Смернице за ИКТ компаније у погледу безбедности деце на интернету 2023.

паметно и безбедно 19833

Смернице за ИКТ компаније у погледу безбедности деце на интернету

Признања

Ове смернице су развиле Међународна унија за телекомуникације (ИТУ) и радна група аутора који су дали допринос, а долазе из водећих институција активних у сектору информационих и комуникационих технологија (ИКТ), као и на питањима заштите деце, а укључују ЕБУ, Глобално партнерство за заустављање насиља над децом, ГСМА, Међународна алијанса за особе са инвалидитетом, The Internet Watch Foundation (IWF), Privately SA и УНИЦЕФ. Радном групом предсједао је Ањан Босе (УНИЦЕФ), а координисала је Fanny Rotino (ИТУ).

Ове смернице ИТУ-а не би биле могуће без времена, ентузијазма и преданости аутора који су дали свој допринос. Непроцењиве доприносе такође су дали e-Worldwide Group (e-WWG), Facebook, Tencent Games, Twitter, компанија Walt Disney, као и друге интересне стране у ИКТ индустрији, којима је заједнички циљ да учине интернет бољим и безбеднијим местом за децу и младе. ИТУ је захвалан следећим партнерима који су дали своје драгоцено време и увиде (наведени по абецедном реду организација):

- Giacomo Mazzone (ЕБУ)
- Salma Abbasi (e-WWG)
- David Miles i Caroline Hurst (Facebook)
- Amy Crocker i Serena Tommasino (Глобално партнерство за заустављање насиља над децом)
- Jenny Jones (ГСМА)
- Lucy Richardson (Међународна алијанса за особе са инвалидитетом - ИДА)
- Fanny Rotino (ИТУ)
- Tess Leyland (IWF)
- Deepak Tewari (Privately SA)
- Adam Liu (Tencent Games)
- Katy Minshall (Twitter)
- Anjan Bose, Daniel Kardefelt Winther, Emma Day, Josianne Galea Baron, Sarah Jacobstein и Steven Edwin Vosloo (УНИЦЕФ)
- Amy E. Cunningham (Компанија Walt Disney)

ИСБН

978-92-61-30081-4 (Штампана верзија)

978-92-61-30411-9 (Електронска верзија)

978-92-61-30071-5 (ЕПУБ верзија)

978-92-61-30421-8 (Моби верзија)

Молимо вас да узмете у обзир природну околину пре него што одштампате овај извештај.

Предговор

Експлозија дигиталних технологија створила је без преседана могућности за децу и младе да комуницирају, повезују се, деле, уче, приступају информацијама и изражавају своје мишљење о питањима која утичу на њихов живот и њихове заједнице.

Али шири и доступнији приступ услугама на интернету такође представљају значајне изазове за дечију безбедност и добробит - како на интернету тако и ван њега. Од питања приватности, вршњачког насиља и насилног и/или непримереног садржаја за одређени узраст, до превараната на интернету и злочина над децом као што су врбовање, сексуално злостављање и искоришћавање на интернету, данашња деца суочена су са многим ризицима. Претње се умножавају, а починиоци све више истовремено делују преко граница, што њихово праћење чини тешким, а још теже их је процесуирати.

Уз то, глобална пандемија вируса Ковид-19 забележила је пораст броја деце која су се први пут придружила свету на интернету, да би подржала своје студије и одржала социјалну интеракцију. Због ограничења која је наметнуо вирус не само да су млађа деца започела интеракцију на интернету много раније него што су њихови родитељи могли да планирају, већ је потреба за усклађивањем радних обавеза многим родитељима онемогућила надзор над њиховом децом, стављајући младе људе у ризик да приступе непримереном садржају или да буду на мети криминалаца у производњи материјала сексуалног злостављања деце (ЦСАМ).

Криминалци профитирају од технолошког напретка, као што су међусобно повезивање апликација и игара, брзо дељење датотека, пренос уживо, крипто валуте, Dark Web и снажни софтвери за шифровање. Међутим, они такође профитирају од често некоординисаног и неодлучног деловања технолошког сектора у циљу ефикасне борбе против проблема.

Технологије у настајању могу да буду део решења, на пример Интерполова база података о сексуалном злостављању деце заснована на вештачкој интелигенцији која користи софтвер за поређење слика и видео-записа за брзо успостављање веза између жртава, насилника и места. Али сама технологија неће решити проблем.

Да би се смањили ризици дигиталне револуције и дала могућност све већем броју младих да искористе њене предности, заједнички и координисани одговор више интересних страна никада није био битнији. Владе, цивилно друштво, локалне заједнице, међународне организације и интересне стране у ИКТ индустрији морају да се окупе ради заједничког циља.

Препознавши то, 2018. године државе чланице ИТУ затражиле су свеобухватно ажурирање наших смерница у погледу безбедности деце на интернету. Ове нове ИТУ смернице су преиспитане, поново написане и преобликоване да би одражавале врло значајне помаке у дигиталном крајолику у којем се деца ове генерације налазе. Поред тога што се бави новим достигнућима у дигиталним технологијама и платформама, ово ново издање бави се и важном празнином: ситуацијом са којом се суочавају деца са инвалидитетом, за коју свет на интернету нуди посебно пресудан спас за пуно и испуњено друштвено учествовање.

Технолошка индустрија има пресудну и проактивну улогу у успостављању основа за безбеднију и заштићенију употребу интернет услуга и других технологија за данашњу децу и будуће генерације.

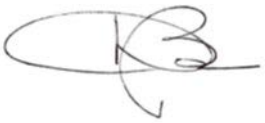
Предузеће мора све више стављати дечије интересе у средиште свог рада, обраћајући посебну пажњу на заштиту приватности личних података младих корисника, чувајући њихово право на слободу изражавања, борећи се против растуће пошасти материјала сексуалног злостављања деце и обезбеђујући да постоје системи који ефикасно решавају повреде дечијих права када се догоде.

Тамо где домаћи закони још увек нису сустигли међународно право, свако предузеће има прилику - и одговорност - да своје оперативне оквире усклади са највишим стандардима и најбољом праксом.

Надамо се да ће ове смернице ИКТ компанијама послужити као чврст основ на којем ће се развијати пословне политике и иновативна решења. У правом духу улоге ИТУ-а као глобалног сазивача, поносна сам на чињеницу да су ове смернице производ заједничких глобалних напора и да су у њиховој изради учествовали стручњаци из широке међународне заједнице као коаутори.

Такође ми је драго да представим нашу нову маскоту заштите деце на интернету Санга: пријатељски настројеног и неустрашивог лика којег је у потпуности дизајнирала група деце као део ИТУ-овог новог међународног програма информисања младих.

У доба када све више младих људи користи интернет, ИТУ смернице за заштиту деце су важније него икад. ИКТ компаније, владе, родитељи и едукатори, као и сама деца, сви имају виталну улогу. Захвална сам, као и увек, на вашој подршци и радујем се наставку наше блиске сарадње по овом критичном питању.



Дорин Богдан-Мартин
Директорица Бироа за развој
телекомуникација, ИТУ

Садржај

Табела

1. Преглед

Сврха овог документа је да пружи смернице интересним странама ИКТ компанија да изграде властите ресурсе за заштиту деце на интернету (ЦОП). Циљ ових смерница за ИКТ компаније у погледу безбедности деце на интернету је пружити користан, флексибилан и једноставан за коришћење оквир за визије предузећа и њихову одговорност да заштите кориснике. Оне су такође усмерене на стварање основа за безбеднију и заштићенију употребу интернетских услуга и сродних технологија за данашњу децу и будуће генерације.

Као алат, ове смернице такође имају за циљ јачање пословног успеха помажући великим и малим предузећима и интересним странама да развију и одржавају атрактиван и одржив пословни модел, уз разумевање правне и моралне одговорности према деци и друштву.

Као одговор на значајан напредак у технологији и спајању, ИТУ, УНИЦЕФ и партнери за заштиту деце на интернету развили су и ажурирали смернице за широк спектар компанија које развијају, пружају или користе телекомуникације или сродне активности у испоруци својих производа и услуга.

Нове смернице за ИКТ компаније у погледу безбедности деце на интернету резултат су консултација са члановима Иницијативе за заштиту деце на интернету, као и ширих консултација са члановима цивилног друштва, привреде, академске заједнице, влада, медија, међународних организација и младих.

Сврха овог документа је да:

- успостави заједничку референтну тачку и смернице за ИК технологије и интернетску индустрију и релевантне интересне стране;
- пружи смернице компанијама о идентификацији, спречавању и ублажавању било каквих негативних утицаја њихових производа и услуга на дечија права;
- пружи смернице компанијама о утврђивању начина на које могу да промовишу дечија права и одговорно дигитално грађанство међу децом;
- предложи заједничке принципе који чине основ националних или регионалних обавеза у свим сродним индустријама, имајући на уму да ће се различите врсте предузећа користити различитим моделима имплементације.

Обим

Заштита деце на интернету је сложен изазов који укључује више различитих управљачких, политичких, оперативних, техничких и правних аспеката. Ове смернице покушавају да реше, организују и одреде приоритете за многа од ових подручја, на основу постојећих и добро познатих модела, оквира и других референци.

Смернице се фокусирају на заштиту деце у свим подручјима и од свих ризика дигиталног света и, као такве, истичу добру праксу интересних страна у ИКТ индустрији коју компаније могу узети у обзир у процесу израде, развоја и управљања политикама заштите деце на интернету. Оне наводе актере у ИКТ индустрији не само о томе како управљати и обуздати незаконите активности на интернету против којих су они дужни да делују (попут материјала сексуалног злостављања деце на интернету) путем својих услуга, већ се такође фокусирају и на друга питања која не могу да се дефинишу као кривична дела у свим надлежностима. То укључује насиље међу вршњацима, сајбер малтретирање и узнемиравање на интернету, као и питања која се односе на приватност или општу добробит, превару или друге претње, које у одређеном контексту могу да буду штетне за децу.

У ту сврху ове смернице укључују препоруке о доброј пракси у отклањању ризика са којима се деца суочавају у дигиталном свету и како поступати у циљу успостављања безбедног окружења за децу на интернету. Ове смернице дају савете о томе како ИКТ компаније могу да раде на обезбеђењу дечије безбедности приликом коришћења ИК технологија, интернета или било које повезане технологије или уређаја који се на њега могу повезати, укључујући мобилне телефоне, конзоле за играње, играчке повезане с интернетом, сатове, интернет ствари и системе вођене вештачком интелигенцијом. Стога пружају преглед кључних питања и изазова у вези са заштитом деце на интернету и предлажу акције за предузећа и интересне стране за развој локалних и унутрашњих политика заштите деце на интернету. Ове смернице не покривају аспекте као што су стварни процес развоја или текст који би политике ИКТ компанија у вези са заштитом деце на интернету могле да обухвате.

Структура

Одељак 1 - Преглед: Овај одељак истиче сврху, обим и циљну публику ових смерница.

Одељак 2 - Увод у заштиту деце на интернету: Овај одељак даје преглед питања заштите деце на интернету, наводећи неке основне информације, укључујући посебну ситуацију деце са инвалидитетом. Штавише, пружа примере постојећих међународних и националних модела за заштиту деце на интернету као могуће области интервенције за интересне стране у ИКТ индустрији.

Одељак 3 – Кључна подручја заштите и промоције дечијих права: Овај одељак наводи пет кључних подручја у којима компаније могу да предузмумере да би обезбедиле деци безбедну и позитивну употребу ИК технологија.

Одељак 4 – Опште смернице: Овај одељак даје препоруке свим интересним странама у ИКТ индустрији у погледу дечије безбедности приликом употребе ИК технологија и промоцији позитивне употребе ИК технологија, укључујући одговорно дигитално друштво међу децом.

Одељак 5 - Контролна листа у вези са карактеристикама: Овај одељак истиче посебне препоруке за интересне стране о конкретним акцијама за поштовање и подршку дечијим правима, са следећим карактеристикама:

- Карактеристика А: Обезбедити повезивање, услуге складиштења података и хостинга
- Карактеристика Б: Понудити уређени дигитални садржај
- Карактеристика Ц: Хостовати садржај који генеришу корисници и повезани корисници
- Карактеристика Д: Системи вођени вјештачком интелигенцијом

Циљана публика

Надовезујући се на Водеће принципе Уједињених нација о пословању и људским правима,[1] дечија права и пословни принципи позивају предузећа да испуне своју одговорност да поштују дечија права избегавањем било каквих негативних утицаја повезаних са њиховим пословањем, производима или услугама. Ови принципи такође артикулишу разлику између поштовања (минимума који је потребан предузећу да би се избегло наношење штете деци) и подршке (на пример, предузимањем добровољних акција којима се жели унапредити остваривање дечијих права). Предузећа треба да обезбеде дечија права како на заштиту на интернету, тако и на приступ информацијама и слободу изражавања, истовремено промовишући позитивну употребу ИК технологија од стране деце.

[1] Водећи принципи Уједињених нација о пословању и људским правима.

Традиционалне разлике између различитих делова индустрије телекомуникација и мобилне телефоније, као и интернет компанија и емитера, брзо се руше и постају нејасне. Спајање увлачи ове претходно различите дигиталне токове у једну струју која досеже милијарде људи у свим деловима света. Сарадња и партнерство су основе успостављања темеља за заштићенију и безбеднију употребу интернета и повезаних технологија. Владе, приватни сектор, креатори политика, едукатори, цивилно друштво, родитељи и старатељи имају виталну улогу у постизању овог циља. ИКТ индустрија може да делује у пет кључних подручја, како је описано у одељку 3.

2. Шта је заштита деце на интернету?

Током последњих 10 година, употреба и улога интернета у животима људи знатно су се променили. Захваљујући распрострањености паметних телефона и таблета, доступности Wi-Fi и 4Г технологије и развоју платформи друштвених медија и апликација, све више људи приступа интернету из све већег броја разлога.

У 2019. години више од половине светске популације користило је интернет. Највећи део корисника су људи млађи од 44 године, са подједнаком употребом интернета између корисника од 16. до 24. године и од 35. до 44. године. На глобалном нивоу, сваки трећи корисник интернета је дете (0-18 година), а УНИЦЕФ процењује да је 71% младих већ на интернету.[2] Ширење приступних тачака интернету, мобилне технологије и све већег спектра уређаја са могућношћу приступа интернету, у комбинацији са огромним ресурсима који се могу наћи у сајбер простору, пружају невиђене могућности за учење, дељење и комуникацију.

Предности употребе ИК технологија укључују шири приступ информацијама о социјалним услугама, образовним ресурсима и здравственим саветима. Док деца и млади и породице користе интернет и мобилне телефоне да траже информације и помоћ и пријављују случајеве злостављања, ове технологије могу да помогну у заштити деце и младих од насиља и искоришћавања. Провајдери услуга дечије заштите такође користе ИК технологије за прикупљање и пренос података, што олакшава регистрацију рођења, вођење случајева, тражење породице, прикупљање података и мапирање насиља, између осталог.

Штавише, интернет је повећао приступ информацијама у свим крајевима света, омогућавајући деци и младима да истражују готово било коју тему од интереса, приступе свјетским медијима, истражују пословне могућности и прикупљају идеје за будућност. Употреба ИК технологија омогућава деци и младима да остваре своја права и изразе своја мишљења, а такође им омогућава да се повежу и комуницирају са својим породицама и пријатељима. ИК технологије такође служе као најважнији начин културне размене и извор забаве.

Упркос дубоким предностима интернета, деца и млади се такође могу суочити с низом ризика када користе ИК технологије. Могу да буду изложени неприкладном садржају или неприкладном контакту, укључујући потенцијалне починиоце сексуалног злостављања. Они могу да претрпе репутацијску штету због објављивања осетљивих личних података или на интернету или путем "секстинга", често не успевајући да схвате импликације својих поступака на себе и

[2] ОЕЦД, “Нове технологије и деца 21. вијека: Најновији трендови и исходи”, Образовни радни документ бр. 179.

друге и њихове дугорочне „дигиталне отиске“. Такође се суочавају са ризицима повезаним с приватношћу на интернету који произлазе из прикупљања података, прикупљања и коришћења информација о локацији.

Конвенција о правима детета, која је најратификованији међународни уговор о људским правима,[3] утврђује грађанска, политичка, економска, социјална и културна права деце. Њиме се утврђује да сва деца и млади имају право на образовање; разоноду, игру и културу; одговарајуће информације; слободу мисли и изражавања; и приватност, као и да изразе своје ставове о питањима која утичу на њих у складу са њиховим развојним капацитетима. Конвенција такође штити децу и младе од свих облика насиља, искоришћавања, злостављања и дискриминације било које врсте, и утврђује да би најбољи интерес детета требало да буде примарна брига у свим питањима која утичу на њих. Родитељи, старатељи, едукатори и чланови заједнице, укључујући вође заједнице и актере цивилног друштва, имају одговорност да његују и подржавају децу и младе у њиховом преласку у одрасло доба. Владе имају важну улогу у обезбеђивању да све такве интересне стране испуне ту улогу.

Што се тиче заштите дечијих права на интернету, ИКТ компаније морају заједно да раде на постизању пажљиве равнотеже између права деце на заштиту и права на приступ информацијама и слободе изражавања. Компаније би зато требало да дају приоритет мерама за заштиту деце и младих на интернету које су циљане и које нису претерано рестриктивне, ни за дете ни за друге кориснике. Штавише, све је већи консензус да би промоција дигиталног грађанства међу децом и младима, и развој производа и платформи који олакшавају деци позитивну употребу ИК технологија, требало да буде приоритет приватног сектора.

Иако интернет технологије деци и младима нуде бројне могућности за комуникацију, учење нових вештина, креативност и допринос за побољшање друштва за све, оне такође могу да представљају нове ризике за безбедност деце и младих. Могу да изложе децу и младе потенцијалним ризицима и штетама у вези са питањима приватности, незаконитог садржаја, узнемиравања, сајбер малтретирања, злоупотребе личних података или вербовања у сексуалне сврхе, па чак и сексуалног злостављања и искоришћавања деце. Могу да буду изложени и репутацијској штети, укључујући „осветничку порнографију“ повезану с објављивањем осетљивих личних података или на интернету или путем „секстинга“, што је начин на који корисници шаљу сексуално експлицитне поруке, фотографије или слике између мобилних телефона. Они се такође суочавају са ризицима з вези са приватношћу на интернету када користе интернет. деца, по природи својих година и зрелости, често нису у стању у потпуности да ухвате ризике повезане са интернетским светом и могуће негативне последице за друге и себе због свог непримереног понашања.

Упркос предностима, постоје и недостаци у употреби нових и напреднијих технологија. Развој вештачке интелигенције и машинског учења, виртуелне и проширене стварности, великих података, роботике и интернета ствари има за циљ да још више трансформише медијску праксу деце и младих. Иако се ове технологије претежно развијају да би проширile обим пружања услуга и побољшале погодност (путем, на пример, гласовне помоћи, приступачности и нових облика дигиталног урањања), неке такве технологије могу да имају ненамерне последице, па чак и да их злостављачи деце користе да служе њиховим потребама. Стварање заштићеног и безбедног интернет окружења за децу и омладину захтева ефикасно учествовање влада, приватног сектора и свих интересних страна. Фокусирање на дигиталне вештине и писменост родитеља и едукатора такође мора да буде један од првих циљева, у чијем постизању ИКТ компаније могу да имају виталну и одрживу улогу.

[3] Конвенција о правима детета УН-а. Све земље осим три (Сомалија, Јужни Судан и Сједињене Америчке Државе) ратификовале су Конвенцију о правима детета.

Нека деца можда добро разумеју ризике на интернету и како на њих одговорити. Међутим, то се не може рећи за сву децу свуда, посебно међу рањивим групама. Према циљу 16.2 Циљева одрживог развоја Уједињених нација - зауставити злостављање, експлоатацију, трговину људима и све облике насиља и мучења над децом, заштита деце на интернету је од виталног значаја.

Од 2009. године, Иницијатива заштите деце на интернету, међународна акција са више интересних страна коју је покренуо ИТУ, има за циљ подизање свести о ризику за децу на интернету и да одговори на те ризике. Иницијатива окупља партнере из свих сектора глобалне заједнице да би деци свуда обезбедило безбедно интернет искуство. Као део Иницијативе, ИТУ је 2009. године објавио сет смерница за заштиту деце на интернету за четири групе: децу, родитеље, старатеље и едукаторе, ИКТ компаније, и креаторе политика. Заштита деце на интернету подразумева се у овим смерницама као свеобухватан приступ да се одговори на све потенцијалне претње и штете са којима се деца и млади могу да суоче било на интернету или на некој од интернетских технологија. У овом документу заштита деце на интернету такође укључује штету нанету деци која се догоди ван интернета, али је повезана са доказима о насиљу и злостављању на интернету. Поред разматрања дечјег понашања и активности деце на интернету, заштита деце на интернету такође се односи на злоупотребу технологије од стране особа које нису деца ради искоришћавања деце.

Све релевантне интересне стране имају улогу у помагању деци и младима да имају користи од могућности које интернет пружа, док стичу дигиталну писменост и отпорност у погледу њихове добробити и заштите на интернету.

