përhapjen gjeografike dhe ashpërsinë e CSAM në internet. Sot linjat e nxehta INHOPE po punojnë në terren në çdo kontinent, duke marrë raporte dhe duke hequr me shpejtësi CSAM nga interneti, dhe duke shkëmbyer të dhëna me zbatuesit e ligjit.

Microsoft PhotoDNA krijon hashe të imazheve dhe i krahason ato me një bazë të dhënash të hasheve tashmë të identifikuar dhe konfirmuar të jenë CSAM. Nëse gjen një gabim, imazhi bllokohet. Sidoqoftë, ky mjet nuk përdor teknologji të njohjes së fytyrës, dhe as nuk mund të identifikojë një person ose objekt në figurë. Por, me shpikjen e PhotoDNA për Video, gjërat kanë marrë një kthesë të re.

PhotoDNA për Video zbërthen video në kornizat kryesore dhe në thelb krijon hashe për ato pamje ekrani. Në të njëjtën mënyrë që PhotoDNA mund të përputhet me një imazh që është ndryshuar për të shmangur zbulimin, PhotoDNA për Video mund të gjejë përmbajtje të abuzimit seksual të fëmijëve që është redaktuar ose bashkuar në një video që përndryshe mund të duket e padëmshme.

Microsoft ka lëshuar një mjet të ri për identifikimin e ngacmuesve të fëmijëve që i ngacmojnë fëmijët për t'i abuzuar në bisedat në internet. **Projekti Artemis,** zhvilluar në bashkëpunim me The Meet Group, Roblox, Kik dhe Thorn, bazohet në teknologjinë e patentuar në Microsoft dhe do të vihet në dispozicion lirisht përmes Thorn për kompanitë e shërbimit në internet që ofrojnë një funksion bisede. Projekti Artemis është një mjet teknik i cili ndihmon për të ngritur flamuj të kuq te Administratorët kur ndonjë moderim është i nevojshëm në dhomat e bisedës. Kjo teknikë e zbulimit të pastrimit do të jetë në gjendje të zbulojë, adresojë dhe raportojë ngacmuesit që përpiqen të joshin fëmijët për qëllime të këqia.

Thorn ka zhvilluar reklama parandaluese që synojnë ata që kërkojnë materiale të abuzimit seksual të fëmijëve, të cilat kanë shërbyer miliona herë katër motorë kërkimi për një periudhë tre vjeçare. Për më tepër, reklamat kanë parë një normë klikimi prej 3 përqind nga njerëzit që kërkojnë ndihmë pasi kanë kërkuar materiale të paligjshme.

Siguria e Thorn, një mjet që mund të vendoset direkt në një platformë të një kompanie private për të identifikuar, hequr dhe raportuar CSAM.

Drita Thorn, një software që i jep zbatimit të ligjit në të gjitha 50 shtetet në Shtetet e Bashkuara të Amerikës dhe në Kanada aftësinë për të përshpejtuar identifikimin e viktimës dhe për të zvogëluar kohën e hetimit me më shumë se 60 përqind.

Geebo, një faqe e klasifikuar dhe e angazhuar për të mbajtur shantazhet seksuale jashtë platformës së saj, nuk ka pasur kurrë raste që përfshin abuzimin seksual të fëmijëve. Ata arrijnë ta bëjnë këtë pjesërisht për shkak të procesit të tyre të para-shqyrtimit.

Google AI klasifikues mund të përdoret për të zbuluar materialin e abuzimit seksual të fëmijëve në rrjete, shërbime dhe në platforma. Ky mjet është i disponueshëm falas përmes **Google Content Security API**, i cili është një paketë mjetesh që rrit kapacitetin për të rishikuar përmbajtjen në një mënyrë që kërkon që më pak njerëz të ekspozohen ndaj tij. Ky mjet do të ndihmonte ekspertët njerëzorë të rishikonin materialin në një shkallë edhe më të madhe dhe të vazhdonin me shkelësit, duke synuar imazhe që nuk janë shënuar më parë si materiale të paligjshme. Ndarja e kësaj teknologjie do të shpejtonte identifikimin e imazheve qeë përdoret për të zbuluar materialin e abuzimit seksual të fëmijëve në rrjete, shërbime dhe në platforma.