Заштита деце и младих заједничка је одговорност свих интересних страна. Да би се то догодило, креатори политика, ИКТ компаније, родитељи, старатељи, едукатори и друге интересне стране, морају да обезбеде да деца и млади могу да остваре свој потенцијал - на интернету и ван њега. Иако не постоји универзална дефиниција, заштита деце на интернету има за циљ целовит приступ изградњи безбедних, прикладних за све узрасте, инклузивних и партиципативних дигиталних простора за децу и младе, које карактеришу:

- реаговање, подршка и самопомоћ у случају суочавања са претњама;
- спречавање штета;
- динамичан баланс између обезбеђења заштите и пружања могућности деци да буду дигитални грађани;
- подржавање права и одговорности и деце и друштва.

Штавише, због брзог напретка у технологији и друштву и безграничне природе интернета, заштита деце на интернету мора да буде агилна и прилагодљива да би била ефикасна. Развојем технолошких иновација појавиће се нови изазови који ће се разликовати од регије до регије. Најбоље ће се изаћи на крај са њима заједничким радом у виду глобалне заједнице, јер треба пронаћи нова решења за те изазове.

2.1 Основне информације

Пошто је интернет у потпуности интегрисан у животе деце и младих, немогуће је посматрати одвојено дигитални и физички свет.

Таква повезаност изузетно оснажује. свет интернета омогућава деци и младима да преброде недостатке и инвалидитет, а пружио је нова места за

забаву, образовање, учествовање и изградњу односа. Данашње дигиталне платформе се користе за разне активности и често су мултимедијална искуства.

Приступ и учење коришћења и навигације овом технологијом сматра се пресудним за развој младих људи и ИК технологије се први пут користе у раном узрасту. Зато је пресудно да сви актери буду свесни да деца и млади људи често почињу да користе платформе и услуге пре него што достигну дефинисану минималну старосну границу које се технолошка индустрија мора придржавати, па би зато образовање уз мере заштите требало интегрисати у све интернет услуге које користе деца.

2.1.1 Деца у дигиталном свету

Приступ интернету

У 2019. години више од половине светске популације користило је интернет (53.6 посто), са процењених 4.1 милијарду корисника. На глобалном нивоу, сваки трећи корисник интернета је дете млађе од 18 година[1]. Према УНИЦЕФ-у, широм света 71% младих већ је на интернету[2]. Упркос захтевима минималне старосне границе, Ofcom (Регулатор за комуникације Велике Британије) процењује да готово 50% деце између 10 и 12 година већ има профил на друштвеним мрежама.[3] Деца и млади људи сада су значајно, трајно и доследно присутни на интернету. Интернет служи у друге друштвене, економске или политичке сврхе и постао је породични или потрошачки производ или услуга која је саставни део начина на који породице, деца и млади живе свој живот.

У 2017. години, на регионалном нивоу, приступ интернету за децу и младе био је чврсто повезан са нивоом националног дохотка. Земље са ниским приходима имају тенденцију да имају мање деце корисника интернета него земље са високим приходима. деца и млади у већини земаља викендом проводе више времена на интернету него радним даном, а адолесценти од 15 до 17 година проводе највише времена на интернету, у просеку између 2,5 и 5,3 сати, у ~~зависности од~~ земље.

[1] Livingstone, S., Carr, J., и Byrne, J. (2015) Свако треће: *Задатак за глобално управљање интернетом у решавању дечијих права.* Глобална комисија за управљање интернетом: Paper Series. London: CIGI i Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

[2] Комисија за широкопојасни приступ, „безбедност деце на интернету: Смањење ризика од насиља, злостављања и искоришћавања на интернету (2019)," *Комисија за широкопојасни приступ за одживи развој,* октобар 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

[3] ББЦ, "Употреба социјалних медија од стране малољетника 'расте', каже Ofcom ".

Употреба интернета

Међу децом и младима најпопуларнији уређај за приступ интернету је мобилни телефон, а следе га стони рачунари и лаптопи. деца и млади проводе у просеку два сата дневно на интернету у току седмице и четири сата сваког дана викенда. Док се неки осећају трајно повезанима, многи други још увек немају приступ интернету код куће. У пракси већина деце и младих који користе интернет имају приступ путем више уређаја, а они који се барем једном недељно повезују понекад користе и до три различита уређаја. Старија деца и деца у богатијим земљама углавном користе више уређаја, а дечаци користе нешто више уређаја него девојчице у свим анкетираним земљама.

Најпопуларнија активност - и за девојчице и за дечаке је гледање видео-клипова. Више од три четвртине деце и младих који користе интернет кажу да видео-клипове гледају на интернету барем једном седмично, било сами или с другим члановима своје породице. Многа деца и млади људи могу се сматрати 'активним социјализаторима' користећи неколико платформи друштвених медија као што су Facebook, Twitter, TikTok или Инстаграм. Деца и млади се такође баве политиком путем интернета и њихов глас се чује путем блогова.

Укупни ниво учешћа у игрању на интернету разликује се од земље до земље и приближно је у складу са лакоћом приступа интернету за децу и младе. Међутим, доступност и приступачност игара на интернету брзо се мењају, а старосна граница деце и младих који први пут приступају играма на интернету се смањује.

Недељно се 10%-30% деце и младих који се користе интернетом - која су консултована у одабраном низу земаља - бави креативним активностима на интернету.[1] У образовне сврхе, многа деца и млади свих узраста користе интернет за израду домаћих задатака, или чак да надокнаде градиво након пропуштених предавања или потраже здравствене информације на интернету сваке седмице. Чини се да старија деца имају већи апетит за информацијама од млађе деце.

[1] Livingstone, S., Kardefelt Winther, D., и Hussein, M. (2019.). Глобал Кидс Онлајн упоредни извештај о истраживању Innocenti. УНИЦЕФ-ова канцеларија за истраживање - Innocenti, Firenca, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html.

Сексуално искоришћавање и злостављање деце на интернету

Сексуално искоришћавање и злостављање деце (ЦСЕА) на интернету расте запањујућом брзином. Пре десет година било је мање од милион досијеа материјала о злостављању деце. У 2019. тај број се попео на 70 милиона, што је скоро 50% више у односу на бројке из 2018. године. Поред тога, први пут су видео-записи злостављања премашили број фотографија у пријавама надлежним органима, што показује потребу за новим алатима за суочавање са овим трендом. Жртве сексуалног искоришћавања и злостављања деце на интернету припадају свим старосним групама, али постају све млађе. Године 2018. мрежа линија за подршку INHOPE забележила је промену профила жртава са пубертетских на предпубертетске. Поред тога, истраживање ЕЦПАТ International-а и ИНТЕРПОЛ-а у 2018. години показало је да су млађа деца била подложнија да буду подвргнута тешком злостављању, укључујући мучење, насилно силовање или садизам. То укључује новорођенчад која су стара само неколико дана, седмица или месеци. Иако су девојчице погођеније, злостављање дечака може бити теже. Исти извештај показује да су 80% жртава о којима се говори у извештајима биле девојчице, а 17% дечаци. Деца оба пола наведена су у 3% процењених извештаја.[1]

Снимак података[2]

- Сваки трећи корисник интернета широм света је дете.
- Сваке пола секунде једно дете први пут иде на интернет.
- 800 милиона деце користи друштвене медије.
- Процењује се да у једном тренутку 750.000 појединаца на интернету жели да се повеже са децом у сексуалне сврхе.
- У спремишту ЕУРОПОЛ-а налази се више од 46 милиона јединствених слика или видео-записа материјала сексуалног злостављања деце.
- Више од 89% жртава је узраста између 3 и 13 година.

За више информација о обиму и реакцијама на сексуално искоришћавање и злостављање деце на интернету погледајте Глобални савез WeProtect.

[1] ЕЦПАТ и Интерпол, "У сусрет глобалном показатељу о неидентификованим жртвама у материјалу сексуалног искоришћавања деце: сажети извештај", 2018.
[2] Заустављање насиља над децом, "безбедни на интернету".

2.1.2 Утицај различитих платформи на дечије дигитално искуство

Интернет и дигитална технологија деци и младима представљају и могућности и ризике. Неки од њих наведени су у наставку.

Када деца користе **друштвене медије**, имају користи од многих прилика за истраживање, учење, комуникацију и развијање кључних вештина. Деца друштвене мреже виде као платформе које им омогућавају да истражују своје личне идентитете у безбедном окружењу. Имати одговарајуће вештине и знати како решити питања у вези са приватношћу и репутацијом важно је за младе људе.

"Знам да све што објавите на интернету остаје ту заувијек и да то може да утиче на ваш живот у будућности", дечак који има 14 година, Чиле.

Међутим, с обзиром на то да истраживања показују да већина деце користи друштвене медије пре навршених тринаест година, а услуге провере годишта су углавном слабе или их нема, ризици са којима се деца могу да сусрену могу да буду веома велики. Даље, док деца желе да науче дигиталне вештине, да постану дигитални грађани и да контролишу поставке приватности, они обично размишљају о приватности у односу на своје пријатеље и познанике - „Шта могу да виде моји пријатељи?“ - а мање у односу на странце и треће стране. Ово, у комбинацији са дечијом природном знатижељом и уопштено са нижим прагом страха од ризика, може да их учини рањивим на вербовање, искоришћавање, малтретирање или друге врсте штетног садржаја или контаката.

Раширена популарност размене слика и видео-записа путем мобилних апликација, а посебно коришћење платформи за стримовање уживо од стране деце представља даљњу забринутост у вези са приватношћу и ризиком. Нека деца стварају сексуалне слике себе, пријатеља, браће и сестара и деле их на интернету. У 2019. години готово трећина (29%) свих интернет страница с натписом IWF садржавале су самостално генерисане слике. Од тога је 76% показивало девојке узраста од 11 до 13 година, већином у својим спаваћим собама или другим собама у кућном окружењу. За неку, посебно старију децу, то може да се сматра природним истраживањем сексуалности и сексуалног идентитета, док за другу, посебно млађу децу, често постоји присила одрасле особе или другог детета. Без обзира на случај, резултирајући садржај је у многим земљама незаконит и може да изложи децу ризику од кривичног гоњења или може да се користи за даљње искоришћавање детета, вербовање или изнуђивање.

Слично томе, **игре на интернету** омогућавају деци да испуне своје основно право на игру, као и да граде мреже, проводе време са пријатељима и упознају нове пријатеље и развијају важне вештине. Иако ово може да буде веома позитивно, у неким случајевима, и ако нема надзора и подршке одговорне одрасле особе, платформе за игре такође могу да представљају ризик за децу. То укључује претерано играње, финансијске ризике повезане са прекомерним куповинама у игри, прикупљање и уновчавање личних података деце од стране актера из ИКТ индустрије, сајбер злостављање, говор мржње, насиље и излагање непримереном понашању или садржају, вербовање коришћењем стварних, компјутерски генерисаних или чак слика из виртуелне реалности и видео- записа који приказују и нормализују сексуално искоришћавање и злостављање деце. Ови ризици нису јединствени за окружење за играње, већ се примењују на друга дигитална окружења у којима деца проводе време.

Надаље, технолошки развој довео је до појаве "**интернета ствари**", где је све већи број и обим уређаја са могућности да се повежу, комуницирају и умрежавају путем интернета. То укључује играчке, мониторе за бебе и уређаје које покреће вјештачка интелигенција који могу да представљају ризике у погледу приватности и нежељеног контакта.

Добре праксе: Истраживање

У контексту интернетског или сајбер малтретирања, Microsoft је провео истраживање дигиталне безбедности и сајбер малтретирања. Године 2012. анкетирао је децу од 8 до 17 година у 25 земаља о негативном понашању на интернету. Резултати су показали да је у просеку 54% учесника навело да се брину да ће бити малтретирани на интернету, 37% је изјавило да су доживели сајбер малтретирање, а 24% је открило да су некога малтретирали. Исто истраживање је показало да је мање од троје од десет родитеља разговарало са децом о насиљу на интернету. Од 2016. Microsoft проводи **редовно истраживање** ризика на интернету дајући годишње извештаје о индексу дигиталне учтивости.

ФАЦЕС је мултимедијални програм који су произвели НХК Јапан и конзорцијум различитих јавних сервиса са причама о жртвама насиља на интернету и ван њега широм света. Серија се састоји од портрета адолесцената у којима протагонисти пред камерама објашњавају како су реаговали на нападе путем интернета. Серију, која је такође произведена у двоминутним клиповима, прихватили су Facebook, УНЕСКО, и Савет Европе, и доступна је на многим језицима.

У 2019. години, УНИЦЕФ је објавио дискусиони документ о Правима детета и играње на интернету: Прилике и изазови за децу и ИКТ индустрију да би се позабавили могућностима и изазовима за децу у једној од најбрже растућих индустрија забаве. Рад истражује сљедеће теме:

- право деце на игру и слободу изражавања (време играња и здравствени исходи);
- недискриминација, учешће и заштита од злостављања (Социјална интеракција и инклузија, токсична окружења, старосне границе и верификација, заштита од врбовања и сексуалног злостављања);
- право на приватност и слободу од економског искоришћавања (пословни модели за приступ подацима, бесплатне игре и уновчавање, недостатак транспарентности у комерцијалном садржају).

Добре праксе: Технологија

Google-ова лабораторија за виртуелну реалност испитује како виртуелна реалност може да помогне у охрабривању младих да се боре против насиља ван интернета и на интернету.[1]

У септембру 2019. ББЦ је покренуо мобилну апликацију која се зове **Own IT**, апликацију за безбедност намењену деци од 8 до 13 година која добијају први паметни телефон. Апликација је део ББЦ-јеве посвећености у пружању подршке младим људима у данашњем промењивом медијском окружењу и прати успешно покретање интернет странице Own IT у 2018. години. Апликација комбинује најсавременију технологију машинског учења за праћење дечијих активности на њиховим паметним телефонима с опцијом да деца самостално пријаве своје емоционално стање. Она користи ове информације за испоруку прилагођеног садржаја и интервенција које помажу деци да остану сретна и безбедна на интернету, нудећи пријатељске и подржавајуће подстицаје када њихово понашање почне да одудара од нормалног. Корисници могу да приступе апликацији када траже помоћ, али им је на располагању и пружање тренутних савета и подршке на екрану када им је потребна путем посебно развијене тастатуре. Карактеристике укључују:

- подсећање корисника да добро размисле пре него што поделе личне податке попут бројева мобилних телефона на друштвеним медијима;
- помоћ да разумију како би други могли да схвате поруке пре него што притисну слање;
- праћење њиховог расположења током времена и пружање смерница како побољшати ситуацију ако је то потребно;
- пружање информација о темама попут коришћења телефона касно навече и утицаја на добробит корисника.

Апликација садржи посебно допуштен садржај са ББЦ-а. Пружа корисне материјале и ресурсе који помажу младим људима да искористе време на интернету на најбољи начин и изграде здраво понашање и навике на интернету. Помаже младим људима и родитељима да конструктивније разговарају о својим искуствима на интернету, али родитељима неће давати извештаје или повратне информације, а нити један податак неће напустити уређаје корисника. Апликација не прикупља никакве личне податке или садржај генерисан од корисника док се цело машинско учење одвија у апликацији и на уређају корисника. Машине се посебно подешавају са подацима који се користе за тестирање да би се обезбедило да нема кршења приватности.

[1] За више информација погледајте Alexa Hasse и др., "Млади и сајбер злостављање: Још један поглед", Беркман Клајн центар за интернет и друштво, 2019.

2.1.3 Посебна ситуација код деце са сметњама у развоју[4]

Деца и млади са инвалидитетом суочавају се са ризицима на интернету на сличан начин као и она без инвалидитета, али, поред тога, могу да се суоче са специфичним ризицима који се односе на њихове инвалидности. Деца и млади са инвалидитетом често се суочавају са искљученошћу, стигматизацијом и препрекама (физичким, економским, друштвеним и у ставовима) у учешћу у својим заједницама. Ова искуства могу имати негативан утицај на дете с инвалидитетом и навести га да тражи социјалне

[4] Погледати Савет Европе, "Два клика напред и један клик назад: извештај о деци са инвалидитетом у дигиталном окружењу", 2019.

интеракције и пријатељства на просторима на интернету. Иако такве интеракције могу да буду позитивне и помогну у изградњи самопоштовања и стварању мрежа подршке, оне такође могу такву децу да изложе већем ризику случајевима врбовања, подстицања на интернету и / или сексуалног узнемиравања. Истраживања показују да су деца и млади који имају потешкоће ван интернета и они погођени психосоцијалним потешкоћама под повећаним ризиком од таквих инцидената.[5]

Деца која су жртве изван интернета, вероватно ће бити жртве и на интернету. То децу са инвалидитетом ставља у већи ризик на интернету, али имају и већу потребу да буду на интернету. Истраживања показују да ће деца са инвалидитетом вероватније доживети злостављање било које врсте,[6] а посебно је вероватно да ће доживети сексуалну виктимизацију.[7] Виктимизација може да укључује малтретирање, узнемиравање, искључење и дискриминацију на основу стварне или замишљене инвалидности детета или због аспеката повезаних с његовом инвалидношћу, попут начина на који се понаша или говори или опреме или услуга које користи.

Починиоци врбовања, подстицања путем интернета и / или сексуалног узнемиравања деце и младих са инвалидитетом могу да укључују не само преступнике са преференцијама који циљају децу и младе, већ и оне који циљају децу и младе са инвалидитетом. Такви починиоци могу да буду „привrженици“ - особе које немају инвалидитет а које сексуално привлаче особе са инвалидитетом (најчешће особе са ампутацијама и особе које користе помагала у кретању), а од којих се неки и сами претварају да имају инвалидитет.[8] Радње таквих људи могу да укључују преузимање фотографија и видео-записа деце и младих са инвалидитетом (које су нешкодљиве природе) и / или њихово дељење путем намјенских форума или профила на друштвеним медијима. Алати за пријављивање на форумима и друштвеним медијима често немају одговарајући пут за решавање таквих радњи.

Постоји брига да „родитељско дељење“ (родитељи који деле информације и фотографије своје деце и младих на интернету) може да наруши дјететову приватност, да доведе до малтретирања, изазове срамоту или има негативне последице касније у животу. [9] Неки родитељи деце са сметњама у развоју могу да деле информације или медијски материјал свог детета у потрази за подршком или саветом, што може као резултат имати да њихово дете ставља у ризик кршења приватности у том тренутку и у будућности. Такви родитељи такође ризикују да буду на мети неупућених или несавесних људи који нуде третмане, терапије или "лекове" за дететов инвалидитет. Једнако тако, неки родитељи деце и младих са инвалидитетом могу да буду превише заштитнички настројени због недостатка знања о томе како најбоље усмеравати своје дете да користи интернет или како га заштитити од насиља или узнемиравања.[10]

Појединa деца и млади са инвалидитетом могу да се суоче са потешкоћама у коришћењу или чак искључењем из окружења на интернету због неприступачног дизајна (нпр. апликације које не допуштају повећање величине текста), ускраћивања тражених погодности (нпр. софтвера за читање текста са екрана или прилагодљивих рачунарских контрола), или потреба за одговарајућом подршком (нпр. подучавање како се користи опрема, подршка један на један за навигацију у друштвеним интеракцијама).[11]

[5] Andrew Schrock и др., “Подстицање, узнемиравање и проблематичан садржај”, Беркманов центар за интернет и друштво, 2008.

[6] УНИЦЕФ, „извештај о стању деце у свету: деца са инвалидитетом,” 2013.

[7] Katrin Mueller-Johnson и др., “Сексуална виктимизација младих са тјелесним инвалидитетом: Испитивање нивоа распрострањености, ризика, и заштитних фактора”, Часопис о међуљудском насиљу, 2014.

[8] Richard L Bruno, „Привrженици, глумци и људи који то желе бити: Два случаја фактичког поремећаја инвалидности”, Сексуалност и инвалидитет, 1997.

[9] УНИЦЕФ, “Приватност деце у доба Web 2.0 и 3.0: Изазови и могућности за политику”, Innocenti дискусиони рад 2017-03 .

[10] УНИЦЕФ, “Постоји ли љествица дјечјег учешћа на интернету?”, Innocenti истраживачки сажетак, 2019.

[11] За Смернице о овим правима, види Конвенцију УН-а о правима особа с инвалидитетом и Факултативни протокол, посебно члан 9. о приступачности и члан 21. о слободи изражавања и мишљења и приступу информацијама.

2.2 Постојећи национални и транснационални модели за заштиту деце на интернету

На глобалном нивоу усваја се неколико модела да би се деца и млади заштитили на интернету. Интересне стране у ИКТ индустрији требало би да их сматрају смјерницама за међународне иницијативе и оквиром који ће обезбедити да се не штеде напори у заштити деце и младих на интернету. Интернет индустрија је разнолика и замршена област, састављена од компанија различитих величина и функција. Важно је да се заштитом деце не баве само платформе и услуге засноване на садржају већ и они који подржавају инфраструктуру интернета.

Мора се напоменути да је капацитет ИКТ компанија да уведу свеобухватну политику заштите деце ограничен њиховим доступним ресурсима. Стога ове смернице препоручују да ИКТ компаније раде заједно на увођењу услуга за заштиту корисника. Делећи ресурсе и инжењерску стручност, ИКТ компаније би могле ефикасније да створе „безбедне просторе“ да би се спречило злостављање.

Сарадња ИКТ компанија

Технолошка коалиција је пример успешне сарадње између интересних страна у ИКТ индустрији у борби против сексуалног искоришћавања и злостављања деце.

Транснационални модели

ИКТ компаније би требало да укључе релевантне међународне смернице у свој структурни програм, и требало би да се придржавају свих релевантних националних или транснационалних закона који се примењују у земљама у којима послују. ИКТ компаније не би требало да разматрају само радње које морају да предузму на правном нивоу, већ и које активности могу да обављају и, где је то могуће, да настоје да проводе иницијативе на глобалном нивоу. Неки од модела који пружају принципе за такве иницијативе укључују:

- Министарски добровољни принципи пет држава за борбу против сексуалног искоришћавања и злостављања деце (2020);
- Комисија за широкопојасни приступ за одрживи развој, безбедност деце на интернету: Смањење ризика од насиља, злостављања и искоришћавања на интернету (2019);
- Глобални савез WePROTECT, Глобални стратешки одговор на сексуално искоришћавање и злостављање деце на интернету (2019);
- Глобално партнерство за заустављање насиља над децом, безбедно за учење: Позив на акцију;
- дечије достојанство у дигиталном свету, Савез за достојанство детета: извештај радне групе за Технологију (2018);
- Директива (ЕУ) 2018/1808 Европског парламента и савета: Директива о аудиовизуелним медијским услугама;
- Општа уредба Европске комисије о заштити података (2018);
- Препорука ОЕЦД-а у погледу безбедности деце на интернету (2012).

Национални модели

Постоји низ националних и међународних модела који утврђују јасне улоге и одговорности технолошких компанија у решавању заштите деце на интернету. Неке од њих нису специфичне за децу саме по себи, али се могу на њих односити као на кориснике интернета. Они пружају свеобухватне смернице ИКТ компанијама у вези са регулаторним политикама, стандардима и сарадњом са другим секторима. У сврху овог документа истакнути су кључни принципи таквих модела, који се примењују на ИКТ компаније.

Кодекс дизајна прилагођеног узрасту, Велика Британија

Почетком 2019. године Канцеларија комесара за информације објавила је приедлоге за свој кодекс за дизајнирање прилагођено узрасту ради унапређења заштите дечијих података. Предложени кодекс заснован је на најбољем интересу за децу, како је утврђено у Конвенцији о правима детета УН-а, и у њему је изнето неколико очекивања од ИКТ компанија. Кодекс се састоји од петнаест стандарда који укључују услуге одређивања локације за децу искључене у почетним подешавањима, ИКТ компаније да прикупљају и задржавају само минималну количину личних података деце, да производи буду приватни по самом дизајну и да објашњења одговарају узрасту и да су доступна.

Закон о штетним дигиталним комуникацијама, Нови Зеланд

Законом из 2015. године сајбер злостављање је окарактерисано као специфично кривично дело и фокусира се на широк распон штета, од сајбер малтретирања до порнографије из освете. Циљ му је обесхрабрити, спречити и умањити штетну дигиталну комуникацију, чинећи незаконитим постављање дигиталне комуникације са намером да се изазове озбиљна емоционална узнемиреност код друге особе, и поставља низ од 10 принципа комуникације. Омогућава корисницима да се жале независној организацији ако су ови принципи прекршени или се примењују на судске налоге против аутора или домаћина комуникације ако проблем није решен.

Комесар eSafety, Аустралија

Основана 2015. године, аустралијски Комесар eSafety прва је светска владина агенција посвећена борби против злоупотребе на интернету и одржавању безбедности својих грађана на интернету. Као национални независни регулатор за безбедност на интернету, eSafety има снажну комбинацију функција. Оне се крећу од превенције преко подизања свести, образовања, истраживања и давања смерница за најбољу праксу, до ране интервенције и санације штете кроз више законских регулаторних планова које дају eSafety-ју овлаштења да брзо уклони сајбер малтретирање, злостављање засновано на сликама и незаконит садржај на интернету. Ова широка надлежност омогућава eSafety-ју да се брине о безбедности на интернету на вишестран, целовит и проактиван начин. У 2018. години eSafety је развио Safety by Design (SbD), иницијативу која ставља безбедност и права корисника у средиште дизајна, развоја и увођења интернетских производа и услуга. Скуп принципа безбедности по дизајну налази се у средишту иницијативе која утврђује реалне, ефикасне и остваривe мере које ИКТ компаније треба да предузму да би боље заштитиле и одбраниле грађане на интернету. Три свеобухватна принципа су:

1) **Одговорности пружаоца услуга**: терет безбедности никада не би требало да падне на крајњег корисника. Могу се предузети превентивни кораци да би се обезбедило да се познате и предвиђене штете процене у дизајну и пружању услуга на интернету, заједно са корацима да би се смањила вероватноћа да ће услуге олакшати, започети или подстакнути незаконито и неприкладно понашање.
2) **Давање могућности и аутономије корисницима**: достојанство корисника и њихови најбољи интереси су од централне важности. Људске делатности и аутономију треба подржати, појачати и ојачати у дизајну услуга омогућавајући корисницима већу контролу, управљање и регулацију сопствених искустава.
3) **Транспарентност и одговорност**: ово су обележја снажног приступа безбедности, које пружају гаранције да службе делују у складу са објављеним безбедоносним циљевима, као и едукација и давање могућности јавности да предузму мере ради решавања безбедносних проблема.

Глобални савез WePROTECT

У средишту стратегије WePROTECT Глобалног савеза је подршка земљама да развију координисане одговоре више интересних страна за борбу против сексуалног искоришћавања деце на интернету, вођене својим Моделима националног одговора, који делују као нацрт за деловање на националном нивоу. Пружа оквир за земље на који би требало да се ослоне у борби против сексуалног искоришћавања деце на интернету. Унутар WePROTECT Модела националног одговора, постоји јасан скуп обавеза за ИКТ компаније које се односе на:

- поступке обавештавања и уклањања;
- пријављивање сексуалног искоришћавања и злостављања деце (ЦСЕА);
- развој технолошких решења; и
- инвестирање у ефикасне превентивне програме и услуге реаговања за заштиту деце на интернету.

Глобално партнерство и фонд за заустављање насиља над децом

Глобално партнерство и фонд за заустављање насиља над децом покренуо је генерални секретар Уједињених нација 2016. године са једним циљем: катализовати и подржати акцију за заустављање свих облика насиља над децом до 2030. године, кроз јединствену сарадњу више од 400 партнера из свих сектора.

Фокус рада је на спашавању и пружању подршке жртвама, технолошким решењима за откривање и спречавање прекршаја, пружању подршке органима за провођење закона, законодавним и политичким реформама, и генерисању података и доказа о размерама и природи сексуалног искоришћавања и злостављања деце на интернету, као и разумевању дечијих перспектива.[12]

3. Кључна подручја заштите и промоције дечијих права

Овај одељак наводи **пет кључних подручја** у којима ИКТ компаније могу да предузму мере за заштиту деце и младих када користе ИК технологије и да промовишу њихову позитивну употребу ИК технологија.

3.1 Разматрања о интеграцији права детета у све одговарајуће корпоративне политике и процесе управљања

Разматрање интеграције права детета захтева да компаније предузму одговарајуће мере за идентификовање, спречавање, ублажавање и, по потреби, санирање потенцијалних и стварних негативних утицаја на дечија права. Водећи принципи УН-а о пословању и људским правима позивају сва предузећа и индустрије да успоставе одговарајуће политике и процесе да би испунили своју одговорност према поштовању људских права.

[12] За више информација погледајте Заустављање насиља над децом, "Корисници фонда за заустављање насиља".

ИКТ компаније би требало да посвете посебну пажњу деци и младима као рањивој групи с обзиром на њихову заштиту података и слободу изражавања. Резолуција Генералне скупштине Уједињених нација 68/167 о праву на приватност у дигитално доба потврђује право на приватност и слободу изражавања без излагања незаконитом уплитању. Поред тога, Резолуција 32/13 Савета УН-а за људска права о промоцији, заштити и уживању људских права на интернету препознаје глобалну и отворену природу интернета као покретачке снаге у убрзавању напретка према развоју и потврђује да иста права која људи имају ван интернета такође морају да буду заштићена на интернету. У државама у којима недостаје одговарајући правни оквир за заштиту права деце и младих на приватност и слободу изражавања, ИКТ компаније би требало да прате појачану дубинску анализу да би обезбедиле да су политике и праксе у складу са међународним правом. Како се грађански ангажман младих наставља да повећава путем комуникација на интернету, ИКТ компаније имају већу одговорност за поштовање права деце и младих, чак и тамо где домаћи закони још увек нису сустигли међународне стандарде.

> Компаније би требало да имају успостављен механизам за жалбе на оперативном нивоу који ће обезбедити формат за погођене појединце да изразе забринутост због потенцијалних прекршаја. Механизми на оперативном нивоу треба да буду доступни деци, њиховим породицама и онима који заступају њихове интересе. Принцип 31 Водећих принципа о пословању и људским правима појашњава да такви механизми треба да буду легитимни, доступни, предвидљиви, непристрасни, транспарентни, компатибилни са правима, извор континуираног учења и засновани на ангажовању и дијалогу. Заједно са интерним процесима за решавање негативних утицаја, механизми за жалбе требало би да обезбеде да компаније имају успостављене оквире који обезбеђују деци и младима одговарајући начин да траже помоћ када су њихова права угрожена.

Компаније треба да заузму приступ према ИКТ безбедности заснован на усклађености који се фокусира на испуњавање националног законодавства, слијеђење међународних смерница када нема националног законодавства и избјегавање негативних утицаја на права деце и младих, и да компаније проактивно промовишу развој и добробит деце и младих волонтерским акцијама које унапређују права деце и младих на приступ информацијама, слободу изражавања, учешће, образовање и културу.

Добре праксе: Дизајн који одговара политици и узрасту

Компанија за развој апликација Toca Boca производи дигиталне играчке из перспективе детета. Политика приватности компаније осмишљена је тако да наводи које податке компанија прикупља и како се користе. Toca Boca, Inc је члан ПРИВО безбедне дечије приватности ЦОРПА програма за цертификацију безбедних уточишта.

LEGO® Life је пример безбедне платформе друштвених медија за децу млађу од 13 година за дељење својих ЛЕГО креација, за добијање инспирације и безбедну интеракцију. Овдје се од деце не траже никакви лични подаци за стварање профила, за шта је само потребна адреса е-поште родитеља или старатеља. Апликација ствара прилику деци и породицама да разговарају о безбедности на интернету и приватности у позитивном окружењу.

Примери дизајна примереног узрасту укључују специфичне понуде неких од великих јавних сервиса за одређене старосне групе: на пример, Немачки АРД (Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland - Das Erste) и ЗДФ (Zweites Deutsches Fernsehen) циља своју публику почевши од узраста од 14 година, нудећи прилагођени садржај путем интернет канала funk.net. ББЦ (Британска радиодифузна корпорација) покренула је CBeebies који је усмерен на децу млађу од 6 година. Садржај интернет странице је посебно прилагођен одговарајућим старосним групама.

Добре праксе: Политика и технологија

Twitter константно улаже у власничку технологију, што је допринело стабилном смањењу оптерећења за људе код слања пријава.[1] Конкретно, више од 50% твитова, у поређењу са 20% у 2018. години, које је Twitter испратио да одговори на њихову насилну природу, тренутно се проактивно појављују коришћењем технологије, уместо да се ослањају на пријављивање Twitter-у. Нова технологија се користи за бављење политичким садржајима поља приватног информисања, осетљивим медијима, понашањем из мржње, злостављањем и лажним представљањем.

[1] Twitterov,"15. извештај о транспарентности: Повећање проактивног извршења

3.2 Развој стандардних поступака за руковање материјалима сексуалног злостављања деце

У 2019. години IWF је деловала на 132.676 интернет страница за које је потврђено да садрже сексуално злостављање деце.[13] Било која интернет адреса би могла да садржи стотине, ако не и хиљаде слика и видео-записа. Од слика над којима је IWF предузела мере, 45% је приказивало децу узраста 10 или мање година и 1.609 интернет страница приказивало је децу узраста 0–2 године, од којих је 71% садржавало најтеже сексуално злостављање, попут силовања и сексуалног мучења. Ове узнемирујуће чињенице истичу важност заједничког деловања ИКТ компанија, влада, органа за провођење закона и цивилног друштва у борби за превенцију материјала сексуалног злостављања деце.

[13] IWF, "Зашто. Како. Ко. И резултати. Годишњи извештај 2019".

Иако се многе владе боре против ширења и дистрибуције материјала сексуалног злостављања деце доношењем закона, прогоном и процесуирањем насилника, подизањем свести и пружањем подршке деци и младима у опоравку од злостављања или искоришћавања, постоје многе земље које још увек немају успостављене одговарајуће системе. У свакој земљи су потребни механизми који ће омогућити широј јавности да пријави насилни и експлоатациони садржај ове природе. ИКТ компаније, органи за провођење закона, владе и цивилно друштво морају да сарађују да би обезбедили успостављање одговарајућег правног оквира у складу са међународним стандардима. Такви оквири би требало да инкриминишу све облике сексуалног искоришћавања и злостављања деце, укључујући и материјал сексуалног злостављања деце, и да заштите децу која су жртве таквог злостављања или искоришћавања. Ти оквири морају да обезбеде да процеси пријављивања, истраге и уклањања садржаја раде што ефикасније.

ИКТ компаније би требало да обезбеде везе до националних линија за подршку или других локално доступних линија за подршку, попут WF портала у неким земљама, а у недостатку локалних могућности пријављивања, да обезбеде везе до других међународних линија за подршку по потреби, као што је Амерички национални центар за несталу и злостављану децу (НЦМЕЦ) или Међународно удружење интернетских линија за подршку (INHOPE), где се било која међународна линија за подршку може да користи за подношење пријаве.

Одговорне компаније предузимају низ корака да би спречиле да се њихове мреже и услуге користе за ширење материјала сексуалног злостављања деце. То укључује увођење језика у услове и одредбе или кодексе понашања који изричито забрањују такав садржај или понашање;[14] развијање снажних процеса обавештавања и уклањања; те рад и подршка националним линијама за подршку.

Поред тога, неке компаније примењују техничке мере да би спречиле злоупотребу својих услуга или мрежа за дељење познатог материјала сексуалног злостављања деце. На пример, неки провајдери интернетских услуга блокирају приступ интернет адресама за које је одговарајући орган потврдио да садрже материјал сексуалног злостављања деце ако је интернет страница хостована у земљи у којој нису успостављени процеси да би се обезбедило да ће се он брзо уклонити. Други користе технологије хеширања за аутоматско откривање и уклањање слика сексуалног злостављања деце које су већ познате полицији или линијама за подршку. Чланови ИКТ индустрије требало би да размотре и укључе све релевантне службе у своје операције да би се спречило ширење сексуалног злостављања деце.

Актери у ИКТ индустрији требало би да се обавежу на доделу пропорционалних ресурса и наставе да развијају и деле, по могућности, технолошка решења отвореног кода за откривање и уклањање материјала сексуалног злостављања деце.

Добре праксе: Технологија

Microsoft користи четвороструки приступ за подстицање одговорне и безбедне употребе технологије, са фокусом на саму технологију, самоуправљање, партнерства и образовање и допирање до потрошача. Microsoft је такође уградио функције које дају могућност појединцима да ефикасније управљају безбедношћу на интернету. "Породична безбедност" је једна од таквих карактеристика која омогућава родитељима и старатељима да надгледају употребу интернета своје деце.

Microsoft проводи политике против узнемиравања на својим платформама, а корисници који злоупотребљавају ове прописе подлијежу укидању профила или, у случају озбиљнијих кршења, мерама за провођење закона.

[14] Треба имати на уму да непримерено понашање корисника није ограничено на материјал сексуалног злостављања деце и да компанија треба на одговарајући начин да поступа с било којом врстом непримереног понашања или садржаја.

Microsoft PhotoDNA је алат који креира хешеве слика и упоређује их са базом података хешева који су већ идентификовани и за које је потврђено да су материјал сексуалног злостављања деце. Ако пронађе подударање, слика се блокира. Овај алат је омогућио провајдерима садржаја уклањање милиона незаконитих фотографија са интернета; помогао је осудити дечије сексуалне предаторе; а у неким случајевима помогао је полицији да спаси потенцијалне жртве пре него што су биле физички повређене. Microsoft се већ дуго залаже за заштиту својих купаца од незаконитих садржаја на својим производима и услугама, а примена технологије коју је компанија већ направила у борби против раста оваквих незаконитих видео-записа био је логичан следећи корак. Међутим, овај алат не користи технологију препознавања лица нити може да идентификује особу или предмет на слици. Али са појавом PhotoDNA for Video ствари су попримиле нови заокрет. PhotoDNA for Video раставља видео-запис у кључне кадрове и у основу ствара хешеве за те снимке екрана. На исти начин на који PhotoDNA може да пронађе подударање са сликом која је измењена да би се избегло откривање, PhotoDNA for Video може да пронађе садржај сексуалног искоришћавања деце који је уређен или спојен у видео-запис који би у противном могао да изгледа безазлен.

Штавише, Microsoft је у скорије време објавио нови алат за препознавање дечијих предатора који у чатовима на интернету врбују децу ради злостављања. Пројекат Артемис, развијен у сарадњи са компанијама The Meet Group, Roblox, Kik и Thorn, надовезује се на Microsoft-ову патентирану технологију и путем Thorn-а ће бити доступан бесплатно квалификованим услужним компанијама на интернету које нуде функцију чата. Пројекат Артемис је технички алат који даје упозорења администраторима када је потребна модерација у чет собама. Овом техником откривања врбовања моћи ће открити, реаговати и пријавити предаторе који покушавају да намаме децу у сексуалне сврхе.

IWF пружа низ услуга члановима ИКТ индустрије да би заштитио своје кориснике од тога да случајно наиђу на материјал сексуалног злостављања деце. Оне укључују:

- динамичку блок листу интернет адреса материјала уживо, обезбеђеног квалитета;
- хеш листу познатог криминалног садржаја који се односи на материјал сексуалног злостављања деце;
- јединствену листу кључних ријечи тајних израза за које се зна да су повезане са материјалима сексуалног злостављања деце;
- списак детаља о називима домена који су познати по хостовању садржаја сексуалног злостављања деце да би се омогућило брзо уклањање домена у којима се налази незаконити садржај.

3.3 Стварање безбеднијег окружења на интернету прилагођеног узрасту

Врло мало ствари у животу може се сматрати апсолутно безбедним и без ризика све време. Чак и у градовима у којима је кретање саобраћаја високо регулисано и строго контролисано, несреће се и даље дешавају. На исти начин, сајбер простор није без ризика, посебно за децу и младе. О деци и младима се може размишљати као о примаоцима, учесницима и актерима у њиховом окружењу на интернету. Ризици са којима се суочавају могу да се поделе у четири подручја:[15]

[15] Sonia Livingstone и др., "ЕУ Кидс Онлајн: Завршни извештај", Лондонска школа економије, 2009.

- ***Непримерен** садржај* - деца и млади могу наићи на непримерен и незаконит садржај док траже нешто друго кликом на вероватно безазлен линк у инстант поруци, на блогу или приликом дељења датотека. Они такође могу да траже и деле неприкладан материјал или материјал неприлагођен узрасту. Оно што се сматра штетним садржајем разликује се од земље до земље; Примери укључују садржај који промовише злоупотребу опојних дрога, расну мржњу, ризично понашање, самоубиство, анорексију или насиље.
- *Непримерено понашање* деца и одрасли могу да користе интернет за узнемиравање или чак искоришћавање других људи. деца могу понекад да емитују увредљиве коментаре или неугодне слике или могу да украду садржај или повреде ауторска права.
- *Неприкладан контакт* - И одрасли и млади могу путем интернета да траже децу или друге младе људе који су рањиви. Често, њихов циљ је уверити мету да су развили смислен однос, али основна сврха је манипулативна. Они могу покушати да наговоре дете да изврши сексуална или друга изопачена дела на интернету, користећи веб-камеру или други уређај за снимање, или ће покушати да уговоре лични састанак и физички контакт. Овај процес се често назива „врбовање“.
- *Комерцијални ризици* - Ова категорија односи се на ризике нарушавања приватности података који се односе на прикупљање и употребу дечијих података, као и дигитални маркетинг. безбедност на интернету је изазов заједнице и прилика за ИКТ компаније, владе и цивилно друштво да раде заједно на успостављању безбедносних принципа и пракси. ИКТ компаније могу да понуде читав низ техничких приступа, алата и услуга за родитеље, децу и младе, и пре свега треба направити производе који су једноставни за употребу, безбедни по дизајну и примјерени узрасту за њихов широк спектар корисника. Додатни приступи укључују понуду алата за развој одговарајућих система за провјеру старости који поштују дечија права на приватност и приступ или ограничавају приступ деци и младима садржају који је Непримерен њиховим годинама или ограничавају људе са којима деца могу да имају контакт или време у којем могу да користе интернет. Оно што је најважније, оквири „безбедност по дизајну“[16], укључујући и приватност, морају да буду укључени у процесе развијања иновација и дизајна производа. дечија безбедност и одговорно коришћење технологије морају се пажљиво размотрити и о њима се не смије мислити накнадно.