Në vitin 2015, Google zgjeroi punën e tyre në hashe duke prezantuar teknologjinë e parë të llojit të saj të gjurmëve të gishtave dhe përputhjes për videot në **YouTube**, të cilat skanojnë dhe identifikojnë videot e ngarkuara që përmbajnë material të njohur të abuzimit seksual të fëmijëve.

Gjatë Hackathon të Sigurisë së Fëmijëve 2019, **Facebook** njoftoi burimin e hapur të dy teknologjive që zbulojnë foto dhe video identike dhe gati njelloj. Këto dy algoritme janë në dispozicion në GitHub që lejon sistemet e ndarjes së hashit të flasin me njëri-tjetrin, duke i bërë sistemet shumë më të fuqishme.

Linja e **IWF** mbetet gjithnjë vigjilente, jo vetëm duke ndjekur mijëra raporte nga anëtarët e publikut, të cilët mund të kenë rastisur në abuzimin seksual të fëmijëve në internet, por gjithashtu duke kryer një rol unik proaktiv të kërkimit të kësaj përmbajtje të paligjshme në internet. Duke fuqizuar linjat e nxehta për të përdorur informacionin e tyre dhe fokusin e burimeve, më shumë përmbajtje mund të identifikohet dhe hiqet. Për më tepër, IWF është duke punuar vazhdimisht me Google, Microsoft dhe Facebook dhe kompani të tjera brenda anëtarësimit të saj për të shtyrë vazhdimisht kufijtë teknikë. IWF ofron zgjidhjen e Portalit të Raportimit, që lejon përdoruesit e internetit në vende dhe kombe pa linja të nxehta, të raportojnë imazhe dhe video të abuzimit seksual të fëmijëve të dyshuar direkt në IWF përmes një faqe në internet të porositur.

IWF në bashkëpunim me organizatën bamirëse për mbështetjen e viktimave Marie Collins Foundation synon të krijojë një fushatë të re duke u bërë thirrje djemve të rinj të raportojnë çdo imazh seksual ose video të fëmijëve të moshës nën 18 vjeç që mund të pengohen gjatë shfletimit në internet.

Interpol ka krijuar një bazë të dhënash për imazhet dhe Abuzimit Seksual të Fëmijëve Ndërkombëtarë (ICSE), e cila është një mjet i inteligjencës dhe i hetimit, duke lejuar hetues të specializuar nga më shumë se 50 vende të ndajnë të dhëna për rastet e abuzimit seksual të fëmijëve. Duke analizuar përmbajtjen dixhitale, vizive dhe audio të fotografive dhe videove, ekspertët e identifikimit të viktimave mund të marrin të dhëna, të identifikojnë çdo mbivendosje në raste dhe të kombinojnë përpjekjet e tyre për të gjetur viktimat e abuzimit seksual të fëmijëve. Aktualisht, baza e të dhënave të Shfrytëzimit Seksual të Fëmijëve Interpol mban më shumë se 1.5 milion imazhe dhe video dhe ka ndihmuar në identifikimin e 19’400 viktimave në të gjithë botën.

Griffeye Brain përdor inteligjencën artificiale për të skanuar përmbajtjen e paklasifikuar më parë dhe për ta krahasuar atë me atributet e përmbajtjes së njohur CSAM dhe për të nënvizuar artikujt e dyshuar për rishikim nga një agjent.

RAINN krijoi dhe operon Linjën Kombëtare të Sulmit Seksual në partneritet me më shumë se 1 000 ofrues të shërbimeve të raportimit të sulmeve seksuale në të gjithë vendin dhe operon Linjën e Ndihmës së Sigurt **DoD** për Departamentin e Mbrojtjes. **RAINN** gjithashtu kryen programe për të parandaluar dhunën seksuale, për të ndihmuar viktimat dhe për të siguruar që autorët e krimit të sillen para drejtësisë.

Safehorizon është një organizatë jofitimprurëse për ndihmën ndaj viktimave dhe që mbështesin viktimat e dhunës dhe abuzimit në New York City që nga viti 1978. Safehorizon ofron shërbime të linjave të ndryahme për viktimat e dhunës.

Projecti Arachnid është një mjet inovativ i operuar nga Qendra Kanadeze, Projekti Arachnid për të luftuar përhapjen në rritje të materialit të abuzimit seksual të fëmijëve (CSAM) në internet.

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

With the support of:

International Telecommunication Union
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-30451-5

Published in Switzerland

Geneva, 2020 Photo credits: Shutterstock