Неки програми омогућавају родитељима надгледање текстуалних порука и других комуникација које њихова деца и млади шаљу и примају. Ако ће се користити програми ове врсте, важно је да се о томе отворено разговара с дететом, иначе се такво понашање може да доживи као „шпијунирање“ и може да поткопа поверење у породици.

Политике прихватљиве употребе један су од начина на који ИКТ компаније могу да утврде какво се понашање подстиче и код одраслих и код деце, које врсте активности нису прихватљиве и последице било каквог кршења ових политика. Јасни и транспарентни механизми пријављивања треба да буду доступни корисницима који се брину о садржају и понашању. Поред тога, пријављивање треба испратити на одговарајући начин, уз благовремено пружање информација о статусу пријаве. Иако компаније могу различито да примењују пратеће механизме од случаја до случаја, битно је поставити јасан временски оквир за реаговање, саопштити одлуку донесену у вези са пријавом и понудити начин решавања ако корисник није задовољан одговором.

16 Комесар eSafety, Преглед безбедности по дизајну, 2019.

Добре праксе: Извјештавање

Facebook је, у настојању да сузбије сексуално узнемиравање на дигиталним платформама, суфинансирао пројекат deSHAME са Европском унијом, сарадњу између Childnet, Save the Children, Kek Vonal и UCLan. Циљ овог пројекта је повећати пријављивање сексуалног узнемиравања путем интернета међу малољетницима и побољшати мултисекторску сарадњу у превенцији и реаговању на овакво понашање.

Како је једна од главних сврха пројекта подстицање корисника да пријављују садржаје који су узнемиравајућег карактера или су непримерени, Facebook-ови стандарди заједнице такође су релевантни као смернице о томе шта је допуштено, а шта није допуштено на Facebook-у. Они такође наводе типове корисника којима не допушта постављање садржаја. Facebook је такође створио безбедоносне елементе попут елемента "Познајете ли ову особу?"; „други“ инбокс који прикупља нове поруке од људи које корисник не познаје; и поп-ап прозор који се појављује на обавештењима ако то изгледа као да је малолетника контактирала одрасла особа коју он или она не познаје.

Провајдери садржаја и услуга на интернету могу такође да опишу природу садржаја или услуга које пружају и предвиђени циљни старосни распон. Ови описи требало би да буду усклађени са постојећим националним и међународним стандардима, релевантним прописима и савјетима о маркетингу и оглашавању за децу које одговарајући органи за класификацију стављају на располагање. Овај процес постаје све компликованији с растућим спектром интерактивних услуга које омогућавају објављивање корисничког садржаја, на пример путем огласних плоча, чет соба и услуга друштвених мрежа. Када компаније посебно циљају децу и младе и када су услуге претежно усмерене на млађу публику, очекивања **у смислу лакоће за коришћење, лако разумљивом и приступачном садржају** и безбедности биће много већа.

Компаније се такође подстичу да усвоје највише стандарде заштите приватности када је у питању прикупљање, обрада и чување података од или о деци и младима, јер деци и младима може недостајати зрелост да увиде шире друштвене и личне последице откривања или пристанка на дељење својих личних података на интернету или на употребу њихових личних података у комерцијалне сврхе. Услуге усмерене на или које би вероватно привукле као главну публику децу и младе морају узети у обзир ризике у којима се могу наћи због приступа или прикупљања и употребе личних података (укључујући податке о локацији) и обезбедити да се ти ризици решавају на прави начин и да су корисници информисани. Конкретно, компаније би требало да обезбеде да језик и стил било којег материјала или комуникације који се користе за промоцију услуга, пружање приступа услугама или путем којих се приступа, прикупља и користе лични подаци, помажу разумијевању и помажу корисницима у управљању заштитом њихове приватности на јасан и једноставан начин и да објашњавају на шта пристају јасним, разумљивим језиком.

Добре праксе: Иновација

У 2018. – 2019. УНИЦЕФ-ова Регионална канцеларија за Источну Азију и Пацифик организовала је пет округлих столова са више интересних страна ради размјене обећавајућих пракси ИКТ компанија за борбу против сексуалног искоришћавања и злостављања деце на интернету. Учесници округлих столова биле су водеће компаније из приватног сектора, као што су Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Монголија) Mobifone + (Вијетнам), Globe Telecom (Филипини), True (Тајланд), ГСМА и партнери из цивилног друштва, укључујући INHOPE, ЕЦПАТ International и Међународну линију за помоћ деци.

У склопу истог пројекта, у фебруару 2020. године, УНИЦЕФ је покренуо Think Tank да би убрзао лидерство у ИКТ компанијама у источној Азији и пацифичком региону да би спријечио насиље над децом у свету на интернету. Think Tank је инкубатор идеја и иновација, који се ослања на јединствене перспективе актера у ИКТ индустрији (стварање производа, маркетинг итд.) за развој утицајних образовних материјала и идентификацију најефикаснијих платформи за испоруку, као и за развој оквира за евалуацију који може да измјери утицај ових образовних материјала и порука усмјерених на децу. Think Tank чине Facebook, Теленор, академски стручњаци, агенције Уједињених нација, попут ИТУ-а, УНЕСКО-а и УНОДЦ-а, и друге, попут аустралијског комесара eSafety, ЕЦПАТ International, ИЦМЕЦ-а, ИНТЕРПОЛ-а и Глобалног фонда за заустављање насиља. Инаугуративни састанак Think Tank-а, одржан паралелно с АСЕАН-овом регионалном конференцијом о заштити деце на интернету, окупио је стручњаке, укључујући Microsoft, да би истражили технологије и истраживачке могућности за боље праћење промјена у понашању на интернету, на основу преузимања безбједносних материјала и порука на интернету.

3.4 Едукација деце, родитеља и едукатора о безбедности деце и њиховој одговорној употреби ИК технологија

Техничке мере могу да буду важан део обезбеђења заштите деце и младих од потенцијалних ризика на интернету, али оне су само један елеменат једначине. **Алати за родитељску контролу, подизање свести** и образовање такође су кључне компоненте које ће помоћи у оснаживању и информисању деце и младих свих узраста, као и родитеља, старатеља и едукатора. Иако компаније имају важну улогу у подстицању деце и младих да користе ИК технологије на одговоран и безбедан начин, ту одговорност деле са родитељима, школама, децом и младима.

Многе компаније улажу у образовне програме осмишљене да би корисницима омогућиле доношење основаних одлука о садржају и услугама. Компаније помажу родитељима, старатељима и едукаторима у усмеравању деце и младих према безбеднијим, одговорнијим и примеренијим искуствима на интернету и мобилним телефонима. То укључује објављивање знаковног садржаја осетљивог на старосну границу и обезбеђивање да се информације о ставкама као што су цене садржаја, услови претплате и начин отказивања претплате јасно саопштавају. Промовисање поштовања услова минималне старосне границе од стране друштвених медија у свим земљама у којима је могуће проверавање старости такође би помогло у заштити деце омогућавањем приступа услугама одговарајућем узрасту. Важно разматрање које треба ускладити са овом препоруком је додатно прикупљање личних података које ово може да подразумева и потреба да се ограничи прикупљање и чување ових података и њихова обрада.

Такође је важно пружити информације деци и младима директно о безбеднијој употреби ИК технологија и позитивном и одговорном понашању. Поред подизања свести о безбедности, компаније могу да омогуће позитивна искуства развијањем садржаја за децу и младе о томе да поштују једни друге, буду љубазни и отвореног ума када користе ИК технологије и брину се о пријатељима. Оне могу да пруже информације о радњама које треба предузети ако постоје негативна искуства, попут малтретирања на интернету или врбовања, олакшавајући пријаву таквих инцидената и пружајући функцију за одбијање примања анонимних порука.

Родитељи понекад имају мање разумевања и знања о интернету и мобилним уређајима од деце и младих. Штавише, спајање мобилних уређаја и интернет услуга отежава родитељски надзор. ИКТ компаније могу да раде у сарадњи са владом и едукаторима на јачању способности родитеља да подрже своју децу у изградњи њихове дигиталне отпорности и понашања као одговорних дигиталних грађана. Циљ није пренети одговорност за употребу ИК технологија од стране деце и младих само на родитеље, већ препознати да су родитељи у бољој позицији да одлуче шта је прикладно за њихову децу и да их треба упознати са свим ризицима да би боље заштитили своју децу и оснажити их за предузимање акције.

Информације могу да се преносе на интернету и ван њега путем више медијских канала, узимајући у обзир да неки родитељи не користе интернет услуге. Важно је сарађивати са школским дистриктима да би се припремили наставни планови и програми о безбедности на интернету и одговорној употреби ИК технологија од стране деце и младих, као и образовни материјали за родитеље. Примери укључују објашњење врста услуга и опција доступних за праћење активности, радње које се предузимају ако се дете суочава са малтретирањем или врбовањем на интернету, како избећи нежељену пошту и управљати подешавањима приватности и како разговарати са дечацима и девојчицама различитих старосних група о осетљивим проблемима. Комуникација је двосмеран процес и многе компаније нуде могућност купцима да их контактирају да би пријавили проблеме или разговарали о проблемима.

Како садржај и услуге постају све богатији, сви ће корисници и даље имати користи од савета и подсетника о природи одређене услуге и начину безбедног уживања у њој. Иако је важно децу научити одговорном коришћењу интернета, знамо да деца воле експериментисати, ризиковати, да су знатижељна и можда не доносе увек најбоље одлуке. Давање шансе да се баве својим делатностима доприноси њиховом развоју и здрав је начин који ће им помоћи да развију аутономију и отпорност, све док повратни ефекат није преоштар. Иако се деци мора дозволити да преузимају одређене ризике у интернетском окружењу, пресудно је да их родитељи и компаније могу подржати када ствари крену по злу, јер то може надокнадити негативан утицај неугодног искуства и претворити га у корисну лекцију за будућност.

Добре праксе: Образовање

НХК Јапан води кампању превенције самоубистава за младе на Twitter-у: У Јапану самоубиства међу тинејџерима достижу врхунац када се врате у школу након љетног распуста. Повратак у стварност је разлог за врхунац. Продукцијски тим НХК Heart Net TB (НХК Јапан) производи мултимедијални програм # У ноћи 31. августа. Повезујући телевизију, пренос уживо и друштвене медије, НХК је успјешно створио "место" на којем су тинејџери могли без страха да поделе своја осећања.

Добре праксе: Образовање

Twitter је такође објавио водич за едукаторе о медијској писмености. Састављен са УНЕСКО-ом, приручник првенствено има за циљ да помогне едукаторима да развију код млађих генерација вештине медијске писмености. Други аспект безбедоносног рада Twittera односи се на њихово откривање операција са информацијама. Ово је архива операција са информацијама које подржава држава и коју Twitter јавно дели. Иницијатива је покренута да би се оснажило академско и јавно разумевање кампања повезаних са овом проблематиком широм света, и да би се оснажила независна контрола трећих лица ових тактика на Twitter платформи.

Пројекат deSHAME, који суфинансирају Facebook и Европска унија, такође омогућава стварање ресурса за широк распон старосних група, са посебним фокусом на децу узраста од 9 до 13 година. Као део пројекта, развијен је алат под називом „Искорачи, говори!“, који пружа низ материјала за образовање, обуку и подизање свести, као и практичне алате за мултисекторске стратегије превенције и реаговања. Пројекат ће ове материјале за учење пренети другим европским земљама и партнерима широм света у сврху промоције дигиталних права младих.

Google је развио низ образовних иницијатива, ресурса и алата који помажу у промоцији безбедности за младе на интернету. Једна од њих је кампања Буди сјајан на интернету организована око дигиталног грађанства, креирана у сарадњи са организацијама као што су ConnectSafely, Породични институт за безбедност на интернету и коалиција Internet Keep Safe. Ова кампања је усмерена на младе људе узраста од 8 до 11 година. Садржи интернетску игру за младе (Интерланд) која подучава основама дигиталне безбедности и ресурсе за едукаторе, попут дигиталног грађанства и безбедносног плана и програма. Безбедносни план и програм нуди планове лекција за пет кључних тематских подручја кампање, од којих се једно фокусира на сајбер малтретирање. Као додатак овоме Google је направио курс дигиталног грађанства и безбедности на интернету за едукаторе ученика свих старосних група, пружајући даљњу подршку за интегрисање дигиталног грађанства и безбедносних активности у учионици. Google такође нуди неколико програма који помажу младима да се директно укључе у напоре на пољу безбедности на интернету и на пољу дигиталног грађанства. Глобална иницијатива Web Rangers један је од таквих програма који младе подучава о безбедности на интернету и подстиче их да креирају сопствене кампање око позитивне и безбедне употребе интернета. Постоје и посебни програми за младе за одређене државе, попут програма Internet Citizens Internet Legends у Великој Британији, које је покренуо Google.

На **Евровизијској размени вести за младе**, Европска радиодифузна унија окупља 15 европских телевизијских кућа да би размењивале програме, формате и решења на интернету и ван њега. Последњих година, подучавање дигиталне писмености и упозоравање деце на ризике на интернету постали су кључни за њихове програме. Међу најуспјешнијим иницијативама последњих година су огласи на друштвеним мрежама и вести прилагођене за децу које су произвели Super и Ultra nytt под НРК, норвешким јавним емитером.

Добре праксе: Стратешка партнерства

Као део пројекта подржаног од Фонда за заустављање насиља над децом, Capital Humano y Social Alternativo је 2018. године склопио партнерство с компанијом Telefónica, највећим провајдером интернет, кабловских и телефонских услуга у Перуу, са 14.4 милиона корисника, укључујући више од 8 милиона Мовистар мобилних корисника.

Неколико активности је проведено у оквиру овог плодног партнерства:

- **Виртуелни курс о заштити деце на интернету** је развијен од стране компаније Telefónica уз техничку подршку Capital Humano y Social Alternativo. Овај курс је сада отворено доступан на интернет страници Telefónica-е, а компанија прати број људи који се упишу и успешно завршавају курс. Перуанско министарство образовања сложило се да ће укључити приступ овом виртуелном курсу путем своје службене интернет странице.
- **Књижица о безбедности на интернету** направљена је од стране Capital Humano y Social Alternativo, а компанија Telefónica је дистрибуира у више од 300 мобилних продајних центара. Циљ је подићи свијест корисника Telefónica-е о безбедности на интернету и ризицима повезаним са сексуалним искоришћавањем и злостављањем деце на интернету.
- **Интерактивну игру о сексуалном искоришћавању и злостављању деце на интернету** развила је компанија Telefónica уз техничку подршку Capital Humano y Social Alternativo, коју њени корисници могу да играју док чекају своје редове у трговинама

Надовезујући се на успех са Telefónica-ом, Capital Humano y Social Alternativo удружила се са компанијом **Econocable**, провајдером интернета и кабловских услуга који ради у удаљеним подручјима у Перуу са ниским приходима.

3.5 Промовисање дигиталне технологије као начина за повећање грађанског ангажмана

Члан 13. Конвенције о правима детета УН-а каже да „дете има право на слободу изражавања; то право мора, независно од граница, укључивати слободу тражења, примања и ширења обавештења и идеја сваке врсте, усмено или писмено, штампањем, уметничким обликовањем или путем било којег другог средства према избору детета." Компаније могу да испуне своју дужност поштовања грађанских и политичких права деце и младих обезбеђујући да технологија и примена закона и политика развијених за заштиту деце и младих од штете на интернету немају ненамерне последице сузбијања њиховог права на учешће и изражавање или спречавање приступа информацијама које су важне за њихову добробит. Неопходно је обезбедити да системи провере старости не угрожавају истинску потребу одређених старосних група за приступ садржајима који су релевантни за њихов развој.

Истовремено, предузећа и ИКТ компаније такође могу да подрже права деце и младих пружајући механизме и алате за олакшавање учешћа младих. Они могу нагласити способност интернета да олакша позитиван ангажман у ширем грађанском животу, покреће друштвени напредак и утиче на одрживост и отпорност заједница, на пример, учествовањем у социјалним и еколошким кампањама и позивањем на одговорност оних који су одговорни. Уз одговарајуће алате и информације, деца и млади су у бољој позицији да приступе могућностима за здравствену заштиту, образовање и запошљавање те да изразе своја мишљења и потребе у школама, заједницама и земљама. Оспособљавају се за приступ информацијама о својим правима и тражење информација о стварима које их лично погађају, попут њиховог сексуалног здравља, и о политичкој и владиној одговорности.

Компаније такође могу да улажу у стварање интернетских искустава примерених деци и младима и породицама. Оне могу да подрже развој технологије и садржаја који подстичу и омогућавају деци и младима да уче, стварају иновације и праве решења. Увек би требало да имају на уму безбедност по дизајну у својим производима.

Поред тога, компаније могу проактивно да подрже права деце и младих радећи на уклањању дигиталне поделе. За учешће деце и младих потребна је дигитална писменост - способност разумевања и интеракције у дигиталном свету. Без ове могућности, грађани не могу да учествују у многим друштвеним функцијама које су постале дигитализоване, укључујући подношење пријава за порез, пружање подршке политичким кандидатима, потписивање петиција на интернету, регистрацију рођења или једноставно немају приступ комерцијалним, здравственим, образовним или културним информацијама. Без деловања, јаз између грађана који могу да приступе тим форумима и оних који то не могу због недостатка приступа интернету или дигиталне писмености и даље ће се повећавати, што ће ове посљедње довести у значајан недостатак. Компаније могу да подрже мултимедијске иницијативе за његовање дигиталних вештина које деци и младима требају да би били самопоуздани, повезани и активно укључени грађани.[17] У многим земљама дигитална и медијска писменост и напори на уклањању дигиталне поделе део су мисије јавних медијских сервиса последњих година. Италијански парламент, на пример, предложио је да приоритети националних емитера укључују уклањање дигиталне поделе и обезбеђење заштите деце ван интернета и на интернету, пример који би могле да следе друге земље.

[17] Примере учешћа младих из мобилне заједнице погледајте овдје.

Добре праксе: Вишеагенцијска сарадња

Недавно се Microsoft придружио глобалној кампањи Power of ZERO, коју води организација No Bully, чији је циљ помоћи малој деци и одраслима који брину о њима, да науче добро користити дигиталне технологије и да развију глас, саосјећање и инклузивност који су срце дигиталног грађанства. Иницијатива нуди едукаторима мале деце (кампања је усмерена на децу узраста до 8 година) и породицама бесплатан материјал за учење да би помогла малој деци да граје „12 моћи за добро“ (Моћ Зерових 12 животних вештина или „моћи“, за децу да се успешно крећу у онлајн и офлајн свету, укључујући отпорност, поштовање, инклузивност и креативност) и постављају им снажне основе у раном узрасту.

4. Опште смернице за ИКТ компаније

Табела 1. даје широке смернице за ИКТ компаније за идентификацију, спречавање и ублажавање било каквих негативних утицаја производа и услуга на права деце и младих, те за промоцију позитивне употребе ИК технологија од стране деце и младих.

Имајте на уму да неће сви кораци наведени у Табели 1. бити прикладни за све компаније и услуге, нити се сви потребни кораци за сваку услугу налазе у овој Табели. Опште смернице за ИКТ компаније допуњују се контролном листом по карактеристикама (види одељак 5) и обратно. Контролне листе по карактеристикама у табелама 2-5 истичу додатне кораке који су најважнији за поједине услуге. Имајте на уму да се контролне листе по карактеристикама могу преклапати и да више контролних листа могу бити релевантне за исту услугу.

Табела 1. Опште смернице за ИКТ компаније

Разматрања о интеграцији права детета у све одговарајуће корпоративне политике и процесе управљања	ИКТ компаније могу да идентификују, спрече и ублаже негативне утицаје ИК технологија на права деце и младих, и да идентификују могућности за подршку у напретку права деце и младих предузимањем следећих радњи:
	Обезбеђивањем да одређени појединац и / или тим буду именовани одговорним за овај процес и да има приступ потребним интерним и екстерним интересним странама. Давањем овлаштења овој особи или тиму да преузму водећу улогу у подизању профила заштите деце на интернету у цијелој компанији.
	Развијањем политике заштите и чувања деце и / или интегрисањем посебних ризика и могућности које се односе на права деце и младих у опредељења политике компаније (нпр. људска права, приватност, маркетинг и релевантни кодекси понашања).
	Интегрисањем дубинске анализе о питањима заштите деце на интернету у постојеће оквире људских права или процене ризика (на нивоу корпорације, производа или технологије и / или државе) да би се утврдило може ли предузеће или ИКТ компаније да својим активностима изазива или доприноси негативним утицајима или да ли се негативни утицаји могу директно приписати његовом пословању, производима или услугама или пословним односима.
	Препознавањем утицаја на дечија права различитих старосних група као резултата пословања компаније и дизајна, развоја и увођења производа и услуга, као и могућности за подршку правима деце и младих.

Разматрања о интеграцији права детета у све одговарајуће корпоративне политике и процесе управљања (наставак)	Усвајањем приступа дјечјој заштити заснованој на оснаживању и образовању. Узимањем у обзир права детета на заштиту података, њиховог права на приватност и слободу говора, истовремено нудећи образовање и смернице кроз услуге компаније. Ослањањем на интерну и екстерну стручност и саветовање са кључним интересним странама, укључујући децу и младе, о механизмима за безбедност деце на интернету да би добили сталне повратне информације и смернице о приступима компаније.
	У државама којима недостају одговарајући правни оквири за заштиту права деце и младих на приватност и слободу изражавања, компаније би требало да обезбеде да су политике и праксе у складу са међународним стандардима. Погледати Резолуцију Генералне скупштине Уједињених нација 68/167 о праву на приватност у дигитално доба.
	Обезбеђивањем приступа правном леку успостављањем могућности жалби на оперативном нивоу и кроз механизме пријављивања било каквих кршења права детета (нпр. материјал сексуалног злостављања деце, непримерен садржај или контакт или кршење приватности).
	Именовањем руководиоца политике заштите деце или друге одређене особе која се може контактирати у вези са питањима заштите деце на интернету. Ако је дете у опасности од штете, руководилац политике заштите деце треба одмах упозорити одговарајуће власти. Уредничке смернице ББЦ-а (2019.), на пример, одређују именовање руководиоца политике заштите деце, што се у јавним медијима сматра обавезним.
Развој стандарда ИКТ компанија за заштиту деце на интернету	Направити и применити стандарде за компаније и ИКТ индустрију за заштиту деце и младих, с обзиром на специфичну индустрију и карактеристике.
Развој стандардних поступака за руковање материјалима сексуалног злостављања деце	У сарадњи са владом, органима за провођење закона, цивилним друштвом и организацијама линија за подршку, ИКТ компаније имају кључну улогу у борби за сузбијање материјала сексуалног злостављања деце предузимањем следећих радњи:
	Забранити учитавање, објављивање, пренос, дељење или стављање на располагање садржаја који крши права било које стране или крши било који локални, државни, национални или међународни закон.
	Комуницирати са националним агенцијама за провођење закона или националним линијама за подршку да би пренијели пријаве материјала сексуалног злостављања деце чим провајдер сазна за њих. Обезбедити да постоје интерне процедуре за усклађивање одговорности за пријављивање према локалним и међународним законима. Када компанија послује на тржиштима са мање развијеним регулаторним надзором и надзором над провођењем закона у вези са овим питањем, она може да упути оне који желе да поднесу пријаве на Међународно удружење интернетских линија за подршку (INHOPE), где се може извршити пријава на било којој међународној линији за подршку.

Развој стандардних поступака за руковање материјалима сексуалног злостављања деце **(наставак)**	Успоставити интерне процедуре да би се обезбедило поштовање локалних и међународних закона о борби против материјала сексуалног злостављања деце. Основати виши положај или тим посвећен интеграцији ових поступака у организацију. Чланови ИКТ индустрије би затим требало да извештавају о предузетим радњама и резултатима које је постигао овај тим у свом годишњем извештају о корпорацији и одрживости. Када национални прописи не пружају довољну заштиту, ИКТ компаније би требало да поштују, али превазиђу национално законодавство и употријебе своје могућности за лобирање за законодавне промјене да би ИКТ компанијама омогућили да се боре против материјала сексуалног злостављања деце. Унутар организације треба успоставити виши положај или тим који ће бити посвећен интеграцији ових поступака и праћењу операција. Њихов рад би требало да буде транспарентно описан у годишњим извештајима о корпорацији и одрживости и доступан јавности.
	Навести да ће предузеће у потпуности сарађивати у истрагама органа за провођење закона у случају да се незаконит садржај пријави или открије и да ће се забиљежити детаљи у вези са казнама као што су новчане казне или укидање привилегија наплате.
	Користити услове и одредбе за кориснике и / или прихватљиве политике употребе за изричито навођење става компаније о злоупотреби његових услуга за чување или дељење материјала сексуалног з лостављања деце и последицама било које злоупотребе.
	Развити поступке обавештавања, уклањања и извештавања који омогућавају корисницима да пријаве материјал сексуалног злостављања деце или непримерен контакт и одређени профил / локацију где је откривен. Успоставити извештај о пратећем поступку, договорити се о процедурама за прикупљање доказа и брзо уклањање или блокирање приступа материјалу сексуалног злостављања деце. Обезбедити да провајдери услуга, по потреби, затраже мишљење стручњака (нпр. националних органа за борбу против материјала сексуалног злостављања деце) пре уништавања незаконитог садржаја. Обезбедити да релевантне треће стране са којима је компанија у уговорном односу имају успостављене исто тако снажне процесе обавештавања и уклањања.
	Треба да буду спремне за руковање материјалом сексуалног злостављања деце и да пријаве случајеве одговарајућим властима. Ако однос са органима за провођење закона и националном линијом за подршку већ није успостављен, треба да се ангажују да заједно развијају процесе.
	Радити путем интерних функција, као што су брига о корисницима, спречавање превара и безбедност, да би се обезбиједило да предузеће може подносити пријаве за сумњу на незаконит садржај директно органима за провођење закона и линијама за подршку. У идеалном случају, то би требало учинити на начин који не излаже особље у првом реду штетном садржају нити поновно прави жртву од погођеног детета / деце и младих. Позабавити се ситуацијама у којима особље може да буде изложено изопаченом материјалу, провести политику или програм за пружање подршке за развој отпорности, безбедности и добробити особља.

Развој стандардних поступака за руковање материјалима сексуалног злостављања деце **(наставак)**	Укључити политике задржавања и чувања података за подршку органима за провођење закона у случају кривичних истрага кроз активности као што је прикупљање доказа. Документовање праксе компаније приликом руковања материјалом сексуалног злостављања деце, почевши од праћења и настављајући се до коначног преноса и уништавања садржаја. У документацију укључити списак целог особља одговорног за руковање материјалом.
	Промовисати механизме пријављивања материјала сексуалног злостављања деце и обезбедити да корисници знају како поднети пријаву ако открију такав садржај. Ако је доступна национална линија за подршку, понудите везу до те линије за подршку са корпоративне интернет странице и са било којих релевантних услуга са садржајима које компанија промовише.
	Користити се свим релевантним услугама / скуповима података да би спречили ширење познатог садржаја сексуалног злостављања деце путем својих услуга или платформи.
	Редовно активно процењивати сав садржај хостован на серверима компаније, укључујући комерцијалне (брендиране провајдере садржаја или оне уговорене са трећим лицима). Размислите о употреби алата као што су хеш скенирање познатих слика сексуалног злостављања деце, софтвер за препознавање слика или блокирање интернет адреса за борбу против материјала сексуалног злостављања деце.
Стварање безбеднијег окружења на интернету прилагођеног узрасту	ИКТ компаније могу помоћи у стварању безбеднијег, угоднијег дигиталног окружења за децу и младе свих узраста предузимањем следећих радњи:
	Усвојити принципе безбедности и приватности по дизајну у технологијама и услугама компанија и дати приоритет решењима која смањују количину података који се односе на децу на минимум.
	Применити дизајне прилагођене узрасту у понуђеним услугама. Представити деци информације о правилима интернет странице на приступачан начин и примерено њиховом узрасту, пружајући одговарајућу количину детаља. Поред одредби и услова прилагођених узрасту и који су приступачни, ИКТ компаније би на сличан начин требале и јасно преносити информације, попут правила и кључних политика. Оне би требало да нагласе прихватљиво и неприхватљиво понашање приликом коришћења услуге, последице кршења било којих правила, специфичности услуге и оно на шта корисник пристаје пријављивањем. Такве информације треба да буду посебно усмерене на младе кориснике и њихове родитеље и старатеље.
	Користити услове услуге или услове и одредбе да бисте скренули пажњу корисницима на садржај на интернет услугама компаније који можда није примерен за све узрасте. Услови и одредбе такође треба да укључују јасне механизме за пријављивање и поступање у случају кршења таквих правила.

Стварање безбеднијег окружења на интернету прилагођеног узрасту **(наставак)**	Размотрити могућност пружања механизама као што су софтвер за родитељску контролу и други алати који омогућавају родитељима и старатељима да управљају приступом деци интернетским ресурсима, истовремено им пружајући смернице о њиховој одговарајућој употреби да се не би кршила дечија права. Они укључују листе за блокирање / дозволу приступа, филтере садржаја, надзор употребе, управљање контактима и временска / програмска ограничења.
	Понудити једноставне опције родитељског надзора које родитељима и старатељима омогућавају ограничавање одређених услуга и садржаја којима деца могу да приступе када користе електронске уређаје. Ова ограничења могу да укључују контроле на нивоу интернета, уређаја и контроле апликација. С обзиром да ово има огромне импликације на дететову способност да унапреди своје дигиталне вештине и на смањивање његових могућности на интернету, ове контроле би требало да буду дизајниране за врло малу децу у складу са њиховим развојним контекстом и са одговарајућим смјерницама за родитеље.
	Тамо где је то могуће, промовисати националне службе подршке које родитељи и старатељи могу да користе за пријављивање кршења права и тражење подршке у случају злостављања или искоришћавања.
	Избегавати штетне или непримерене рекламне садржаје на интернету и успоставити обавезу за провајдере услуга да откривају клијенте са садржајем који је намијењен одраслој публици и може да буде штетан за децу и младе. Штетно оглашавање такође може да укључује оглашавање хране и пића која садрже пуно масти, шећера или соли. Ускладити пословне праксе са прописима и савјетима о маркетингу и оглашавању за децу и младе. Пратити где, када и како деца и млади могу наићи на потенцијално штетне рекламне поруке намењене другом сегменту тржишта.
	Обезбедити да се политике прикупљања података придржавају релевантних закона који се тичу приватности деце и младих, укључујући разматрање да ли је потребан пристанак родитеља пре него што комерцијална предузећа могу да прикупи личне податке од детета или о детету.
	Прилагодити и применити повишена подразумијевана подешавања приватности за прикупљање, обраду, складиштење, продају и објављивање личних података, укључујући информације у вези са локацијом и навике прегледања, прикупљене од особа млађих од 18 година. Подразумевана подешавања приватности и информације о важности приватности требало би да одговарају узрасту корисника и природи услуге.
	Применити техничке мере, као што су одговарајући алати за родитељску контролу, безбедност по дизајну, различита искуства за различите узрасте, садржај заштићен лозинком, листе за блокирање / дозволу приступа, контроле куповине / времена, функције одјаве, филтрирање и модерирање, да би се спречио приступ и изложеност малолетника непримереном садржају или услугама. Применити технологију која може идентификовати узраст корисника и представити им верзију апликације која одговара узрасту. За садржај или услуге осетљиве на узраст, интересне стране у ИКТ индустрији би требало да предузму кораке за провјеру старости корисника. Тамо где је могуће, користити провјеру старости да би ограничили приступ садржају или материјалу који је, било законом или политиком, намијењен само особама старијим од одређеног узраста. Компаније би такође требало да препознају потенцијал злоупотребе таквих технологија са циљем ограничавања права деце и младих на слободу изражавања и приступа информацијама или угрожавања њихове приватности.

Стварање безбеднијег окружења на интернету прилагођеног узрасту **(наставак)**	Обезбедити да су садржај и услуге који нису прикладни за кориснике свих старосних група: • класификовани у складу са националним стандардима и културним нормама; • у складу са постојећим стандардима у еквивалентним медијима; • идентификовани са истакнутим опцијама приказа за контролу приступа; • у понуди заједно са провером старости, где је то могуће и уз јасне услове који се односе на брисање било којих података који могу да се користе за личну идентификацију који су добијени кроз поступак провере. На пример, с обзиром на медијске стандарде, сви регулаторни органи за медије постављају низ захтјева који се односе на садржај прилагођен узрасту, а провајдери интернета морају да прилагоде спремишта и да примене смернице на своју понуду садржаја. Погледати, Ofcom у Уједињеном Краљевству, ЦСА у Француској и АГЦОМ у Италији.
	Понудити јасне алате за пријављивање и развити пратећи поступак на пријаву о непримереном садржају, контактима и злоупотребама, а корисницима услуга пружити детаљне повратне информације о процесу који се односи на пријаву.
	Обезбедити предмодерацију интерактивних простора дизајнираних за децу и младе на начине који се подударају са правима деце на приватност и њиховим развојним капацитетима. Активна модерација може да подстакне атмосферу у којој насиље и узнемиравање нису прихватљиви. Неприхватљиво понашање укључује: • објављивање неугодних или претећих коментара на нечијем профилу; • отварање лажних профила или интернет страница мржње ради понижавања жртве; • слање ланчаних порука и прилога са штетном намером; • хаковање нечијег профила ради слања увредљивих порука другима.
	Предузети посебне мере опреза са члановима особља или сарадницима који раде са децом и младима, за које може бити потребна претходна провера кривичне евиденције код полицијских власти.
	Било који инцидент сумње на врбовање одмах упутите интернетском или интерактивном извршном руководећем тиму који је одговоран за пријављивање одговарајућим властима: • пријавити врбовање извршном руководећем тиму и именованом руководиоцу политике заштите деце, где је то могуће; • омогућити корисницима да директно пријаве надлежним органима случајеве врбовања; • успоставити могућност директног контакта путем адреса е-поште ради упозорења и пријављивања.
	У сваком тренутку дати приоритет безбедности и добробити детета. Деловати увек у професионалним границама и обезбедити да је сваки контакт са децом важан за услугу, програм, догађај, активност или пројекат. Никада не преузимајте искључиву одговорност за дете. Ако је детету потребна њега, упозорити родитеља, старатеља или пратиоца. Слушати и поштовати децу у свако доба. Ако се неко понаша непримерено у близини деце, пријавите то понашање локалном контакту за заштиту деце.

Стварање безбеднијег окружења на интернету прилагођеног узрасту (наставак)	Успоставити јасан скуп правила која су на видном месту и осликавају кључне тачке из услова услуге и смерница прихватљиве употребе. Језиком који је разумљив за кориснике ова правила би требало да дефинишу: • природу услуге и шта се очекује од њених корисника; • шта је прихватљиво а шта није у смислу садржаја, понашања и језика, као и забрана незаконите употребе; • последице пропорционалне кршењу, на пример, пријављивање органима за провођење закона или суспензија корисничког профила.
	Олакшати корисницима да пријаве забринутост због злоупотребе служби за бригу о корисницима, путем успостављених стандардних и приступачних поступака за решавање различитих проблема, као што је примање нежељених комуникација (нпр. нежељене СМС поруке).
	Бити транспарентан и пружити корисницима јасне информације о природи понуђених услуга, на пример: • врста садржаја / услуге и трошкови; • минимална старосна граница потребна за приступ; • доступност родитељског надзора, укључујући оно што контроле покривају (нпр. интернет) или не покривају (нпр. Wi-Fi) и обуку о томе како их користити; • врста прикупљених корисничких података и како се користе.
	Промовисати националне службе подршке које омогућавају деци и младима да пријаве и потраже подршку у случају злостављања или искоришћавања (погледати, на пример, Child Helpline International).
Едукација деце, родитеља и едукатора о безбедности деце и њиховој одговорној употреби ИК технологија	ИКТ компаније могу да допуне техничке мере образовним активностима и активностима оснаживања предузимањем следећих радњи:
	Јасног описа доступног садржаја и одговарајуће родитељске контроле или породичних безбједоносних поставки. Учинити језик и терминологију доступним, видљивим, јасним и релевантним за све кориснике, укључујући децу, родитеље и старатеље, посебно у односу на одредбе и услове, трошкове укључене у употребу садржаја или услуга, политике приватности, безбедносне информације и механизме пријављивања.
	Обучити кориснике о начину решавања проблема у вези са употребом интернета, укључујући нежељену пошту, крађу података и непримерен контакт, попут малтретирања и врбовања, и описати које радње корисници могу да предузму и како могу да изнесу забринутост због непримерене употребе.
	Успоставити механизме и едуковати родитеље да се укључе у ИКТ активности своје деце и младих, посебно оних који имају млађу децу, тако што ће, на пример, омогућити родитељима да прегледају поставке приватности деце и младих.
	Сарађивати са владом и едукаторима да би изградили капацитете родитеља за подршку и разговор са својом децом и младима о томе да буду одговорни дигитални грађани и корисници ИК технологија.

Едукација деце, родитеља и едукатора о безбедности деце и њиховој одговорној употреби ИК технологија **(наставак)**	На основу локалног контекста, треба обезбедити образовне материјале за употребу у школама и домовима да би побољшали употребу ИК технологија код деце и младих и развили критичко размишљање да би им омогућили да се понашају безбедно и одговорно када користе услуге ИК технологија.
	Подржите кориснике ширењем смерница о породичној безбедности на интернету које подстичу родитеље и старатеље да: • се упознају са производима и услугама које користе деца и млади; • обезбеде умерену употребу електронских уређаја од стране деце и младих као дијела здравог и уравнотеженог начина живота; • пажљиво обрате пажњу на понашање деце и младих да би утврдили промене које би могле указивати на сајбер злостављање или узнемиравање.
	Пружити родитељима потребне информације да би разумели како њихова деца и млади користе услуге ИК технологија, решавали проблеме у вези са штетним садржајем и понашањем и били спремни да уче децу и младе одговорној употреби. То се може олакшати употребом алата и интеракцијом са школским дистриктима за пружање наставних планова и програма за децу и образовних материјала за родитеље у вези са безбедности на интернету.
Коришћење технолошког напретка за заштиту и образовање деце	Вештачка интелигенција која чува приватност, а која разуме текстове, слике, разговоре и контекст, може да открије и реши читав низ штета и претњи на интернету и да користи те информације за оснаживање и образовање деце да се носе с њима. Када се користи интернет у окружењу паметних уређаја, они могу да заштите податке и приватност младих, а истовремено да им дају подршку.
	Јавни сервис и национални медији могу играти кључну улогу кроз своје програмске понуде (офлајн и онлајн) за образовање родитеља и деце и њихово освешћивање о ризицима и могућностима интернетског света
Промовисање дигиталне технологије као начина за повећање грађанског ангажмана	ИКТ компаније могу да охрабре и оснаже децу и младе подржавајући њихово право на учешће кроз сљедеће радње:
	Пружање информација о услузи да би истакли користи које деца остварују понашајући се примерно и одговорно, попут употребе услуге у креативне сврхе.
	Успоставити писане поступке који обезбеђују доследно провођење политика и процеса који штите слободу изражавања за све кориснике, укључујући децу и младе, као и документацију о усклађености са тим политикама.

Промовисање дигиталне технологије као начина за повећање грађанског ангажмана **(наставак)**	**Избегавајте** прекомерно блокирање легитимног и развојно одговарајућег садржаја. Да се захтеви и алати за филтерисање не би злоупотребљавали за ограничавање приступа информацијама деци и младима, обезбедити транспарентност блокираног садржаја и успоставити поступак за кориснике који пријављују ненамерно блокирање. Овај поступак требало би да буде доступан свим потрошачима, укључујући вебмастере. Сваки поступак извештавања треба пружити јасне, одговорне и процењене услове пружања услуге.
	Развити онлајн платформе које промовишу право деце и младих на изражавање; олакшати њихово учешће у јавном животу; и подстицати њихову сарадњу, предузетништво и грађанско учествовање.
	Развити образовни садржај за децу и младе који подстиче учење, креативно размишљање и решавање проблема.
	Промовисати дигиталну писменост, изградњу капацитета и ИКТ вештине да би се деца и млади, посебно они у руралним подручјима и подручјима са недовољно високим нивоом услуга, опремили за коришћење ИКТ ресурса и потпуно безбедно учешће у дигиталном свету.
	Сарађујте са локалним цивилним друштвом и владом на националним и локалним приоритетима за ширење универзалног и равноправног приступа ИКТ-има, платформама и уређајима као и основној инфраструктури за подршку истих.
	Обавестите и укључите купце, укључујући родитеље, његоватеље, децу и младе, о понуђеним услугама, попут: • врсте садржаја и одговарајуће родитељске контроле; • механизама пријављивања случајева погрешне употребе, злоупотребе и непримереног или незаконитог садржаја; • поступака праћења извештаја; • врсте услуга које су старосно ограничене; • безбедног и одговорног коришћења интерактивних услуга „властитог бренда“.
	Бавите се ширим питањима у вези са безбедним и одговорним дигиталним грађанством, на пример интернетском репутацијом и дигиталним отиском, штетним садржајем и његом. Размислите о партнерству са локалним стручњацима, попут дечијих невладиних организација, добротворних организација и родитељских група, да бисте помогли обликовати поруку компаније и имали жељену публику.
	Ако компанија већ ради с децом или школама, на пример, кроз програме корпоративне друштвене одговорности, истражите могућност да се овај ангажман прошири на образовање и интеракцију са децом и младима као и на едукаторе о порукама у вези са заштитом деце на интернету.
Инвестирање у дигитално истраживање	Уложите у истраживање засновано на доказима и у дубинску анализу технологија, утицај технологија на децу, разматрање заштите деце и права детета с обзиром на дигитално окружење, интегрисање онлајн система заштите у услуге које користе деца и млади и боље разумевање које врсте интервенција су најефикасније у побољшању дечијих онлајн искустава.

Типологија ИКТ компанија

Иако су ове смернице Међународне уније за телекомуникације усмерене на ИКТ индустрију у целини, важно је препознати да се услуге које пружају ИКТ компаније, начин њиховог рада, регулаторне шеме у оквиру којих функционишу и предмет и обим њихових понуда веома разликују. Било која технолошка компанија чији су производи и услуге усмерени директно или индиректно на децу може да има користи од раније наведених општих принципа и може да се прилагоди на основу свог специфичног подручја деловања. Основна идеја је подржати и водити ИКТ индустрију у предузимању правих мера за бољу заштиту деце на интернету од опасности наношења штете, истовремено оснажујући децу да се крећу онлајн светом на најбољи могући начин. Типологија у наставку ће помоћи да се пружи јасније разумевање неких из циљне публике и како се исти уклапају у контролне листе у следећем одељку. Треба напоменути да су ово само неки специфични примери категорија и да нису коначни:

(а) Провајдери интернетских услуга, укључујући фиксне широкопојасне услуге или услуге мобилних мрежних оператера: иако ово обично одражава услуге које се пружају на дугорочнијој бази претплаћеним купцима, могло би се проширити и на предузећа која пружају бесплатна или плаћена јавна Wi-Fi жаришта.

(б) Друштвене мреже односно платформе за размену порука и платформе за онлајн игре. (ц) Произвођачи хардвера и софтвера, попут добављача ручних уређаја, укључујући мобилне телефоне, играће конзоле, кућне уређаје засноване на гласовној помоћи, интернет ствари и паметне дечије играчке повезане са интернетом.

(д) Компаније које пружају дигиталне медије (креатори садржаја, омогућавање приступа или хостинг садржаја).

(е) Компаније које пружају услуге преноса, укључујући преносе уживо.

(ф) Компаније које нуде услуге дигиталног складиштења датотека, добављачи услуга у облаку.

5. Контролна листа по карактеристикама

Ово поглавље допуњује претходни општи попис за индустрију нудећи препоруке за предузећа која пружају услуге са специфичним карактеристикама за поштивање и подршку дечијих права на мрежи. Сљедеће контролне листе за одређене карактеристике наводе начине допуњавања заједничких принципа и приступа представљених у Табели 1. јер они важе за различите услуге те би их стога требало узети у обзир као додатак корацима из Табеле 1.

Овде истакнуте карактеристике се пресецају и неколико контролних листа специфичних за карактеристике може да буде релевантно за исту компанију.

Следеће контролне листе су организоване и позивају се на исте кључне области као и опште смернице у Табели 1. Свака листа за проверу карактеристика развијена је са кључним сарадницима и због тога постоје мање разлике у табелама.

5.1 Карактеристика А: Обезбедити повезивање, услуге складиштења података и хостинга

Приступ интернету је основни за остваривање дечијих права, а повезаност може деци отворити читав свет. Провајдери услуга повезивања, складиштења података и хостинга имају огромне могућности да у своје понуде за децу и младе угради безбедност и приватност. Ова функција је између осталог намијењена мобилним оператерима, провајдерима интернет услуга, системима за складиштење података и услугама хостинга.

Мобилни оператери омогућавају приступ интернету и нуде низ мобилних услуга преноса података. Многи оператери су се већ пријавили на кодексе праксе заштите деце на интернету и нуде низ алата и информативних извора ради подршке својој посвећености заштити деце на интернету.

Већина провајдера интернетских услуга делује и као канал који пружа приступ интернету и са интернета и као складиште података путем својих услуга хостинга, кеш меморисања и складиштења. Као резултат тога, они су примарно одговорни за заштиту деце на интернету.

Приступ интернету на јавним мјестима

Све је уобичајеније да општине, трговци, транспортне компаније, ланци хотела и друга предузећа и организације пружају приступ интернету путем Wi-Fi и хот-спотова. Такав приступ је обично бесплатан или се пружа уз минималне трошкове, а понекад уз минималне формалности приликом пријаве као јавна услуга или од стране компаније да привуче купце у своје просторије или наведе више људи да користе њене услуге.

Промовисање Wi-Fi мреже је ефикасан начин да се обезбеди доступност интернета у одређеном подручју. Међутим, треба водити рачуна када је такав приступ омогућен у јавним просторима у којима је вероватно да ће деца редовно да бораве. Корисници морају имати на уму чињеницу да Wi-Fi сигнали могу бити доступни пролазницима, а кориснички подаци угрожени. Због тога провајдер Wi-Fi мреже неће увек бити у могућности да подрже или надзиру употребу интернет конекције коју је испоручио и корисници зато морају да предузму мере предострожности да избегавају дељење осетљивих информација путем јавно доступне Wi-Fi мреже.

У јавним просторима, провајдери Wi-Fi мреже ће можда размислити о увођењу додатних мера за заштиту деце и младих, као што су:

- Проактивно блокирање приступа веб-адресама за које се зна да садрже садржај који је неприкладан за широку публику, поред њихових напора да блокирају приступ материјалу сексуалног злостављања деце.
- Увртавање клаузула у одредбе и услове употребе којима се забрањује употреба Wi-Fi услуга за приступ или приказивање било којег материјала који је можда неприкладан у окружењу у којем бораве деца. Одредбе и услови такође треба да садрже јасне механизме у вези са посљедицама кршења таквих правила.
- Предузимање свих мера за заштиту од неовлаштеног приступа, што за резултат може имати манипулацију или губитак личних података.
- Инсталирање филтера на Wi-Fi систем ради подршке примјени правила о неприкладном материјалу.
- Обезбеђење процедура и софтвера за путоказ и нуђење опционе родитељске контроле која се односи на приступ деце и младих интернетским садржајима.

Добра пракса: Прописи о телекомуникацијама већине држава чланица Европске уније предвиђају, на пример, да приступ мрежи мора да буде идентификован путем појединачних СИМ картица или других алата за идентификацију.

Табела 2. садржи смернице за провајдере услуга повезивања, складиштења података и хостинг услуга о радњама које могу да предузму у циљу побољшања дечије онлајн заштите и дјечјег учешћа.

Табела 2. Контролна листа заштите деце на интернету за Карактеристику А: Обезбедити уређаје за повезивање, складиштење и хостинг података

Увртавање питања права детета у све одговарајуће корпоративне политике и процесе управљања	Провајдери услуга повезивања, складиштења података и хостинга могу да идентификују, спрече и ублаже негативне ефекте ИК технологија на права деце и младих и да идентификују могућности за подршку напретку деце и младих.
	Види опште Смернице у Табели 1.
Развој стандардних процеса ради решавања проблема материјала сексуалног злостављања деце	У сарадњи са владом, органима за провођење закона, цивилним друштвом и организацијама СОС сервиса, провајдери услуга повезивања, складиштења података и хостинг услуга могу да играју кључну улогу у борби против материјала сексуалног злостављања деце предузимањем следећих радњи:
	Сарадња са владом, органима за провођење закона, цивилним друштвом и организацијама СОС сервиса у борби против материјала сексуалног злостављања деце и ради пријављивања случајева одговарајућим органима. Ако сарадња са полицијом и СОС телефон за помоћ још нису успостављени, ангажујте се на заједничком успостављању сарадње.
	Провајдери услуга повезивања, складиштења података или хостинга могу такође да изврше обуку полиције из области ИК технологија.
	Ако компанија послује на тржиштима са мање развијеним правним и законским надзором овог питања, иста може упутити оне који желе да поднесу пријаве на Међународно удружење оператера интернет механизама за пријаве INHOPE (International Association of Internet Hotlines) где се пријаве могу поднијети код било ког међународног интернет механизма за пријаве.
	Размислите о постављању међународно признатих пописа за блокирање УРЛ-ова или веб-локација које су креирали одговарајући органи (нпр. Национална агенција за провођење закона или врућа линија за пријављивање, Cybertip Canada, Interpol, IWF), да би корисницима отежали приступ идентификованом злостављачком материјалу.
	Развити поступке обавештавања, уклањања и пријављивања те повезати пријаве злоупотребе са тим процесима путем споразума о јавној служби о поступку одговора и времену уклањања.
	Погледајте, на пример, УНИЦЕФ-ов и ГСМА водич о политикама и пракси обавештавања и уклањања.
	Успоставите механизам пријављивања са јасним информацијама о његовој употреби, на пример, давањем смерница о илегалном садржају и понашању које треба пријавити и појашњавањем тога који се материјали не могу приложити уз извештај да би се избјегла даљна дистрибуција на интернету.

Развој стандардних процеса ради решавања проблема материјала сексуалног злостављања деце (***наставак***)	Подржите провођење закона у случају кривичних истрага кроз активности као што је прикупљање доказа. Користите услове и одредбе услуге да бисте посебно забранили употребу услуга за складиштење, дељење или дистрибуцију материјала сексуалног злостављања деце. Обавезно наведите да ови услови јасно наводе да се материјал сексуалног злостављања деце неће толерисати. Обавезно наведите да се у условима услуге и одредбама наводи да ће компанија у потпуности сарађивати у кривичним истрагама у случају откривања или пријаве материјала сексуалног злостављања деце.
	Тренутно постоје два решења за пријављивање материјала сексуалног злостављања деце на интернету на националном нивоу: врућe линије и портали за пријављивање. Потпуну ажурну листу свих постојећих телефонских линија и портала можете пронаћи на веб-страници INHOPE. Врућe линије: Ако национална врућа линија није доступна, потражите могућности за успостављање исте (погледајте Водич за врућe линије GSMA INHOPE за низ опција, укључујући рад с INHOPE и Фондацијом INHOPE. Доступна је интерактивна верзија GSMA INHOPE водича која садржи смернице о томе како развити интерне процесе за особље за бригу о клијентима које ће подносити извештаје сумњивог садржаја полицији и мрежи INHOPE. Портали за пријављивање: IWF нуди рјешење портала за пријављивање које омогућава корисницима интернета у земљама и земљама без врућих линија да директно IWF-у пријављују слике и видеозаписе за које сумњају да могу да представљају сексуално злостављање деце и то путем посебне мрежне странице портала.
	За провајдере услуга повезивања, складиштења података и хостинг услуга чије услуге укључују неку врсту хостинга садржаја, потребно је имати успостављене поступке обавештавања и уклањања.
Стварање безбеднијег и старосно прикладног дигиталног окружења	Провајдери услуга интернет конекције, складиштења података и хостинга могу помоћи у стварању безбеднијег, угоднијег дигиталног окружења за децу свих узраста предузимањем следећих радњи:
	Провајдери услуга складиштења/хостинга података требало би да размотре представљање функције пријављивања на свим веб-страницама и сервисима као и развити и документовати јасне процесе за брзо управљање извештајима о злоупотреби или другим кршењима услова и одредби.
	Интернет провајдери би требало да понуде техничку контролу властитог бренда или да означе доступност алата које су креирали специјализовани провајдери услуга који су примјерени понуђеним услугама, а крајњи корисници их могу лако применити и понудити могућност блокирања или филтерисања приступа интернету путем корпоративне мреже. Обезбедите одговарајуће механизме за провјеру старости ако компанија нуди садржај или услуге (укључујући услуге властитог бренда или услуге треће стране које компанија промовише), које су легалне или одговарајуће за одрасле кориснике (нпр. одређене наградне игре, лутрије).

Едукација деце, родитеља и наставника о дјечјој безбедности и њиховој одговорној употреби ИК технологија	Провајдери услуга повезивања, складиштења података и хостинга требало би да понове кључне поруке из одредби и услова из смерница заједнице написаних на језику прилагођеном корисницима да подрже децу и њихове родитеље и старатеље. У оквиру саме услуге, у тренутку преношења садржаја, уврстити подсетнике на теме као што је врста садржаја која се сматра неприкладном.
	Пружите деци и младима информације о безбеднијој употреби интернета. Размотрите креативне начине за промоцију кључних порука, као што су следеће: "Никада не делите никакве контакт-информације са непознатим лицима, укључујући вашу физичку локацију и телефонски број. „Никада немојте пристати да се сами састанете са неким кога сте упознали на мрежи без претходног саветовања са одраслом особом. увек реците поузданом пријатељу где се налазите " „Не одговарајте на малтретирање, непристојне или увредљиве поруке. Али сачувајте доказе - не бришите поруку.“ "Реците одраслој особи или пријатељу од повјерења ако вам је због нечега или некога непријатно." “Никада не дајте лозинку или корисничко име налога! Имајте на уму да други људи на мрежи могу давати лажне податке да би вас уверили да поделите своје приватне податке."
	Провајдери услуга могу да се удруже са организацијама које су у добром положају ради едукације и подршке деци о безбеднијој употреби интернета и о сродним питањима. Погледајте International Helpline за децу и практични водич за ГСМА за дечије линије за подршку и мобилне операторе: Заједнички рад на заштити дечијих права.
Промовисање дигиталне технологије као начина за повећање цивилног ангажмана	*Види опште Смернице у Табели 1.*

5.2 Карактеристика Б: Понудити организовани дигитални садржај

Интернет пружа све врсте садржаја и активности, од којих су многи намењени деци и младима. Сервиси који нуде професионално уређен садржај имају огромне могућности да у своје понуде за децу и младе угради безбедност и приватност.

Ова услуга се односи на предузећа која креирају сопствени садржај као и на она која омогућавају приступ дигиталном садржају. Између осталог, ово се односи на услуге стриминга вести и мултимедије, националну и јавну радиодифузију и индустрију игара на срећу.

Табела 3. садржи смернице за провајдере услуга које нуде професионално уређен садржај о политикама и радњама које могу предузети у циљу побољшања дечије онлајн заштите и дјечјег учешћа.

Табела 3. Контролна листа заштите деце на интернету за Карактеристику Б: Понудити организовани дигитални садржај

Увртавање питања права детета у све одговарајуће корпоративне политике и процесе управљања	Сервиси који нуде професионално уређен садржај могу да помогну да се идентификују, спрече и ублаже негативни утицаји ИК технологија на права деце и младих и да идентификују могућности за подршку напретку деце и младих предузимањем следећих радњи:
	Развити политике које штите добробит деце и младих који доприносе садржајима на мрежи да би се узела у обзир физичка и емоционална добробит и достојанство лица млађих од 18 година која су укључена у програме, филмове, игре, вести итд. без обзира на пристанак који је могао дати родитељ или друго одрасло лице.
Развијање стандардних процеса за борбу против материјала сексуалног злостављања деце	У сарадњи с државом, полицијом, цивилним друштвом и организацијама врућих линија за подршку, компаније које нуде професионално уређен дигитални садржај могу играти кључну улогу у борби против МСЗД путем следећих активности: У случајевима МСЗД, на пример путем функција „коментарисања“ или „прегледа“, при чему корисници имају капацитет за учитавање садржаја, особље би требало да контактира извршни руководећи тим одговоран за пријављивање таквог материјала одговарајућим органима. Поред тога, потребно је: • одмах упозорити националне агенције за провођење закона; • упозорити руководство агенције и пријавити материјал менаџеру политике заштите деце; • контактирати службу интерне истраге телефоном или е-поштом са детаљима инцидента и затражити савет; • пре брисања материјала, складиштења у заједнички простор или прослеђивања причекајте савет надлежне агенције;
	• имплементирати брзу и ефикасну стратегију ескалације ако је материјал сексуалног злостављања деце објављен или се сумња на незаконито понашање; у ту сврху: • понудити корисницима једноставан и лако доступан начин упозоравања произвођача садржаја на кршење било којих правила онлајн заједнице; • уклонити садржај којим се крше правила; • понудити корисницима једноставан и лако доступан начин упозоравања произвођача садржаја на кршење било којих правила онлајн заједнице; • уклонити садржај којим се крше правила. • пре слања професионално уређеног садржаја са старосним ограничењем на друштвене мреже, припазите на услове и одредбе веб-странице. Пратите минималне старосне захтеве на различитим страницама за друштвено умрежавање. • Одредбе и услови сваког интернет простора треба такође да садрже јасне механизме извештавања о кршењу таквих правила.

Развој стандардних процеса ради решавања проблема материјала сексуалног злостављања деце

Ако је материјал идентификован, треба га пријавити директно организацији специјализованој за интернет безбедност која управља системом извештавања путем јавне телефонске линије и ИТ професионалцима ради пријављивања специфичних облика потенцијално илегалних интернетских садржаја.
На пример, на основу своје политике заштите деце, ББЦ је објавио уредничке смернице о интеракцији са децом и младима на интернету.
ББЦ је развио додатне контролне листе и кодексе понашања за рад са децом и младима на интернету, које се такође односе на подизвођаче и спољне провајдере услуга.
Политика заштите деце регулатора за комуникације у Великој Британији (Ofcom) одвојено се бави онлајн садржајем, мобилним уређајима и играћим конзолама.

Стварање безбеднијег и старосно прикладног дигиталног окружења	Компаније које нуде професионално уређени дигитални садржај могу помоћи у стварању безбеднијег и пријатнијег дигиталног окружења за децу и младе свих узраста предузимањем следећих радњи:
	Сарађујте са другима из бранше да бисте развили системе класификације/оцењивања садржаја који се заснивају на прихваћеним националним или међународним стандардима и у складу са приступима који се заузимају у еквивалентним медијима. где је то могуће, класификација садржаја требало би да буде конзистентна на различитим медијским платформама, на пример, најава филма у биоскопу и на паметном телефону корисницима би приказивала исте класификације.
	Развити производе прилагођене деци и старосно прилагођене садржаје за децу и младе који су осмишљени као безбедни и надограђени поузданим системом провере старости.
	Да бисте помогли родитељима и другима да одлуче да ли је садржај старосно примерен за децу и младе, изградите апликације и услуге на свим медијима да би се ускладили са системима оцењивања садржаја. Усвојите одговарајуће методе провере старости да бисте спречили децу и младе да приступају старосно осетљивом садржају, веб-локацијама, производима или интерактивним услугама. Пружите савете и подсетнике о природи и старосној класификацији садржаја који користе.
	Компанија која нуди аудиовизуелне и мултимедијске услуге можда жели дати лични идентификациони број корисницима који желе да приступе садржају који може да буде штетан за децу и младе.
	Обезбедите транспарентност цена за производе и услуге и прикупљене информације о корисницима. Побрините се да се политике прикупљања података придржавају релевантних закона који се тичу приватности деце и младих, укључујући и то да ли је потребан пристанак родитеља пре него што комерцијална предузећа могу прикупљати личне податке од детета или о њему.
	Побрините се да оглашавање или комерцијална комуникација буду јасно препознатљиви као такви. Надгледајте садржај који је доступан онлајн и прилагодите га корисничким групама које ће му вероватно приступити, на пример, успостављањем одговарајућих правила за онлајн оглашавање деци и младима. Ако понуда садржаја подржава интерактивни елемент, као што је коментарисање, онлајн форуми, друштвене мреже, платформе за игре, чет собе или огласне плоче, успоставите јасан скуп „кућних правила“ на језику прилагођеном купцима у оквиру услуга и корисничких смерница.
	Одлучите који је ниво ангажмана потребан пре покретања онлајн услуге. Услуге усмерене на привлачење деце требало би да представљају само садржаје који су прикладни за младу публику. Ако постоје сумње, могу се консултовати државни органи надлежни за заштиту деце.
	Обезбедити јасно и истинито означавање садржаја. Имајте на уму да корисници могу доћи до непримереног садржаја следећи везе на веб-локацијама трећих страна које заобилазе странице за контекстуализацију садржаја.

Едукација деце, родитеља и едукатора о дјечјој безбедности и њиховој одговорној употреби ИК технологија	Компаније које нуде професионално уређен дигитални садржај могу да допуне техничке мере образовним активностима које оснажују децу предузимањем следећих радњи:
	Пружите купцима конкретне и јасне информације о садржају, као што су врста садржаја, старосне оцене односно ограничења, увредљив језик или насиље и одговарајуће доступне родитељске контроле; и информације о томе како пријавити злоупотребу и непримерен или незаконит садржај и како ће се поступати с извештајима. У интерактивном свету ове информације се дају у облику ознака садржаја за сваки програм.
	Подстакните одрасле, посебно родитеље, његоватеље и старатеље, да буду укључени у потрошњу интернетског садржаја деце и младих да би могли помоћи и усмјеравати децу и младе у избору садржаја приликом куповине и помоћи у успостављању правила понашања. Помозите деци (и родитељима и старатељима) да науче управљати својим временом испред екрана и разумију како користити технологију на начин који им одговара, укључујући и то када треба престати и радити нешто друго.
	Пренесите правила употребе на јасном и доступном језику који подстичу децу и младе на опрез и одговорност када сурфују интернетом.
	Креирајте алате прилагођене старости, попут туторијала и центара за помоћ. По потреби сарађујте са интернет или личним превентивним програмима и терапеутским клиникама. На пример, ако постоји ризик да се деца и млади превише баве технологијом, што им отежава развијање личних односа или учешће у здравим физичким активностима, веб-странца може дати линк за линију за помоћ или терапеутску службу. Нека безбедносне информације, попут линкова за савете, буду истакнуте, лако доступне и јасне када буде велика могућност да ће онлајн садржај привући велики број деце и младих.
	Понудите алат за родитељско навођење, као што је „брава“ за контролу садржаја којем се може приступити путем одређеног претраживача.
	Сарађујте са родитељима да бисте били безбедни да их информације објављене на интернету о деци не излажу ризику. Начин препознавања деце у професионално уређеном садржају захтева пажљиво разматрање и варира у зависности од контекста. Прибавите информисани пристанак деце када их приказујете у програмима, филмовима, видео-записима итд. где год је то могуће, и поштујте свако одбијање учешћа.

Промовисање дигиталне технологије као начина ка додатном цивилном ангажману	Компаније које нуде професионално уређени дигитални садржај могу охрабрити и оснажити децу и младе подржавајући њихово право на учешће кроз сљедеће активности:
	Креирајте, односно понудите низ висококвалитетних, изазовних, едукативних, пријатних и занимљивих садржаја који одговарају узрасту и помажу деци и младима да схвате свет у којем живе. Осим што је атрактиван и употребљив, поуздан и безбједан, такав садржај може да допринесе физичком, менталном и социјалном развоју деце и младих пружајући нове могућности за забаву и образовање. Потребно је снажно подстицати садржаје који деци омогућавају да прихвате различитост и буду позитивни узори.

5.3 Карактеристика Ц: Складиштити садржај који генеришу корисници и повежите кориснике

Раније су интернет светом доминирали одрасли, али сада је јасно да су деца и млади главни учесници на више платформи у стварању и дељењу експлозије садржаја који генеришу корисници. Ова функција се, између осталог, бави услугама друштвених медија, апликацијама и веб-локацијама повезаним са креативном реализацијом.

Сервиси који међусобно повезују кориснике могу да се поделе у три категорије:

- Првенствено апликације за размену порука (Facebook Messenger, Groupme, Line, Tinder, Telegram, Viber, WhatsApp).
- Првенствено услуге друштвених мрежа које траже и складиште садржај који генеришу корисници и који омогућавају корисницима да деле садржај и повезују се унутар и изван својих мрежа (Инстаграм, Facebook, SnapChat, TikTok).
- Првенствено апликације за стриминг уживо (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

Провајдери услуга захтевају минималну старост за пријаву на платформе, али то је тешко провести јер се провера старости ослања на пријављену старост. Већина услуга које међусобно повезују нове кориснике такође омогућавају функције дељења локације, што чини децу и младе који користе ове услуге још осетљивијима на опасности ван интернета.
Табела 4. која је прилагођена правилима која примењује једна од највећих друштвених мрежа, пружа смернице за провајдере услуга који врше хостинг садржаја који креирају корисници и повезују нове кориснике о политикама и радњама које могу предузети да би унаприједили онлајн заштиту и укљученост деце.

Табела 4. Контролна листа заштите деце на интернету за Карактеристику Ц: Складиштити садржај који генеришу корисници и повежите кориснике

Увртавање питања права детета у све одговарајуће корпоративне политике и процесе управљања	Сервиси који врше хостинг садржаја који генеришу корисници и који повезују кориснике могу да идентификују, спрече и ублаже негативне ефекте ИК технологија на права деце и младих и да идентификују могућности за подршку напретку деце и младих.
	Види опште Смернице у Табели 1.
Развој стандардних процеса ради решавања проблема материјала сексуалног злостављања деце	У сарадњи с владом, органима за провођење закона, цивилним друштвом и организацијама СОС сервиса, компаније које врше хостинг садржаја који генеришу корисници и које повезују кориснике могу играти кључну улогу у борби против материјала сексуалног злостављања деце предузимањем следећих радњи:
	Успоставите процедуре за све локације за пружање непосредне помоћи полицији током ванредних ситуација и за рутинске истраге.
	Наведите да ће предузеће у потпуности сарађивати у истрагама у случају да се незаконити садржај пријави или открије и забележите детаље у вези са таквим казнама као што су новчане казне или укидање привилегија наплате.
	Радите са интерним функцијама као што су брига о купцима, спречавање превара и безбедност да бисте били безбедни да компанија може подносити извештаје о сумњи на илегални садржај директно полицији и линијама за подршку. У идеалном случају, то би требало урадити на начин који не излаже садржају особље које ради директно са клијентима нити поново виктимизира угрожено дете/децу и младе. Да бисте се позабавили ситуацијама у којима особље може да буде изложено насилном материјалу, имплементирајте политику или програм за подршку отпорности, безбедности и добробити особља.
	Примените услове из уговора о вршењу услуге и услове за забрану илегалног садржаја и понашања, истичући да: • штетни садржаји, укључујући сумњу на педофилско зближавање са децом са намјером било физичког или нефизичког злостављања, неће бити толерисани: • противзаконити садржај, укључујући аплод или даљне ширење материјала сексуалног злостављања деце, неће бити толерисан; • компанија ће се обратити и у потпуности сарађивати у кривичним истрагама у случају да се пријави или открије противзаконити садржај или било које кршење политике заштите деце.
	Документујте праксу компаније за руковање материјалом сексуалног злостављања деце, почевши од надгледања и проширивања до коначног преноса и уништавања садржаја. У документацију уврстите списак свог особља одговорног за руковање материјалом.
	Усвојите политике у вези са власништвом над садржајем који креирају корисници, укључујући опцију уклањања садржаја који креирају корисници на захтев корисника. Уклоните садржај којим се крше правила провајдера, а о кршењу упозорите корисника који је поставио предметни садржај.

Успостављање стандардних процеса за борбу против МСЗД **(*наставак*)**	Наведите да ће непоштовање политика од стране корисника имати последице, укључујући: • уклањање садржаја, суспензију или затварање налога прекршиоца; • опозив опције дељења одређених врста садржаја или коришћења одређених опција; • спречавање контакта са децом; • пријављивање случаја надлежним органима.
Успостављање стандардних процеса за борбу против МСЗД	Промовишите механизме извештавања за МСЗД или било који други илегални садржај и обезбедите услове да клијенти знају поднети пријаву ако открију такав садржај. Успоставите системе и обезбедите обучено особље за процјену појединачних случајева и предузимање одговарајућих мера. Успоставите добро организоване и свеобухватне оперативне тимове за корисничку подршку. Идеално би било да се ови тимови обуче за решавање различитих врста инцидената да би се дао адекватан одговор и предузеле одговарајуће радње. Када корисник поднесе жалбу, зависно од врсте инцидента, потребно је корисника упутити одговарајућем особљу. Компанија би такође могла да успостави посебне тимове за решавање жалби корисника у случајевима када су извјештаји можда поднесени грешком.
	Успоставите процесе за тренутно уклањање или блокирање приступа материјалу сексуалног злостављања деце, укључујући процесе обавештавања и уклањања илегалног садржаја одмах након идентификовања истог. Побрините се да треће стране са којима је компанија у уговорном односу имају сличне ефикасне поступке обавештавања и уклањања. Ако законодавство дозвољава, материјал се може чувати као доказ кривичног дела у случају истраге.
	Успоставити техничке системе који могу открити познати илегални садржај и спријечити његово учитавање, укључујући и учитавање у приватне групе, или га означити за тренутни преглед од стране безбједносног тима компаније. Предузмите све одговарајуће мере заштите сервиса од злоупотребе у погледу хостинга, дистрибуирања или креирања материјала сексуалног злостављања деце. где је то могуће, успоставите проактивне техничке мере за анализу предмета и метаподатака повезаних са профилом ради откривања криминалног понашања или образаца и предузмите одговарајуће мере.
	Ако апликација или услуга омогућава корисницима да преносе и чувају фотографије на серверима који су у власништву компаније или којима се компанија служи, успоставите процесе и алате за препознавање слика које ће највјероватније садржавати материјал сексуалног злостављања деце. Размотрите проактивне технике идентификације као што су технологија скенирања или људски преглед.

Стварање безбеднијег и старосно прикладног дигиталног окружења	Провајдери услуга који нуде садржај креиран од стране корисника могу помоћи у стварању безбеднијег, угоднијег дигиталног окружења за децу свих узраста предузимањем следећих радњи:
	На језику прилагођеном купцима, а у оквиру услуге и корисничких смерница, дефинишите јасан скуп „кућних правила“ којима се дефинише следеће: • природа услуге и оно што се очекује од њених корисника; • шта јесте, а шта није прихватљиво у смислу садржаја, понашања и језика, као и забрану илегалне употребе; • последице кршења, као на пример пријављивање полицији и суспензија корисничког рачуна.
	Кључне безбедносне и правне поруке требале би бити представљене у старосно прилагођеном формату (тј. користећи интуитивне иконе и симболе) приликом регистрације и приликом предузимања различитих радњи на веб страници.
	Олакшајте клијентима да корисничком сервису пријаве проблем злоупотребе, користећи успостављене стандардне и приступачне поступке за решавање различитих проблема, попут примања нежељених комуникација (нежељене поште, малтретирања) или гледања непримереног садржаја.
	Омогућите подешавања видљивости и поделе садржаја прилагођена узрасту. На пример, нека поставке приватности и видљивости за децу и младе буду по дифолту рестриктивније од поставки за одрасле.
	Успоставите минималне старосне захтеве и подржите истраживање и развој нових система за провјеру старости, попут биометрије, користећи познате међународне стандарде за развој таквих алата. Предузмите кораке за идентификовање и уклањање малољетних корисника који су погрешно приказали своју старост да би добили приступ. Потребно је размотрити додатно прикупљање личних података које би могло обухватити и овај проблем, као и потребу ограничења прикупљања и чувања ових података и њихове обраде. Ако то већ није успостављено, успоставите одговарајуће процесе пријаве да бисте утврдили јесу ли корисници довољно стари за приступ садржају или услузи без угрожавања њиховог идентитета, локације и личних података. Користите национално успостављене функционалне системе за провјеру старости према потреби, тамо где постоје релевантне мере за заштиту приватности података деце. Функција извештавања или служба за помоћ/центар која може подстакнути кориснике да пријаве људе који су погрешно приказали своју старост.

Стварање безбеднијег и старосно прикладног дигиталног окружења (***наставак***)	Заштитите млађе кориснике од нежељене комуникације и обезбедите да се успоставе смернице о приватности и прикупљању информација.
	Пронађите начине да прегледате ускладиштене слике и видео-записе и избришете неприкладне кад их откријете. Алати као што су *hash* скенирање познатих слика и софтвер за препознавање слика су вам на располагању као помоћ. У услугама усмјереним на децу, фотографије и видео-записи могу се претходно провјерити да би се обезбиједило да деца не објављују осјетљиве личне податке о себи или другима.
	Бројне мере могу да се користе за контролу приступа садржају који генеришу корисници и за заштиту деце и младих на мрежи од неприкладног или илегалног садржаја. Обавезно користите безбедне лозинке као корак у циљу заштите деце и младих у играма и другим поставкама друштвених медија. Остале технике укључују: • преглед дискусионих група ради утврђивања штетних предмета, говора мржње и незаконитог понашања и брисање таквог садржаја када се утврди да крши услове коришћења; • премодерисање огласних плоча са тимом специјализованих модератора за децу и младе који проверавају садржај који је у супротности с објављеним "кућним редом". Свака порука се може провјерити пре објављивања, а модератори такође могу да уоче и означе сумњиве кориснике, као и кориснике у невољи; • успостављање тима домаћина заједнице (*хост*) који служе као прва тачка контакта за модераторе када имају проблем у вези са корисником.
	Будите одговорни за преглед комерцијалног садржаја, укључујући форуме, друштвене мреже и веб-локације за игре.

Едукација деце, родитеља и едукатора о безбедности деце и њиховој одговорној употреби ИК технологија	Провајдери услуга који нуде садржај који генеришу корисници могу допунити техничке мере образовним активностима и активностима оснаживања предузимањем следећих радњи:
	Креирајте део посвећен безбедносним саветима, чланцима, карактеристикама и дијалогу о дигиталном држављанству, као и линковима до корисног садржаја независних стручњака. Безбједносни савјети морају да буду лако уочљиви и написани лако разумљивим језиком. Такође се провајдери платформи подстичу да имају јединствени навигациони интерфејс на различитим уређајима, попут рачунара, таблета или мобилних телефона.
	Понудите родитељима јасне информације о врстама садржаја и доступним услугама, укључујући, на пример, објашњење веб локација друштвених мрежа и услуга заснованих на локацији, начин приступа интернету путем мобилних уређаја и опције доступне родитељима за примену контрола.
	Обавестите родитеље о начину пријављивања злоупотребе, погрешне употребе и непримереног или незаконитог садржаја као и о начину на који ће пријава бити решавана. Обавестите их које су услуге ограничене на старост и друге начине за безбедно и одговорно понашање приликом коришћења интерактивних услуга.
	Успоставите систем заснован на „поверењу и угледу“ да би се подстакло добро понашање и омогућило вршњацима да примером преносе најбоље праксе. Промовишите важност друштвеног извештавања, које омогућава људима да се обрате другим корисницима или поузданим пријатељима да би помогли у решавању сукоба или започели разговор о забрињавајућем садржају.
	Пружите савете и подсетнике о природи дате услуге или садржаја и о томе како безбедно уживати у њему. Уградите смернице заједнице у интерактивне услуге, на пример, са поп-ап обавјештењима која подсјећају кориснике на одговарајуће и безбедно понашање, попут недавања њихових контакт информација.
	Сарађујте са родитељима да бисте били сигурни да их информације објављене на интернету о деци не излажу ризику. Прибавите информисани пристанак деце када их приказујете у програмима, филмовима, видео-записима итд. где год је то могуће, и поштујте свако одбијање учешћа.
Промовисање дигиталне технологије као начина за повећање грађанског ангажмана	Компаније које нуде професионално уређени дигитални садржај могу охрабрити и оснажити децу и младе подржавајући њихово право на учешће.
	Види опште Смернице у Табели 1.

5.4 Карактеристика Д: Системи вођени вјештачком интелигенцијом

Са повећаном пажњом која се даје технологијама за учење, појмови „вјештачка интелигенција“, „машинско учење“ и „дубоко учење“ широко су у употреби у истом значењу као одраз концепта репликације „интелигентног“ понашања у машинама. У овом делу се фокусирамо на начине на које процеси машинског учења и дубоког учења утичу на дјечји живот и, коначно, на њихова људска права.

„Због експоненцијалног напретка технологија заснованих на вештачкој интелигенцији у последњих неколико година, тренутни међународни оквир који штити дечија права не бави се изричито многим питањима која су покренута развојем и употребом вештачке интелигенције. Међутим, овај оквир идентификује неколико права која могу бити имплицирана овим технологијама и на тај начин пружа важно полазиште за сваку анализу тога како нове технологије могу позитивно или негативно да утичу на дечија права, попут права на приватност, образовање и играње, као и права на недискриминацију."

Примена вештачке интелигенције може да замени утицај на децу разних услуга које се користе на друштвеним мрежама, попут платформи за стриминг видео-записа. Технологија екрана осјетљивог на додир и дизајн ових платформи омогућавају врло малој деци да прегледају и крећу се овим садржајем. Посебна је забринутост да алгоритми који користе препоручене видео-записе могу да з а р о б е децу у „филтер мехурићима“ лошег или неприкладног садржаја. Како су деца посебно подложна препорукама за садржај, шокантни "повезани видео-записи" им могу привући пажњу и одвратити их од програмирања прилагођенијег деци.

Вештачка интелигенција такође има утицаја на онлајн заштиту деце с обзиром на паметне играчке. Различити процеси који су укључени у рад паметних играчака долазе са својим властитим изазовима, тј. играчком (која се повезује с дететом), мобилном апликацијом која се користи као приступна тачка за Wi-Fi везу и персонализованим онлајн налогом играчке, односно потрошача, где се подаци чувају. Такве играчке комуницирају са серверима заснованим на облаку који чувају и обрађују податке које пружају деца која комуницирају с играчком. Овај модел има безбедносне проблеме ако се безбедност не примењује на сваком нивоу, што су показали бројни случајеви хаковања у којима су процурили лични подаци. Штавише, неки хаковани уређаји (укључујући паметне уређаје с прикључком на интернет, попут бејби монитора, гласовних помоћника итд.) могу се користити за надзор корисника без њиховог знања или пристанка.

При интеграцији механизама одговора на откривене претње деци која користе ове уређаје, на пример, давањем савета и препорука на основу откривеног понашања (као што је раније споменуто у апликацији ББЦ Own It), пресудно је да компаније које дизајнирају паметне уређаје заснивају ове препоруке на доказима и развијају их у договору са стручњацима за заштиту деце.

Иако неке компаније унапређују принципе за етичку употребу вештачке интелигенције, није јасно постоје ли јавне политике усмерене на вештачку интелигенцију и децу. Неколико технолошких и трговинских удружења и група за информатику израдили су етичке принципе у вези са вештачком интелигенцијом. Међутим, они се не односе изричито на права детета, начине на које ове технологије вештачке интелигенције могу створити ризик за децу или проактивне планове за њихово ублажавање.

УНИЦЕФ и УЦ Беркелеу, “Завршни извештај: Вјештачка интелигенција и дечија права”, 2018.

19 Ibid.

20 Ibid.

21 Види Microsoft, "Најважнија питања људских права”, извештај - ФУ17; и Google, “Одговорни развој вештачке интелигенције” (2018).

22 Званични блог Microsoft-a, “Компјутеризована будућност: Вјештачка интелигенција и њена друштвена улога ”, 2018.

The Guardian, “‘Партнерство у вези вештачке интелигенције које су формирали Гоогле, Facebook, Амазон, ИБМ и Microsoft ”, 2016.

„Попут корпорација, владе широм света усвојиле су стратегије за будуће лидере о развоју и употреби вештачке интелигенције, подстичући окружење погодно за иноваторе и корпорације.“ Међутим, нејасно је како се такве националне стратегије директно баве дечијим правима.

Унапређење приступа Facebook-а садржају повезаном са самоубиством и самоповређивањем

У 2019. години, Facebook је почео организовати редовне консултације са стручњацима из целог света ради разговора о неким тежим темама повезаним са самоубиством и самоповређивањем. Ове теме обухватају питања попут како поступати опроштајним писмима самоубица, ризицима повезаним са депресивним садржајем на интернету и значајним приказима самоубиства. Додатни детаљи ових састанака доступни су на Facebook-овој новој страници за превенцију самоубистава, у његовом Безбедносном центру. Ове консултације за резултат су имале неколико побољшања у начину на који Facebook обрађује ову врсту садржаја. На пример, ојачана је политика у вези са самоповређивањем да би се забранило графичко резање слика ради избегавања ненамерног промовисања или изазивања самоповређивања. Чак и када неко тражи подршку или тврди да помаже опоравак, Facebook сада приказује упозорење преко слика залечених посекотина од самоповређивања. Ова врста садржаја сада се открива применом вештачке интелигенције, при чему се аутоматски могу предузети радње на потенцијално штетном садржају, укључујући уклањање истог или додавањем упозорења да се ради о осетљивом садржају. Од априла до јуна 2019. године, Facebook је интервенисао код више од
1,5 милиона садржаја самоубистава и самоповређивања на својој веб-локацији и открио више од 95 посто истих пре него што их је корисник пријавио. У истом периоду, Инстаграм је интервенисао код више од 800 хиљада сличних садржаја, од којих је више од 77 посто откривено пре него што их је корисник пријавио.

Идентификовање потенцијалног малтретирања или вршњачког насиља у стварном времену и слање порука

Инстаграм успоставља вештачку интелигенцију да би искоријенио понашање попут вређања, срамоћења и непоштовања. Коришћењем софистикованих алата за извјештавање, модератори могу брзо затворити налог починиоца онлајн малтретирања.

24 Ibid.

Добра пракса: Употреба вештачке интелигенције у идентификацији материјала сексуалног злостављања деце

Надовезујући се на Microsoft-ов великодушни допринос PhotoDNA у борби против експлоатације деце и недавно покретање Google АПИ-ја за безбедност садржаја, Facebook је такође развио технологије за откривање садржаја сексуалног злостављања деце.

Познате као PDQ и TMK + PDQF, ове технологије су део сета алата које Facebook користи за откривање штетног садржаја. Остали алгоритми и алати доступни индустрији укључују pHash, aHash и dHash. Facebook алгоритам за подударање фотографија, PDQ, дугује велику инспирацију pHash-у, иако је од темеља креиран као посебан алгоритам са независном софтверском имплементацијом. Технологију за подударање видео записа, TMK + PDQF, заједнички су развили Facebook-ов тим за истраживање вештачке интелигенције и научници са Универзитета у Модени и Reggio Emilia у Италији.

Ове технологије стварају ефикасан начин складиштења датотека у облику кратких дигиталних хашева који могу утврдити да ли су две датотеке исте или сличне, чак и без оригиналне слике или видео-записа. Хашеви се такође могу лакше делити са другим компанијама и непрофитним организацијама.

PDQ и TMK + PDQF су дизајнирани за рад у великим размјерама, подржавајући хаширање видео-фрејмова и апликација у реалном времену.

У Табели 5. су дате неке од препорука предузећима за усклађивање својих принципа приликом дизајнирања и имплементације решења намењених деци, а заснованих на вештачкој интелигенцији.

Ове препоруке се заснивају на УНИЦЕФ-овом раду на изради глобалних смерница политике о вештачкој интелигенцији и деци, које ће бити намењене државама и стручњацима из ове области.
Види https://www.unicef.org/globalinsight/featured-projects/ai-children за додатне информације о пројекту. Препоруке се такође ослањају на рад УНИЦЕФ-а и студије Универзитета Калифорније у Berkeley-у о вештачкој интелигенцији и правима детета.

УНИЦЕФ и УЦ Berkeley, “Завршни извештај: Вјештачка интелигенција и дечија права”, 2018.

Табела 5: Контролна листа заштите деце на интернету за Карактеристику Д: Системи вођени вјештачком интелигенцијом

Увртавање питања права детета у све одговарајуће корпоративне политике и процесе управљања	Провајдери система вођених вјештачком интелигенцијом могу да идентификују, спријече и ублаже негативне ефекте ИК технологија на права деце и младих и да идентификују могућности за подршку напретку деце и младих.
	Системи вештачке интелигенције треба да се дизајнирају, развијају, имплементирају и истражују да би се поштовала, промовисала и испуњавала дечија права, како је утврђено у Конвенцији о правима детета. Дјетињство, које се све више одвија у дигиталном окружењу, време је посвећено посебној њези и помоћи. Системе вештачке интелигенције треба искористити тако да ову подршку пруже у пуном потенцијалу.
	Уврстите инклузивни приступ дизајну при развоју производа за децу, чиме се посвећује максимална пажња родној, географској и културној разноликости и укључује широк спектар интересних страна, попут родитеља, наставника, дечијих психолога и, према потреби, саме деце.
	Требало би успоставити оквире управљања, укључујући етичке смернице, законе, стандарде и регулаторне органе ради надзора процеса којима се спречава да се примена система вештачке интелигенције не крше дечија права.
Развој стандардних процеса ради решавања проблема материјала сексуалног злостављања деце	У сарадњи са државом, органима за провођење закона, цивилним друштвом и организацијама за подршку на врућим линијама, провајдери система вођених вјештачком интелигенцијом играју кључну улогу у борби против материјала сексуалног злостављања деце предузимањем следећих радњи:
	Види опште Смернице у Табели 1.

Стварање безбеднијег и старосно прикладног дигиталног окружења	Провајдери система вођених вјештачком интелигенцијом могу да помогну у стварању безбеднијег, угоднијег дигиталног окружења за децу свих узраста предузимањем следећих радњи:
	Усвојите мултидисциплинарни приступ приликом развијања технологија које утичу на децу и консултујте се са цивилним друштвом, укључујући академску заједницу, да би се идентификовали потенцијални утицаји ових технологија на права различитих врста потенцијалних крајњих корисника.
	Примените планирану безбедност и планирану приватност за производе и услуге којима се деца баве или их често користе.
	Како су системи вештачке интелигенције "гладни" података, компаније које користе вештачку интелигенцију за своје услуге требало би да користе посебну будност у погледу прикупљања, обраде, складиштења, продаје и објављивања личних података деце. Системи вештачке интелигенције би требало да буду транспарентни тако да би могло бити могуће открити како и зашто је систем донио одређену одлуку или, у случају робота, поступио на начин на који је поступио. Ова транспарентност је пресудна за развијање повјерења и олакшавање ревизије, истраге и надокнаде када се сумња на штету деце. Побрините се да постоје функционални и законски механизми за помоћ ако деца јесу или ако тврде да су оштећена системима вештачке интелигенције. Потребно је успоставити процесе за благовремено исправљање свих дискриминаторних резултата и успоставити надзорне органе за жалбе и континуирано праћење дечије безбедности и заштите. Одговорност и механизми за обештећење иду руку под руку.
	Сачинити планове за руковање посебно осетљивим подацима, укључујући откривања злоупотребе или друге штете која може да се подијели са компанијом путем њених производа. Дигиталне платформе и системи вештачке интелигенције требало би да смање прикупљање података о деци и повећају дечију контролу над подацима које креирају. Услови употребе треба да буду разумљиви деци да би оснажили своју свијест и способност.
Едукација деце, родитеља и едукатора о дјечјој безбедности и њиховој одговорној употреби ИК технологија	Пружаоци система вођених вештачком интелигенцијом могу да допуне техничке мере образовним активностима и активностима оснаживања.
	Требало би бити могуће објаснити сврху система са вјештачком интелигенцијом деци корисницима и њиховим родитељима или старатељима да би их оснажили да одлуче користити или одбити такве платформе.

Промовисање дигиталне технологије као начина за повећање грађанског ангажмана	Компаније које нуде системе вођене вештачком интелигенцијом могу да охрабре и оснаже децу и младе подржавајући њихово право на учешће. *Види опште Смернице у Табели 1.*
Коришћење технологије	Системи вођени вештачком интелигенцијом требало би да се развијају да би подржали дечји напредак у заштити развоја и благостања као резултат у целом дизајну система, те едуковали децу о развоју и имплементацији. Њихове референте тачке требало би да буду најбоље доступне и широко прихваћене метрике развоја и благостања. Компаније би требало да улажу у истраживање и развој етичких алата заснованих на вештачкој интелигенцији за откривање радњи онлајн материјала сексуалног злостављања деце и онлајн узнемиравања и малтретирања и то у сарадњи са кључним стручњацима за дечија права и децом. Напредак у технологији вештачке интелигенције требало би да се примијени на циљани, старосно прилагођени *messaging* сервис за децу и то без угрожавања њиховог идентитета, локације и личних података.

Референце

Текст Опште уредбе о заштити података (Уредба (ЕУ) 2016/679 Парламента и Савета Европе од 27. априла 2016. О заштити физичких лица у вези са обрадом личних података и слободном кретању тих података, а којом се ван снаге ставља Директива 95/46/ЕЦ (Општа уредба о заштити података) и њен текст објављен у Службеном листу ЕУ.

Измењена Директива о АВМС (услугама аудиовизуелних медија) којом се ван снаге ставља Директива 2010/13/ЕУ о координацији одређених одредби прописаних законом, прописа или управних радњи у државама чланицама у вези с пружањем аудиовизуелних медијских услуга (Директива о аудиовизуелним медијским услугама) с обзиром на промену тржишне стварности и Текста објављеног у Службеном листу ЕУ.

ББЦ политика:

- Политика заштите деце и провођења мера заштите деце, верзија 2017., ревидирана 2018. и ажурирана верзија 2019.
- Оквир за независне продуцентске куће које раде на продукцијама ББЦ-а о правилима екстерних провајдера о заштити деце;
- Смернице: Интеракција са децом и младима на мрежи путем уредничких смерница за онлајн активности

Истрага којом се доказује непоштовање старосне верификације за друштвене медије у Великој Британији: 2016, 2017; 2020.

Објашњења појмова

Дефиниције у наставку су углавном изведене из постојеће терминологије утврђене у Конвенцији о правима детета, 1989. године, као и од Међуагенцијске радне групе за сексуално искоришћавање деце у Терминолошким смјерницама за заштиту деце од сексуалног искоришћавања и сексуалног злостављања, 2016. (Луксембуршке Смернице), Конвенције Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања, 2007., као и УНИЦЕФ-овог Глобал Кидс Онлајн извјештаја, 2019.

Адолесцент

Адослесценти су лица старости између 10 и 19 година. Важно је напоменути да „адолесценти“ нису обавезујући појам према међународном праву, а они млађи од 18 година сматрају се децом, док се 18-годишњаци сматрају одраслима осим ако је праг пунолетности нижи према раније прописаном националном закону.

Вештачка интелигенција

У најширем смислу, израз „вештачка интелигенција“ се нејасно односи на системе који су чиста научна фантастика (тзв. "јака“ вештачка интелигенција са самосвесном формом) и системе који су већ оперативни и способни за обављање врло сложених задатака (ови системи су описани као „слаба“ или „умерена“ вештачка интелигенција, попут препознавања лица или гласа и управљања возилима.)

Системи вештачке интелигенције

Систем вештачке интелигенције је систем заснован на машини који може, за одређени скуп циљева које дефинише човјек, давати предвиђања, препоруке или одлуке које утичу на стварно или виртуелно окружење. Системи вештачке интелигенције су осмишљени за функционисање на различитим нивоима аутономије.

Алекса

Амазон Алекса, познат једноставно као Алекса, виртуелни је асистент заснован на вештачкој интелигенцији, а развио га је Амазон. Способан је за гласовну интеракцију, репродукцију музике, прављење листа обавеза, постављање аларма, стриминг подкастова, репродукцију аудио-књига и пружање информација о времену, саобраћају, спорту и другим информацијама у стварном времену попут вести. Алекса такође може да контролише неколико паметних уређаја користећи самог себе као систем за аутоматизацију куће. Корисници могу да п рошире Алексине могућности инсталирањем "вештина" (додатна функционалност коју су развили независни добављачи, које се у другим поставкама чешће називају апликацијама попут програма за временску прогнозу и аудио-карактеристика).

УНИЦЕФ и ИТУ, “Смернице за ИКТ компаније у погледу безбедности деце на интернету”, 2014.
савет Европе, “Шта је вјештачка интелигенција?”.
ОЕЦД (2019), Препоруке савета о вештачкој интелигенцији, https://webcache.googleusercontent
УНИЦЕФ и ИТУ, “Смернице за ИКТ компаније у погледу безбедности деце на интернету”, 2014.

Најбољи интерес детета

Описује све елементе потребне за доношење одлуке у одређеној ситуацији за одређено дете или групу деце.

Дете

У складу са чланом 1. Конвенције о правима детета, дете је свако млађи од 18 година осим ако је праг пунољетности нижи према раније прописаном националном закону.

Сексуално искоришћавање и злостављање деце

Описује све облике сексуалног искоришћавања и злостављања деце, нпр. (а) подстицање или принуђавање детета да се бави било којом незаконитом сексуалном активношћу; (б) искоришћавање деце за проституцију или друге незаконите сексуалне радње; (ц) израбљивачка употреба деце у порнографским изведбама и материјалима", као и„ сексуални контакт који обично укључује силу над лицем без пристанка истог." Сексуално искоришћавање и злостављање деце се све чешће одвија путем интернета или у вези са онлајн окружењем.

Сексуално искоришћавање и злостављање деце

Брза еволуција ИК технологија створила је нове облике сексуалног искоришћавања и злостављања деце на интернету, који могу да се одвијају виртуелно и не морају укључивати физички сусрет лицем у лице са дететом. Иако правни системи у великом броју држава још увек означавају слике и видео-записе детета сексуалног злостављања као „дечију порнографију" или „недоличне слике деце", ове смернице се колективно односе на субјекте као материјал за сексуално злостављање деце. Ово је у складу са Смјерницама Комисије за широкопојасну мрежу и одговором глобалне сарадње у борби против сексуалног искоришћавања и злостављања деце "WePROTECT Global Alliance Model National Response ". Овај појам прецизније описује садржај. Порнографија се односи на закониту, комерцијализовану индустрију, а како Луксембуршке Смернице наводе да употреба овог израза:

„може (ненамјерно или не) допринијети смањењу тежине, банализацији или чак легитимизацији онога што је заправо сексуално злостављање, односно сексуално искоришћавање деце […] Овај термин ризици „дечије порнографије" инсинуира да се дела врше уз пристанак детета и представљају „легитимни сексуални материјал". Израз материјал за сексуално злостављање деце односи се на материјал који представља дела која су сексуално насилна, односно израбљивачка по дете. То између осталог укључује материјале којима се снима сексуално злостављање деце од стране одраслих; слике деце укључене у сексуално експлицитно понашање; полни органи деце када се слике производе или користе првенствено у сексуалне сврхе.

Види Луксембуршке Смернице за изразе попут „компјутерски или дигитално генерисан материјал сексуалне злоупотребе деце".

Види Конвенцију УН о правима детета.
УНИЦЕФ и ИТУ, "Смернице за ИКТ компаније у погледу безбедности деце на интернету", 2014.
Члан 34 Конвенције УН о правима детета.
„Терминолошке Смернице за заштиту деце од сексуалног искоришћавања и сексуалне злоупотребе" (Луксембуршке Смернице), 2016.
Луксембуршке Смернице (како је горе наведено), 2016 и извештај мреже Глобал Кидс Онлајн, 2019.
Комисија о широкопојасној мрежи за одрживи развој, " Child Online Safety: Минимизација ризика од онлајн сиља, злоупотребе и искоришћавања", 2019; WePROTECT Global Alliance, "Спречавање и борба против сексуалног искоришћавања и злостављања деце (ЦСЕА):Модел националног одговора", 2016.

Деца и млади

Описује лица млађа од 18 година, при чему појам "деца", која се у смерницама такође називају и млађом децом, обухвата сва лица млађа од 15 година и млађа лица између 15 и 18 година старости.

Играчке са интернет конекцијом

Играчке са интернет конекцијом се повезују на интернет помоћу технологија као што су Wi-Fi и Bluetooth и обично раде заједно са пратећим апликацијама да би деци омогућиле интерактивну игру. Према Juniper Research-у, тржиште онлајн играчака у 2015. достигло је 2,8 милијарди УСД, а предвиђа се да ће се до 2020. повећати на 11 милијарди УСД. Ове играчке прикупљају и чувају личне податке од деце, укључујући имена, геолокацију, адресе, фотографије, аудио и видео-записе.

Сајбер малтретирање

Термином сајбер малтретирање се описује намерни агресивни чин који су више пута извршили група или појединац користећи дигиталну технологију и циљајући жртву која се не може лако бранити. То обично укључује „употребу дигиталне технологије и интернета за објављивање штетних информација о некоме, намерно дељење приватних података, информација, фотографија или видео-записа на штетан начин, слање претећих или увредљивих порука (путем е-поште, размене тренутних порука, чета, текстова), ширење гласина и лажних података о жртви или њихово намерно искључивање из онлајн комуникације".

Сајбер мржња, дискриминација и насилни екстремизам

„Сајбер мржња, дискриминација и насилни екстремизам су различити облик сајбер насиља јер циљају колективни идентитет, а не појединце […] који се често односе на расу, сексуалну оријентацију, религију, националност или имиграциони статус, пол/род и политику".

Дигитално грађанство

Дигитално грађанство се односи на способност позитивног, критичког и компетентног укључивања у дигитално окружење, ослањања на вештине ефикасне комуникације и стварања, практиковање облика друштвене партиципације који поштују људска права и достојанство одговорном употребом технологије.

Jeremy Greenberg, "Опасне игре: Играчке са интернет конекцијом, Закон о заштити дечије приватности и лоша безбедност", Georgetown Law Technology Review, 2017.
Anna Costanza Baldry et al. "Сајбер малтретирање и сајбер виктимизација наспрам родитељског надзора, праћења и контроле онлајн активности адолесцената", Преглед услуга за децу и младе, 2019.
Луксембуршке Смернице 2016 и извештај мреже Глобал Кидс Онлајн, 2019. (како је горе наведено), УНИЦЕФ Global Kids Online Report, 2019 (како је горе наведено).
Council of Europe, "Дигитално грађанство и едукација о дигиталном грађанству"

Дигитална писменост

Дигитална писменост значи имати вештине потребне за живот, учење и рад у друштву у ком се комуникација и приступ информацијама све више врши путем дигиталних технологија попут интернет платформи, друштвених медија и мобилних уређаја. Укључује јасну комуникацију, техничке вештине и критичко размишљање.

Дигитална отпорност

Овај појам описује способност детета да се емоционално носи са повређивањем на интернету. Такође се односи на емоционалну интелигенцију потребну да би се разумјело када је дете на мрежи у опасности, знало како затражити помоћ, научило из искуства и да би се опоравило када ствари крену по злу.

Управници

Описује сва лица која су на положају у управној или руководећој структури школе.

(Онлајн) педофилско зближавање

Педофилско (онлајн) зближавање, како је дефинисано у Луксембуршким смјерницама, односи се на „поступак успостављања/изградње односа са дететом лично или путем интернета или других дигиталних технологија да би се олакшао сексуални контакт на интернету или ван њега". То је кривична активност зближавања са дететом ... ,са циљем наговарања детета на сексуални однос.

Информационе и комуникационе технологије

Информационе и комуникационе технологије (ИКТ) описују све информационе технологије којима се истиче аспект комуникације. То укључује све услуге и уређаје за интернетско повезивање, између осталог рачунаре, лаптопе, таблете, паметне телефоне, играће конзоле и паметне сатове. Поред тога, укључује услуге као што су радио и телевизија, широкопојасни, мрежни хардвер и сателитске системе.

Играње онлајн игрица

„Онлајн играње" се дефинише као играње било које врсте појединачне или вишенаменске комерцијалне дигиталне игре путем било ког уређаја повезаног на интернет, укључујући наменске конзоле, десктоп компјутере, лаптопове, таблете и мобилне телефоне. „Екосистем онлајн игара" дефинисан је тако да укључује гледање других како играју видео-игре путем е-спорта, стриминга или платформе за размену видео-записа, што обично пружа могућност гледаоцима да коментаришу или комуницирају са играчима и осталим члановима публике.

Western Sydney University, "Шта је дигитална писменост?".
Dr Andrew K. Przybylski, et al., "Подијељена одговорност: Развијање онлајн отпорности детета", Virgin Media and Parent Zone, 2014.
УНИЦЕФ и ИТУ, "Смернице за ИКТ компаније у погледу безбедности деце на интернету", 2014.
(како је наведено изнад)
УНИЦЕФ, дечија права и онлајн играње: Прилике и изазови за децу и ИКТ дјелатност", 2019.

Контролни алати родитеља

Софтвер који омогућава корисницима, обично родитељу, да контролишу неке или све функције рачунара или другог уређаја који се могу повезати на интернет. Такви програми обично могу да ограниче приступ одређеним врстама или класама веб-локација или мрежних услуга. Неки програми такође пружају обим управљања временом, тј. уређај се може поставити тако да има приступ интернету само у одређеним терминима. Напредније верзије могу да сниимају све текстове послате или примљене са уређаја. Ови програми су обично заштићени лозинком.

Лични подаци

Овај појам описује информације о особи које се могу појединачно идентификовати и које се прикупљају онлајн. То укључује пуно име и презиме, контакт-информације попут кућне адресе и адресе е-поште, бројеве телефона, отиске прстију или материјала за препознавање лица, бројеве обезбеђења или било који други фактор који омогућава физичко или онлајн контактирање или локализацију особе. У овом контексту, ово се односи и на све информације о детету и његовој пратњи које пружаоци услуга прикупљају на мрежи, укључујући повезане играчке и интернет ствари као и било коју другу технологију повезану на интернет.

Приватност

Приватност се често мери у смислу дељења личних података на мрежи, поседовања јавног профила на друштвеним мрежама, дељења информација са људима које су деца упознала на мрежи, коришћења поставки приватности, дељења лозинки са пријатељима и бриге о приватности.

Јавни сервиси

Реч је о националним емитерима или медијима који су дозволу за емитовање добили на основу низа уговорних обавеза са државом или парламентом. Ове обавезе у многим земљама протеклих година проширене су на сузбијање последица дигиталне трансформације путем медија и програма дигиталне писмености и обавеза решавања дигиталне поделе.

Секстинг

Секстинг се обично дефинише као слање, примање или размена лично произведеног сексуалног садржаја, укључујући слике, поруке или видео-записе путем мобилних телефона, односно интернета. Стварање, дистрибуција и поседовање сексуалних слика деце је незаконито у већини земаља. Ако се открију сексуалне слике деце, одрасли их не би требало да гледају. Дељење сексуалних слика одрасле особе са дететом увек је кривично дело које може бити штетно и можда ће бити потребно пријавити такве слике и уклонити их.

УНИЦЕФ и ИТУ, "Смернице за ИКТ компаније у погледу безбедности деце на интернету", 2014. (како је наведено изнад)
Комисија за трговину САД (1998), Закон о заштити приватности деце на дигиталним мрежама, 1998.
Луксембуршке Смернице, 2016 (како је наведено изнад).

Сексуално изнуђивање деце („sextortion“)

Сексуално изнуђивање је „уцењивање особе уз помоћ властитих слика те особе да би се од исте изнудиле сексуалне услуге, новац или друге користи под претњом дељења материјала мимо пристанка приказане особе (нпр. објављивање слика на друштвеним мрежама) ”

Интернет ствари

Интернет ствари представља следећи корак ка дигитализацији друштва и економије, где су предмети и људи међусобно повезани комуникационим мрежама и извештавају о свом статусу односно окружењу.

УРЛ

Скраћеница од „јединствени локатор ресурса“ (енгл. *uniform resource locator*), што је адреса интернет странице.

Виртуелна стварност

Виртуелна стварност је употреба рачунарске технологије за стварање ефекта интерактивног тродимензионалног света у ком објекти имају осећај просторне присутности.

WI-FI

Wi-Fi (engl. *Wireless Fidelity*) је група техничких стандарда који омогућавају пренос података путем бежичних мрежа.

Луксембуршке Смернице, 2016 (како је наведено изнад).
Европска комисија, “Политика: Интернет ствари".
УНИЦЕФ и ИТУ, “Смернице за ИКТ компаније у погледу безбедности деце на интернету”, 2014. (како је наведено изнад)
НАСА, “Виртуелна стварност: Дефиниција и захтеви”.
Комисија за трговину САД (1998), Закон о заштити приватности деце на дигиталним мрежама, 1998.

With the support of: