# Смјернице за ИКТ компаније у погледу безбједности дјеце на интернету 2020.

# Смјернице за ИКТ компаније у погледу безбједности дјеце на интернету

# Признања

Ове смјернице 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 дјеце, а укључују ЕБУ, Глобално партнерство за заустављање насиља над дјецом, 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 смјернице ИТУ-а не би биле могуће без времена, ентузијазма и преданости аутора који су дали свој допринос. Непроцјењиве 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 безбједнијим мјестом за дјецу и младе. ИТУ је захвалан сљедећим партнерима који су дали своје драгоцјено вријеме 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 дјецом)
- 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 прије него што одштампате овај извјештај.

# Предговор

Експлозија дигиталних технологија створила је без преседана могућности за дјецу и младе да комуницирају, повезују се, дијеле, 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 дјечју безбједност и добробит - како на интернету тако и ван њега. Од питања приватности, вршњачког насиља и насилног и/или непримјереног садржаја за одређени узраст, до превараната на интернету и злочина над дјецом као што су врбовање, сексуално злостављање и искоришћавање на интернету, данашња дјеца суочена су са многим ризицима. Пријетње се умножавају, а починиоци све више истовремено дјелују преко граница, што њихово праћење чини тешким, а још теже их је процесуирати.

Уз то, глобална пандемија вируса Ковид-19 забиљежила је пораст броја дјеце која су се први пут придружила свијету на интернету, да би подржала своје студије и одржала социјалну интеракцију. Због ограничења која је наметнуо вирус не само да су млађа дјеца 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 дјецом, стављајући младе људе у ризик да приступе непримјереном садржају или да буду на мети криминалаца у производњи материјала сексуалног злостављања дјеце (ЦСАМ).

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

Технологије у настајању могу да буду дио рјешења, на примјер Интерполова база података о сексуалном злостављању дјеце заснована на вјештачкој интелигенцији која користи софтвер за поређење слика и видео-записа за брзо успостављање веза између жртава, насилника и мјеста. Али сама технологија неће ријешити 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 смјерница у погледу безбједности дјеце на интернету. Ове нове ИТУ смјернице су преиспитане, поново написане и преобликоване да би одражавале врло значајне помаке у дигиталном крајолику у којем се дјеца 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 дјеца са инвалидитетом, за коју свијет на интернету нуди посебно пресудан спас за пуно и испуњено друштвено учествовање.

Технолошка индустрија има пресудну и проактивну улогу у успостављању основа за безбједнију и заштићенију употребу интернетских услуга и других технологија за данашњу дјецу и будуће генерације.

Предузеће мора све више стављати дјечје 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 дјеце и обезбјеђујући да постоје системи који ефикасно рјешавају повреде дјечјих права када се догоде.

Тамо гдје домаћи закони још увијек 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 смјернице ИКТ компанијама послужити као чврст основ на којем ће се развијати пословне политике и иновативна рјешења. У правом духу улоге ИТУ-а као глобалног сазивача, поносна сам на чињеницу да су ове смјернице 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 дјеце на интернету Сангоа: пријатељски настројеног и неустрашивог лика којег је у потпуности дизајнирала група дјеце као дио ИТУ-овог новог међународног програма информисања младих.

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

Дорин Богдан-Мартин
Директорица Бироа за развој
телекомуникација, ИТУ

# Садржај


Признања ii

Предговор v

1. Преглед 1

2. Шта је заштита дјеце на интернету? 3

2.1 Основне информације 5

2.2 Постојећи национални и транснационални модели за заштиту дјеце на интернету 13

3. Кључна подручја заштите и промоције дјечјих права 15

3.1 Разматрања о интеграцији права дјетета у све одговарајуће корпоративне политике и процесе управљања 15

3.2 Развој стандардних поступака за руковање материјалима сексуалног злостављања дјеце 17

3.3 Стварање безбједнијег окружења на интернету прилагођеног узрасту 19

3.4 Едукација дјеце, родитеља и едукатора о безбједности дјеце и њиховој одговорној употреби ИК технологија 22

3.5 Промовисање дигиталне технологије као начина за повећање грађанског ангажмана 26

4. Опште смјернице за ИКТ компаније 27

5. Контролна листа по карактеристикама 37

5.1 Карактеристика А: Обезбиједити повезивање, услуге складиштења података и хостинга 37

5.2 Карактеристика Б: Понудити организовани дигитални садржај 41

5.3 Карактеристика Ц: Складиштити садржај који генеришу корисници и повезати кориснике 46

5.4 Карактеристика Д: Системи вођени вјештачком интелигенцијом 51

Референце 57

Објашњења појмова 58

## Табела

Табела 1. Опште смјернице за ИКТ компаније 28

Табела 2. Контролна листа заштите дјеце на интернету за Карактеристику А: Обезбиједити уређаје за повезивање, складиштење и хостинг података 39

Табела 3. Контролна листа заштите дјеце на интернету за Карактеристику Б: Понудити организовани дигитални садржај 42

Табела 4. Контролна листа заштите дјеце на интернету за Карактеристику Ц: Складиштити садржај који генеришу корисници и повежите кориснике 47

Табела 5. Контролна листа заштите дјеце на интернету за Карактеристику Д: Системи вођени вјештачком интелигенцијом 55

# 1. Преглед

Сврха овог документа је да пружи смјернице интересним странама ИКТ компанија да изграде властите ресурсе за заштиту дјеце на интернету (ЦОП). Циљ ових смјерница за ИКТ компаније у погледу безбједности дјеце на интернету је пружити користан, флексибилан и једноставан за коришћење оквир за визије предузећа и њихову одговорност да заштите кориснике. Оне су такође усмјерене на стварање основа за безбједнију и заштићенију употребу интернетских услуга и сродних технологија за данашњу дјецу и будуће генерације.

Као алат, ове смјернице такође имају за циљ јачање пословног успјеха помажући великим и малим предузећима и интересним странама да развију и одржавају атрактиван и одржив пословни модел, уз разумијевање правне и моралне одговорности према дјеци и друштву.

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

Нове смјернице за ИКТ компаније у погледу безбједности дјеце на интернету резултат су консултација са члановима Иницијативе за заштиту дјеце 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 смјернице за ИК технологије и интернетску индустрију и релевантне интересне стране;
- пружи смјернице компанијама о идентификацији, спречавању и ублажавању било каквих негативних утицаја њихових производа и услуга на дјечја права;
- пружи смјернице компанијама о утврђивању начина на које могу да промовишу дјечја права и одговорно дигитално грађанство међу дјецом;
- 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 дјеце на интернету је сложен изазов који укључује више различитих управљачких, политичких, оперативних, техничких и правних аспеката. Ове смјернице покушавају да ријеше, организују и одреде приоритете за многа од ових подручја, на основу постојећих и добро познатих модела, оквира и других референци.

Смјернице се фокусирају на заштиту дјеце у свим подручјима и од свих ризика дигиталног свијета 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 дјеце 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 дјелују (попут материјала сексуалног злостављања дјеце на интернету) путем својих услуга, већ се такође фокусирају и на друга питања која не могу да се дефинишу као кривична дјела 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 пријетње, које у одређеном контексту могу да буду штетне за дјецу.

У ту сврху ове смјернице укључују препоруке о доброј пракси у отклањању ризика са којима се дјеца суочавају у дигиталном свијету и како поступати у циљу успостављања безбједног окружења за дјецу на интернету. Ове смјернице дају савјете о томе како ИКТ компаније могу да раде на обезбјеђењу дјечје безбједности 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 вјештачком интелигенцијом. Стога пружају преглед кључних питања и изазова у вези са заштитом дјеце на интернету и предлажу акције за предузећа и интересне стране за развој локалних и унутрашњих политика заштите дјеце на интернету. Ове смјернице не покривају аспекте као што су стварни процес развоја или текст који би политике ИКТ компанија у вези са заштитом дјеце на интернету могле да обухвате.

## Структура

**Одјељак 1** - Преглед: Овај одјељак истиче сврху, обим и циљну публику ових смјерница.

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

**Одјељак 3** – Кључна подручја заштите и промоције дјечјих права: Овај одјељак наводи пет кључних подручја у којима компаније могу да предузму мјере да би обезбиједиле дјеци безбједну и позитивну употребу ИК технологија.

**Одјељак 4** – Опште смјернице: Овај одјељак даје препоруке свим интересним странама у ИКТ индустрији у погледу дјечје безбједности приликом употребе ИК технологија и промоцији позитивне употребе ИК технологија, укључујући одговорно дигитално грађанство међу дјецом.

**Одјељак 5** - Контролна листа у вези са карактеристикама: Овај одјељак истиче посебне препоруке за интересне стране о конкретним акцијама за поштовање и подршку дјечјим правима, са сљедећим карактеристикама:

- Карактеристика А: Обезбиједити 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] Дјечја права и пословни принципи позивају предузећа да испуне своју одговорност да поштују дјечја права избјегавањем 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 избјегло наношење штете дјеци) и подршке (на примјер, предузимањем добровољних акција којима се жели унаприједити остваривање дјечјих права). Предузећа треба да обезбиједе дјечја права како на заштиту на интернету, тако и на приступ информацијама и слободу изражавања, истовремено промовишући позитивну употребу ИК технологија од стране дјеце.



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

Традиционалне разлике између различитих дијелова индустрије телекомуникација и мобилне телефоније, као и интернетских 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 дијеловима свијета. Сарадња и партнерство су основе успостављања темеља за заштићенију и безбједнију 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 дјелује у пет кључних подручја, како је описано у одјељку 3.

## 2. Шта је заштита дјеце на интернету?

Током посљедњих 10 година, употреба и улога интернета у животима људи знатно су се промијенили. 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 свјетске популације користило је интернет. Највећи дио 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 дијете (0-18 година), а УНИЦЕФ процјењује 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, дијељење и комуникацију.

Предности употребе ИК технологија укључују шири приступ информацијама о социјалним услугама, образовним ресурсима и здравственим савјетима. Док дјеца 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 дјеце и младих од насиља и искоришћавања. Провајдери услуга дјечје 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 свијета, омогућавајући дјеци 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 дјеци 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 размјене и извор забаве.

Упркос дубоким предностима интернета, дјеца 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 осјетљивих личних података или на интернету или путем "секстинга", често не успијевајући да схвате импликације својих поступака на себе и

[2] ОЕЦД, "Нове технологије и дјеца 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 дјетета, која је најратификованији међународни уговор о људским правима,[3] утврђује грађанска, политичка, економска, социјална и културна права дјеце. Њиме се утврђује да сва дјеца 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 дјецу и младе од свих облика насиља, искоришћавања, злостављања и дискриминације било које врсте, и утврђује да би најбољи интерес дјетета 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 дјецу и младе у њиховом преласку у одрасло доба. Владе имају важну улогу у обезбјеђивању да све такве интересне стране испуне ту улогу.

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

Иако интернетске технологије дјеци и младима нуде бројне могућности за комуникацију, учење нових вјештина, креативност и допринос за побољшање друштва за све, оне такође могу да представљају нове ризике за безбједност дјеце и младих. Могу да изложе дјецу и младе потенцијалним ризицима и штетама у вези са питањима приватности, незаконитог садржаја, узнемиравања, сајбер малтретирања, злоупотребе личних података или врбовања у сексуалне сврхе, па чак и сексуалног злостављања и искоришћавања дјеце. Могу да буду изложени и репутацијској штети, укључујући „осветничку порнографију“ повезану с објављивањем осјетљивих 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 у вези са приватношћу на интернету када користе интернет. Дјеца, по природи својих година и зрелости, често нису у стању у потпуности да схвате ризике повезане са интернетским свијетом и могуће негативне посљедице за друге и себе због свог непримјереног понашања.

Упркос предностима, постоје и недостаци у употреби нових и напреднијих технологија. Развој вјештачке интелигенције и машинског учења, виртуелне и проширене стварности, великих података, роботике и интернета ствари има за циљ да још више трансформише медијску праксу дјеце и младих. Иако се ове технологије претежно развијају да би проширили обим пружања услуга и побољшале погодност (путем, на примјер, гласовне помоћи, приступачности и нових облика дигиталног урањања), неке такве технологије могу да имају ненамјерне посљедице, па чак и да их злостављачи дјеце користе да служе њиховим потребама. Стварање заштићеног и безбједног интернетског окружења за дјецу и омладину захтијева ефикасно учествовање влада, приватног сектора и свих интересних страна. Фокусирање на дигиталне вјештине 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 дјетета УН-а. Све земље осим три (Сомалија, Јужни Судан и Сједињене Америчке Државе) ратификовале су Конвенцију о правима дјетета.

Нека дјеца можда добро разумију ризике на интернету и како на њих одговорити. Међутим, то се не може рећи за сву дјецу 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 дјецом, заштита дјеце на интернету је од виталног значаја.

Од 2009. године, Иницијатива заштите дјеце на интернету, међународна акција са више интересних страна коју је покренуо ИТУ, има за циљ подизање свијести о ризику за дјецу на интернету и да одговори на те ризике. Иницијатива окупља партнере из свих сектора глобалне заједнице да би дјеци свуда обезбиједили безбједно интернетско искуство. Као дио Иницијативе, ИТУ је 2009. године објавио сет смјерница за заштиту дјеце на интернету за четири групе: дјецу, родитеље, старатеље и едукаторе, ИКТ компаније, и креаторе политика. Заштита дјеце на интернету подразумијева се у овим смјерницама као свеобухватан приступ да се одговори на све потенцијалне пријетње и штете са којима се дјеца и млади могу да суоче било на интернету или на некој од интернетских технологија. У овом документу заштита дјеце на интернету такође укључује штету нанијету дјеци која се догоди ван интернета, али је повезана са доказима о насиљу и злостављању на интернету. Поред разматрања дјечјег понашања и активности дјеце на интернету, заштита дјеце на интернету такође се односи на злоупотребу технологије од стране особа које нису дјеца ради искоришћавања дјеце.

Све релевантне интересне стране имају улогу у помагању дјеци 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 дјеце 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 обезбиједе да дјеца и млади могу да остваре свој потенцијал - на интернету и ван њега.

Иако не постоји универзална дефиниција, заштита дјеце на интернету има за циљ цјеловит приступ изградњи безбједних, прикладних за све узрасте, инклузивних и партиципативних дигиталних простора за дјецу и младе, које карактеришу:

- реаговање, подршка и самопомоћ у случају суочавања са пријетњама;
- спречавање штета;
- динамичан баланс између обезбјеђења заштите и пружања могућности дјеци да буду дигитални грађани;
- подржавање права и одговорности и дјеце и друштва.

Штавише, због брзог напретка у технологији и друштву и безграничне природе интернета, заштита дјеце 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 рјешења за те изазове.

## 2.1 Основне информације

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

Таква повезаност изузетно оснажује. Свијет интернета омогућава дјеци и младима да превроде недостатке и инвалидитет, а пружио је нова мјеста 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 свјесни да дјеца и млади људи често почињу да користе платформе и услуге прије него што достигну дефинисану минималну старосну границу које се технолошка индустрија мора придржавати, па би зато образовање уз мјере заштите требало интегрисати у све интернетске услуге које користе дјеца.

### 2.1.1 Дјеца у дигиталном свијету

#### Приступ интернету

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

У 2017. години, на регионалном нивоу, приступ интернету за дјецу и младе био је чврсто повезан са нивоом националног дохотка. Земље са ниским приходима имају тенденцију да имају мање дјеце корисника интернета него земље са високим приходима. Дјеца 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 просјеку 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 рјешавању дјечјих 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, „Безбједност дјеце на интернету: Смањење ризика од насиља, злостављања и искоришћавања на интернету (2019),” *Комисија за широкопојасни приступ за одрживи 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 дјецом и младима најпопуларнији уређај за приступ интернету је мобилни телефон, а слиједе га стони рачунари и лаптопи. Дјеца и млади проводе у просјеку два сата дневно на интернету у току седмице и четири сата сваког дана викенда. Док се неки осјећају трајно повезанима, многи други још увијек немају приступ интернету код куће. У пракси већина дјеце и младих који користе интернет имају приступ путем више уређаја, а они који се барем једном недјељно повезују понекад користе и до три различита уређаја. Старија дјеца и дјеца у богатијим земљама углавном користе више уређаја, а дјечаци користе нешто више уређаја него дјевојчице у свим анкетираним земљама.

Најпопуларнија активност - и за дјевојчице и за дјечаке је гледање видео-исјечака. Више од три четвртине дјеце и младих који користе интернет кажу да видео-исјечке гледају на интернету барем једном седмично, било сами или с другим члановима своје породице. Многа дјеца и млади људи могу се сматрати 'активним социјализаторима' користећи неколико платформи друштвених медија као што су Facebook, Twitter, TikTok или Инстаграм. Дјеца 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 дјецу и младе. Међутим, доступност и приступачност игара на интернету брзо се мијењају, а старосна граница дјеце и младих који први пут приступају играма на интернету се смањује.

Недјељно се 10%-30% дјеце и младих који се користе интернетом - која су консултована у одабраном низу земаља - бави креативним активностима на интернету.[1] У образовне сврхе, многа дјеца 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 дјеца имају већи апетит за информацијама од млађе дјеце.

[1] Livingstone, S., Kardefelt Winther, D., и Hussein, M. (2019.). Глобал Кидс Онлајн упоредни извјештај, извјештај 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 дјеце на интернету

Сексуално искоришћавање и злостављање дјеце (ЦСЕА) на интернету расте запањујућом брзином. Прије десет година било је мање од милион досјеа материјала о злостављању дјеце. 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 дјеце на интернету припадају свим старосним групама, али постају све млађе. Године 2018. мрежа линија за подршку INHOPE забиљежила је промјену профила жртава са пубертетских на предпубертетске. Поред тога, истраживање ЕЦПАТ International-а и ИНТЕРПОЛ-а у 2018. години показало је да су млађа дјеца била подложнија да буду подвргнута тешком злостављању, укључујући мучење, насилно силовање или садизам. То укључује новорођенчад која су стара само неколико дана, седмица или мјесеци. Иако су дјевојчице погођеније, злостављање дјечака може бити теже. Исти извјештај показује да су 80% жртава о којима се говори у извјештајима биле дјевојчице, а 17% дјечаци. Дјеца оба пола наведена су у 3% процијењених извјештаја.[1]

**Снимак података**[2]

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

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

[1] ЕЦПАТ и Интерпол, “У сусрет глобалном показатељу о неидентификованим жртвама у материјалу сексуалног искоришћавања дјеце: сажети извјештај”, 2018.
[2] Заустављање насиља над дјецом, “Безбједни на интернету”.

## 2.1.2 Утицај различитих платформи на дјечје дигитално искуство

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

Када дјеца користе **друштвене медије**, имају користи од многих прилика за истраживање, учење, комуникацију и развијање кључних вјештина. Дјеца друштвене мреже виде као платформе које им омогућавају да истражују своје личне идентитете у безбједном окружењу. Имати одговарајуће вјештине и знати како ријешити 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", дјечак који има 14 година, Чиле.*

Међутим, с обзиром на то да истраживања показују да већина дјеце користи друштвене медије прије навршених тринаест година, а услуге провјере годишта су углавном слабе или их нема, ризици са којима се дјеца могу да сусрену могу да буду веома велики. Даље, док дјеца желе да науче дигиталне вјештине, 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 дјечјом природном знатижељом и уопштено са нижим прагом страха од ризика, може да их учини рањивим на врбовање, искоришћавање, малтретирање или друге врсте штетног садржаја или контаката.

Раширена популарност размјене слика и видео-записа путем мобилних апликација, а посебно коришћење платформи за стримовање уживо од стране дјеце представља даљњу забринутост у вези са приватношћу и ризиком. Нека дјеца стварају сексуалне слике себе, пријатеља, браће и сестара и дијеле 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 дјевојке узраста од 11 до 13 година, већином у својим спаваћим собама или другим собама у кућном окружењу. За неку, посебно старију дјецу, то може да се сматра природним истраживањем сексуалности и сексуалног идентитета, док за другу, посебно млађу дјецу, често постоји присила одрасле особе или другог дјетета. Без обзира на случај, резултирајући садржај је у многим земљама незаконит и може да изложи дјецу ризику од кривичног гоњења или може да се користи за даљње искоришћавање дјетета, врбовање или изнуђивање.

Слично томе, **игре на интернету** омогућавају дјеци да испуне своје основно право на игру, као и да граде мреже, проводе вријеме са пријатељима и упознају нове пријатеље и развијају важне вјештине. 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 дјецу. То укључује претјерано играње, финансијске ризике повезане са прекомјерним куповинама у игри, прикупљање и уновчавање личних података дјеце од стране актера из ИКТ индустрије, сајбер злостављање, говор мржње, насиље и излагање непримјереном понашању или садржају, врбовање коришћењем стварних, компјутерски генерисаних или чак слика из виртуелне реалности и видео-записа који приказују и нормализују сексуално искоришћавање и злостављање дјеце. Ови ризици нису јединствени за окружење за играње, већ се примјењују на друга дигитална окружења у којима дјеца проводе вријеме.

Надаље, технолошки развој довео је до појаве "**интернета ствари**", гдје 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 безбједности и сајбер малтретирања. Године 2012. анкетирао је дјецу од 8 до 17 година у 25 земаља о негативном понашању на интернету. Резултати су показали да је у просјеку 54% учесника навело да се брину да ће бити малтретирани на интернету, 37% је изјавило да су доживјели сајбер малтретирање, а 24% је открило да су некога малтретирали. Исто истраживање је показало да је мање од троје од десет родитеља разговарало са дјецом о насиљу на интернету. Од 2016. Microsoft проводи **редовно истраживање** ризика на интернету дајући годишње извјештаје 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 свијета. 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 Савјет Европе, и доступна је на многим језицима.

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

- право дјеце на игру и слободу изражавања (вријеме 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 безбједност намијењену дјеци од 8 до 13 година која добијају први паметни телефон. Апликација је дио ББЦ-јеве посвећености у пружању подршке младим људима у данашњем промјењивом медијском окружењу и прати успјешно покретање интернет странице Own IT у 2018. години. Апликација комбинује најсавременију технологију машинског учења за праћење дјечјих активности на њиховим паметним телефонима с опцијом да дјеца самостално пријаве своје емоционално стање. Она користи ове информације за испоруку прилагођеног садржаја и интервенција које помажу дјеци да остану сретна и безбједна 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 савјета и подршке на екрану када им је потребна путем посебно развијене тастатуре. Карактеристике укључују:

- подсјећање корисника да добро размисле прије него што подијеле личне податке попут бројева мобилних телефона на друштвеним медијима;
- помоћ да разумију како би други могли да схвате поруке прије него што притисну слање;
- праћење њиховог расположења током времена и пружање смјерница 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 вријеме 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 извјештаје или повратне информације, а нити један податак неће напустити уређаје корисника. Апликација не прикупља никакве личне податке или садржај генерисан од корисника док се цијело машинско учење одвија у апликацији и на уређају корисника. Машине се посебно подешавају са подацима који се користе за тестирање да би се обезбиједило 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 дјеце са сметњама у развоју[4]

Дјеца 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. Дјеца 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 дијете с инвалидитетом и навести га да тражи социјалне

[4] Погледати Савјет Европе, "Два клика напријед и један клик назад: Извјештај о дјеци 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 дјецу да изложе већем ризику случајевима врбовања, подстицања на интернету и / или сексуалног узнемиравања. Истраживања показују да су дјеца и млади који имају потешкоће ван интернета и они погођени психосоцијалним потешкоћама под повећаним ризиком од таквих инцидената.[5]

Дјеца која су жртве изван интернета, вјероватно ће бити жртве и на интернету. То дјецу са инвалидитетом ставља у већи ризик на интернету, али имају и већу потребу да буду на интернету. Истраживања показују да ће дјеца са инвалидитетом вјероватније доживјети злостављање било које врсте,[6] а посебно је вјероватно да ће доживјети сексуалну виктимизацију.[7] Виктимизација може да укључује малтретирање, узнемиравање, искључење и дискриминацију на основу стварне или замишљене инвалидности дјетета 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 дјеце и младих са инвалидитетом могу да укључују не само преступнике са преференцијама који циљају дјецу и младе, већ и оне који циљају дјецу и младе са инвалидитетом. Такви починиоци могу да буду „привржениц“ - 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 дјеце и младих са инвалидитетом (које су нешкодљиве природе) и / или њихово дијељење путем намјенских форума или профила на друштвеним медијима. Алати за пријављивање на форумима и друштвеним медијима често немају одговарајући пут за рјешавање таквих радњи.

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

Појединa дјеца 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, „Извјештај о стању дјеце у свијету: Дјеца 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, „Привржениц, глумци и људи који то желе бити: Два случаја фактичког поремећаја инвалидности”, Сексуалност и инвалидитет, 1997.

9 УНИЦЕФ, “Приватност дјеце 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 смјернице 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 дјеце на интернету

На глобалном нивоу усваја се неколико модела да би се дјеца и млади заштитили на интернету. Интересне стране у ИКТ индустрији требало би да их сматрају смјерницама за међународне иницијативе и оквиром који ће обезбиједити да се не штеде напори у заштити дјеце и младих на интернету. Интернет индустрија је разнолика и замршена област, састављена од компанија различитих величина и функција. Важно је да се заштитом дјеце 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 дјеце ограничен њиховим доступним ресурсима. Стога ове смјернице препоручују да ИКТ компаније раде заједно на увођењу услуга за заштиту корисника. Дијелећи ресурсе и инжењерску стручност, ИКТ компаније би могле ефикасније да створе „безбједне просторе“ да би се спријечило злостављање.

**Сарадња ИКТ компанија**

Технолошка коалиција је примјер успјешне сарадње између интересних страна у ИКТ индустрији у борби против сексуалног искоришћавања и злостављања дјеце.

**Транснационални модели**

ИКТ компаније би требало да укључе релевантне међународне смјернице у свој структурни програм, и требало би да се придржавају свих релевантних националних или транснационалних закона који се примјењују 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, гдје 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 дјеце (2020);
- Комисија за широкопојасни приступ за одрживи развој, Безбједност дјеце на интернету: Смањење ризика од насиља, злостављања и искоришћавања на интернету (2019);
- Глобални савез WePROTECT, Глобални стратешки одговор на сексуално искоришћавање и злостављање дјеце на интернету (2019);
- Глобално партнерство за заустављање насиља над дјецом, Безбједно за учење: Позив на акцију;
- Дјечје достојанство у дигиталном свијету, Савез за достојанство дјетета: Извјештај радне групе за Технологију (2018);
- Директива (ЕУ) 2018/1808 Европског парламента и Савјета: Директива о аудиовизуелним медијским услугама;
- Општа уредба Европске комисије о заштити података (2018);
- Препорука ОЕЦД-а у погледу безбједности дјеце на интернету (2012).

**Национални модели**

Постоји низ националних и међународних модела који утврђују јасне улоге и одговорности технолошких компанија у рјешавању заштите дјеце на интернету. Неке од њих нису специфичне за дјецу саме по себи, али се могу на њих односити као на кориснике интернета. Они пружају свеобухватне смјернице 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 примјењују на ИКТ компаније.

**Кодекс дизајна прилагођеног узрасту, Велика Британија**

Почетком 2019. године Канцеларија комесара за информације објавила је приједлоге за свој кодекс за дизајнирање прилагођено узрасту ради унапређења заштите дјечјих података. Предложени кодекс заснован је на најбољем интересу за дјецу, како је утврђено у Конвенцији о правима дјетета УН-а, и у њему је изнијето неколико очекивања од ИКТ компанија. Кодекс се састоји од петнаест стандарда који укључују услуге одређивања локације за дјецу искључене у почетним подешавањима, ИКТ компаније да прикупљају и задржавају само минималну количину личних података дјеце, 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 дјело и фокусира се на широк распон штета, од сајбер малтретирања до порнографије из освете. Циљ му је обесхрабрити, спријечити и умањити штетну дигиталну комуникацију, чинећи незаконитим постављање дигиталне комуникације са намјером 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 примјењују на судске налоге против аутора или домаћина комуникације ако проблем није ријешен.

**Комесар eSafety, Аустралија**

Основана 2015. године, аустралијски Комесар eSafety прва је свјетска владина агенција посвећена борби против злоупотребе на интернету и одржавању безбједности својих грађана на интернету. Као национални независни регулатор за безбједност на интернету, eSafety има снажну комбинацију функција. Оне се крећу од превенције преко подизања свијести, образовања, истраживања и давања смјерница 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 безбједности на интернету на вишестран, цјеловит и проактиван начин.

У 2018. години eSafety је развио Safety by Design (SbD), иницијативу која ставља безбједност и права корисника у средиште дизајна, развоја и увођења интернетских производа и услуга. Скуп принципа безбједности по дизајну налази се у средишту иницијативе која утврђује реалне, ефикасне и остваривe мјере које ИКТ компаније треба да предузму да би боље заштитиле и одбраниле грађане на интернету. Три свеобухватна принципа су:

1) **Одговорности пружаоца услуга**: терет безбједности никада не би требало да падне на крајњег корисника. Могу се предузети превентивни кораци да би се обезбиједило да се познате и предвиђене штете процијене у дизајну и пружању услуга на интернету, заједно са корацима да би се смањила вјероватноћа 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 дјелатности 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 обиљежја снажног приступа безбједности, које пружају гаранције да службе дјелују у складу са објављеним безбједоносним циљевима, као и едукација и давање могућности јавности да предузму мјере ради рјешавања безбједносних 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 дјеце на интернету, вођене својим Моделима националног одговора, који дјелују као нацрт за дјеловање на националном нивоу. Пружа оквир за земље на који би требало да се ослоне у борби против сексуалног искоришћавања дјеце на интернету. Унутар WePROTECT Модела националног одговора, постоји јасан скуп обавеза за ИКТ компаније које се односе на:

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

**Глобално партнерство и фонд за заустављање насиља над дјецом**

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

Фокус рада је на спашавању и пружању подршке жртвама, технолошким рјешењима за откривање и спречавање прекршаја, пружању подршке органима за провођење закона, законодавним и политичким реформама, и генерисању података и доказа о размјерама и природи сексуалног искоришћавања и злостављања дјеце на интернету, као и разумијевању дјечјих перспектива.[12]

## 3. Кључна подручја заштите и промоције дјечјих права

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

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

Разматрање интеграције права дјетета захтијева да компаније предузму одговарајуће мјере за идентификовање, спречавање, ублажавање и, по потреби, санирање потенцијалних и стварних негативних утицаја на дјечја 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 дјецом, "Корисници фонда за заустављање насиља".

ИКТ компаније би требало да посвете посебну пажњу дјеци 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 Савјета 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 дјеце и младих на приватност и слободу изражавања, ИКТ компаније би требало да прате појачану дубинску анализу да би обезбиједиле 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 дјеце и младих, чак и тамо гдје домаћи закони још увијек нису сустигли међународне стандарде.

> Компаније би требало да имају успостављен механизам за жалбе на оперативном нивоу који ће обезбиједити формат за погођене појединце да изразе забринутост због потенцијалних прекршаја. Механизми на оперативном нивоу треба да буду доступни дјеци, 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 рјешавање негативних утицаја, механизми за жалбе требало би да обезбиједе да компаније имају успостављене оквире који обезбјеђују дјеци и младима одговарајући начин да траже помоћ када су њихова права угрожена.

Компаније треба да заузму приступ према ИКТ безбједности заснован на усклађености који се фокусира на испуњавање националног законодавства, слијеђење међународних смјерница када нема националног законодавства и избјегавање негативних утицаја на права дјеце и младих, и да компаније проактивно промовишу развој и добробит дјеце и младих волонтерским акцијама које унапређују права дјеце 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 дјетета. Политика приватности компаније осмишљена је тако да наводи које податке компанија прикупља и како се користе. Toca Boca, Inc је члан ПРИВО безбједне дјечје приватности ЦОРПА програма за цертификацију безбједних уточишта.

LEGO® Life је примјер безбједне платформе друштвених медија за дјецу млађу од 13 година за дијељење својих ЛЕГО креација, за добијање инспирације и безбједну интеракцију. Овдје се од дјеце не траже никакви лични подаци за стварање профила, за шта је само потребна адреса е-поште родитеља или старатеља. Апликација ствара прилику дјеци и породицама да разговарају о безбједности на интернету и приватности у позитивном окружењу.

Примјери дизајна примјереног узрасту укључују специфичне понуде неких од великих јавних сервиса за одређене старосне групе: на примјер, њемачки 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 интернетског канала funk.net. ББЦ (Британска радиодифузна корпорација) покренула је CBeebies који је усмјерен на дјецу 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 допринијело 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, умјесто да се ослањају на пријављивање Twitter-у. Нова технологија се користи за бављење политичким садржајима поља приватног информисања, осјетљивим медијима, понашањем из мржње, злостављањем и лажним представљањем.

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

## 3.2 Развој стандардних поступака за руковање материјалима сексуалног злостављања дјеце

У 2019. години IWF је дјеловала на 132.676 интернет страница за које је потврђено да садрже сексуално злостављање дјеце.[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 мјере, 45% је приказивало дјецу узраста 10 или мање година и 1.609 интернет страница приказивало је дјецу узраста 0–2 године, од којих је 71% садржавало најтеже сексуално злостављање, попут силовања и сексуалног мучења. Ове узнемирујуће чињенице истичу важност заједничког дјеловања ИКТ компанија, влада, органа за провођење закона и цивилног друштва у борби за превенцију материјала сексуалног злостављања дјеце.

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

Иако се многе владе боре против ширења и дистрибуције материјала сексуалног злостављања дјеце доношењем закона, прогоном и процесуирањем насилника, подизањем свијести и пружањем подршке дјеци и младима у опоравку од злостављања или искоришћавања, постоје многе земље које још увијек 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 обезбиједили успостављање одговарајућег правног оквира у складу са међународним стандардима. Такви оквири би требало да инкриминишу све облике сексуалног искоришћавања и злостављања дјеце, укључујући и материјал сексуалног злостављања дјеце, и да заштите дјецу која су жртве таквог злостављања или искоришћавања. Ти оквири морају да обезбиједе да процеси пријављивања, истраге и уклањања садржаја раде што ефикасније.

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

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

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

Актери у ИКТ индустрији требало би да се обавежу на додјелу пропорционалних ресурса и наставе да развијају и дијеле, по могућности, технолошка рјешења отвореног кода за откривање и уклањање материјала сексуалног злостављања дјеце.

### Добре праксе: Технологија

Microsoft користи четвороструки приступ за подстицање одговорне и безбједне 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 безбједношћу на интернету. "Породична безбједност" је једна од таквих карактеристика која омогућава родитељима и старатељима да надгледају употребу интернета своје дјеце.

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

[14] Треба имати на уму да непримјерено понашање корисника није ограничено на материјал сексуалног злостављања дјеце и да компанија треба на одговарајући начин да поступа с било којом врстом непримјереног 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 дјеце. Ако пронађе подударање, слика се блокира. Овај алат је омогућио провајдерима садржаја уклањање милиона незаконитих фотографија са интернета; помогао је осудити дјечје сексуалне предаторе; а у неким случајевима помогао је полицији да спаси потенцијалне жртве прије него што су биле физички повријеђене. Microsoft се већ дуго залаже за заштиту својих купаца од незаконитих садржаја на својим производима и услугама, а примјена технологије коју је компанија већ направила у борби против раста оваквих незаконитих видео-записа био је логичан сљедећи 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 измијењена да би се избјегло откривање, PhotoDNA for Video може да пронађе садржај сексуалног искоришћавања дјеце који је уређен или спојен у видео-запис који би у противном могао да изгледа безазлен.

Штавише, Microsoft је у скорије вријеме објавио нови алат за препознавање дјечјих предатора који у чатовима на интернету врбују дјецу 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 чат собама. Овом техником откривања врбовања моћи ће открити, реаговати и пријавити предаторе који покушавају да намаме дјецу у сексуалне сврхе.

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

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

## 3.3 Стварање безбједнијег окружења на интернету прилагођеног узрасту

Врло мало ствари у животу може се сматрати апсолутно безбједним и без ризика све вријеме. 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 дјецу и младе. О дјеци и младима се може размишљати као о примаоцима, учесницима и актерима у њиховом окружењу на интернету. Ризици са којима се суочавају могу да се подијеле у четири подручја:[15]

[15] Sonia Livingstone и др., “ЕУ Кидс Онлајн: Завршни извјештај”, Лондонска школа економије, 2009.

- *Непримјерен садржај* - Дјеца и млади могу наићи на непримјерен и незаконит садржај док траже нешто друго кликом на вјероватно безазлен линк у инстант поруци, на блогу или приликом дијељења датотека. Они такође могу да траже и дијеле неприкладан материјал или материјал неприлагођен узрасту. Оно што се сматра штетним садржајем разликује се од земље до земље; примјери укључују садржај који промовише злоупотребу опојних дрога, расну мржњу, ризично понашање, самоубиство, анорексију или насиље.
- *Непримјерено понашање* - Дјеца и одрасли могу да користе интернет за узнемиравање или чак искоришћавање других људи. Дјеца могу понекад да емитују увриједљиве коментаре или неугодне слике или могу да украду садржај или повриједе ауторска права.
- *Неприкладан контакт* - И одрасли и млади могу путем интернета да траже дјецу или друге младе људе који су рањиви. Често, њихов циљ је увјерити мету да су развили смислен однос, али основна сврха је манипулативна. Они могу покушати да наговоре дијете да изврши сексуална или друга изопачена дјела 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 дјечјих података, као и дигитални маркетинг. Безбједност на интернету је изазов заједнице и прилика за ИКТ компаније, владе и цивилно друштво да раде заједно на успостављању безбједносних принципа и пракси. ИКТ компаније могу да понуде читав низ техничких приступа, алата и услуга за родитеље, дјецу и младе, и прије свега треба направити производе који су једноставни за употребу, безбједни по дизајну и примјерени узрасту за њихов широк спектар корисника. Додатни приступи укључују понуду алата за развој одговарајућих система за провјеру старости који поштују дјечја права на приватност и приступ или ограничавају приступ дјеци и младима садржају који је непримјерен њиховим годинама или ограничавају људе са којима дјеца могу да имају контакт или вријеме у којем могу да користе интернет. Оно што је најважније, оквири „безбједност по дизајну“[16], укључујући и приватност, морају да буду укључени у процесе развијања иновација и дизајна производа. Дјечја безбједност 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 дјеца и млади шаљу и примају. Ако ће се користити програми ове врсте, важно је да се о томе отворено разговара с дјететом, иначе се такво понашање може да доживи као „шпијунирање“ и може да поткопа повјерење 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 дјеце, које врсте активности нису прихватљиве и посљедице 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 примјењују пратеће механизме од случаја до случаја, битно је поставити јасан временски оквир за реаговање, саопштити одлуку донесену у вези са пријавом и понудити начин рјешавања ако корисник није задовољан одговором.



16 Комесар eSafety, Преглед безбједности 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 непримјерени, Facebook-ови стандарди заједнице такође су релевантни као смјернице 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 безбједоносне 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 обавјештењима ако то изгледа као да је малољетника 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 дјецу које одговарајући органи за класификацију стављају на располагање. Овај процес постаје све компликованији с растућим спектром интерактивних услуга које омогућавају објављивање корисничког садржаја, на примјер путем огласних плоча, чат соба и услуга друштвених мрежа. Када компаније посебно циљају дјецу и младе и када су услуге претежно усмјерене на млађу публику, очекивања **у смислу лакоће за коришћење, лако разумљивом и приступачном садржају** и безбједности 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 дјеци и младима, јер дјеци и младима може недостајати зрелост да увиде шире друштвене и личне посљедице откривања или пристанка на дијељење својих личних података на интернету или на употребу њихових личних података у комерцијалне сврхе. Услуге усмјерене на или које би вјероватно привукле као главну публику дјецу 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 обезбиједити да се ти ризици рјешавају на прави начин и да су корисници информисани. Конкретно, компаније би требало да обезбиједе 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 дјеце 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 дјеци.

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 дјецом у свијету 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 дјецу. 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 дјеце 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 дјеце, родитеља и едукатора о безбједности дјеце и њиховој одговорној употреби ИК технологија

Техничке мјере могу да буду важан дио обезбјеђења заштите дјеце и младих од потенцијалних ризика на интернету, али оне су само један елеменат једначине. **Алати за родитељску контролу, подизање свијести** и образовање такође су кључне компоненте које ће помоћи у оснаживању и информисању дјеце и младих свих узраста, као и родитеља, старатеља и едукатора. Иако компаније имају важну улогу у подстицању дјеце и младих да користе ИК технологије на одговоран и безбједан начин, ту одговорност дијеле са родитељима, школама, дјецом 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 усмјеравању дјеце и младих према безбједнијим, одговорнијим и примјеренијим искуствима на интернету и мобилним телефонима. То укључује објављивање знаковног садржаја осјетљивог на старосну границу и обезбјеђивање да се информације о ставкама као што су цијене 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 провјеравање старости такође би помогло у заштити дјеце омогућавањем приступа услугама одговарајућем узрасту. Важно разматрање које треба ускладити са овом препоруком је додатно прикупљање личних података које ово може да подразумијева и потреба да се ограничи прикупљање и чување ових података и њихова обрада.

Такође је важно пружити информације дјеци и младима директно о безбједнијој употреби ИК технологија и позитивном и одговорном понашању. Поред подизања свијести о безбједности, компаније могу да омогуће позитивна искуства развијањем садржаја за дјецу 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 разумијевања и знања о интернету и мобилним уређајима од дјеце 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 дјецу у изградњи њихове дигиталне отпорности и понашања као одговорних дигиталних грађана. Циљ није пренијети одговорност за употребу ИК технологија од стране дјеце и младих само на родитеље, већ препознати да су родитељи у бољој позицији да одлуче шта је прикладно за њихову дјецу и да их треба упознати са свим ризицима да би боље заштитили своју дјецу 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 безбједности на интернету и одговорној употреби ИК технологија од стране дјеце и младих, као и образовни материјали за родитеље. Примјери укључују објашњење врста услуга и опција доступних за праћење активности, радње које се предузимају ако се дијете суочава са малтретирањем или врбовањем на интернету, како избјећи нежељену пошту и управљати подешавањима приватности и како разговарати са дјечацима и дјевојчицама различитих старосних група о осјетљивим проблемима. Комуникација је двосмјеран 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 савјета и подсјетника о природи одређене услуге и начину безбједног уживања у њој. Иако је важно дјецу научити одговорном коришћењу интернета, знамо да дјеца воле експериментисати, ризиковати, да су знатижељна и можда не доносе увијек најбоље одлуке. Давање шансе да се баве својим дјелатностима доприноси њиховом развоју и здрав је начин који ће им помоћи да развију аутономију и отпорност, све док повратни ефекат није преоштар. Иако се дјеци 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 "мјесто" на којем су тинејџери могли без страха да подијеле своја осјећања.

## 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 вјештине медијске писмености. Други аспект безбједоносног рада Twittera односи се на њихово откривање операција са информацијама. Ово је архива операција са информацијама које подржава држава и коју Twitter јавно дијели. Иницијатива је покренута да би се оснажило академско и јавно разумијевање кампања повезаних са овом проблематиком широм свијета, 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 дјецу узраста од 9 до 13 година. Као дио пројекта, развијен је алат под називом „Искорачи, говори!“, који пружа низ материјала за образовање, обуку и подизање свијести, као и практичне алате за мултисекторске стратегије превенције и реаговања. Пројекат ће ове материјале за учење пренијети другим европским земљама и партнерима широм свијета у сврху промоције дигиталних права младих.

Google је развио низ образовних иницијатива, ресурса и алата који помажу у промоцији безбједности 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 безбједност на интернету и коалиција Internet Keep Safe. Ова кампања је усмјерена на младе људе узраста од 8 до 11 година. Садржи интернетску игру за младе (Интерланд) која подучава основама дигиталне безбједности и ресурсе за едукаторе, попут дигиталног грађанства и безбједносног плана и програма. Безбједносни 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 безбједности на интернету за едукаторе ученика свих старосних група, пружајући даљњу подршку за интегрисање дигиталног грађанства и безбједносних активности у учионици. Google такође нуди неколико програма који помажу младима да се директно укључе у напоре на пољу безбједности на интернету и на пољу дигиталног грађанства. Глобална иницијатива Web Rangers један је од таквих програма који младе подучава о безбједности на интернету и подстиче их да креирају сопствене кампање око позитивне и безбједне употребе интернета. Постоје и посебни програми за младе за одређене државе, попут програма Internet Citizens i Internet Legends у Великој Британији, које је покренуо Google.

На **Евровизијској размјени вијести за младе**, Европска радиодифузна унија окупља 15 европских телевизијских кућа да би размјењивале програме, формате и рјешења на интернету и ван њега. Посљедњих година, подучавање дигиталне писмености и упозоравање дјеце на ризике на интернету постали су кључни за њихове програме. Међу најуспјешнијим иницијативама посљедњих година су огласи на друштвеним мрежама и вијести прилагођене за дјецу које су произвели Super и Ultra nytt под НРК, норвешким јавним емитером.

## Добре праксе: Стратешка партнерства

Као дио пројекта подржаног од Фонда за заустављање насиља над дјецом, Capital Humano y Social Alternativo је 2018. године склопио партнерство с компанијом Telefónica, највећим провајдером интернетских, 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 дјеце 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 успјешно завршавају курс. Перуанско министарство образовања сложило се да ће укључити приступ овом виртуелном курсу путем своје службене интернет странице.
- **Књижица о безбједности 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 безбједности на интернету и ризицима повезаним са сексуалним искоришћавањем и злостављањем дјеце на интернету.
- **Интерактивну игру о сексуалном искоришћавању и злостављању дјеце 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 успјех 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 дјетета УН-а каже да „дијете има право на слободу изражавања; то право мора, независно од граница, укључивати слободу тражења, примања и ширења обавјештења и идеја сваке врсте, усмено или писмено, штампањем, умјетничким обликовањем или путем било којег другог средства према избору дјетета." Компаније могу да испуне своју дужност поштовања грађанских и политичких права дјеце и младих обезбјеђујући да технологија и примјена закона и политика развијених за заштиту дјеце и младих од штете на интернету немају ненамјерне посљедице сузбијања њиховог права на учешће и изражавање или спречавање приступа информацијама које су важне за њихову добробит. Неопходно је обезбиједити да системи провјере 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 дјеце 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 примјер, учествовањем у социјалним и еколошким кампањама и позивањем на одговорност оних који су одговорни. Уз одговарајуће алате и информације, дјеца 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 примјерених дјеци и младима и породицама. Оне могу да подрже развој технологије и садржаја који подстичу и омогућавају дјеци и младима да уче, стварају иновације и праве рјешења. Увијек би требало да имају на уму безбједност по дизајну у својим производима.

Поред тога, компаније могу проактивно да подрже права дјеце и младих радећи на уклањању дигиталне подјеле. За учешће дјеце и младих потребна је дигитална писменост - способност разумијевања и интеракције у дигиталном свијету. 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 дјеловања, 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 вјештина које дјеци 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 подјеле дио су мисије јавних медијских сервиса посљедњих година. Италијански парламент, на примјер, предложио је да приоритети националних емитера укључују уклањање дигиталне подјеле и обезбјеђење заштите дјеце ван интернета и на интернету, примјер који би могле да слиједе друге земље.



17 Примјере 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 дјеци 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 дјеце (кампања је усмјерена на дјецу узраста до 8 година) и породицама бесплатан материјал за учење да би помогла малој дјеци да гаје „12 моћи за добро“ (Моћ Зерових 12 животних вјештина или „моћи“, за дјецу да се успјешно крећу у онлајн и офлајн свијету, укључујући отпорност, поштовање, инклузивност и креативност) и постављају им снажне основе у раном узрасту.

## 4. Опште смјернице за ИКТ компаније

Табела 1. даје широке смјернице за ИКТ компаније за идентификацију, спречавање и ублажавање било каквих негативних утицаја производа и услуга на права дјеце и младих, те за промоцију позитивне употребе ИК технологија од стране дјеце 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 смјернице за ИКТ компаније допуњују се контролном листом по карактеристикама (види одјељак 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 смјернице за ИКТ компаније

| | |
|---|---|
| **Разматрања о интеграцији права дјетета у све одговарајуће корпоративне политике и процесе управљања** | ИКТ компаније могу да идентификују, спријече и ублаже негативне утицаје ИК технологија на права дјеце и младих, и да идентификују могућности за подршку у напретку права дјеце и младих предузимањем сљедећих радњи: |
| | Обезбјеђивањем 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 дјеце на интернету у цијелој компанији. |
| | Развијањем политике заштите и чувања дјеце и / или интегрисањем посебних ризика и могућности које се односе на права дјеце и младих у опредјељења политике компаније (нпр. људска права, приватност, маркетинг и релевантни кодекси понашања). |
| | Интегрисањем дубинске анализе о питањима заштите дјеце на интернету у постојеће оквире људских права или процјене 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 дјечја права различитих старосних група као резултата пословања компаније и дизајна, развоја и увођења производа и услуга, као и могућности за подршку правима дјеце и младих. |

| | |
|---|---|
| **Разматрања о интеграцији права дјетета у све одговарајуће корпоративне политике и процесе управљања (наставак)** | Усвајањем приступа дјечјој заштити заснованој на оснаживању и образовању. Узимањем у обзир права дјетета на заштиту података, њиховог права на приватност и слободу говора, истовремено нудећи образовање и смјернице кроз услуге компаније. |
| | Ослањањем на интерну и екстерну стручност и савјетовање са кључним интересним странама, укључујући дјецу и младе, о механизмима за безбједност дјеце на интернету да би добили сталне повратне информације и смјернице о приступима компаније. |
| | У државама којима недостају одговарајући правни оквири за заштиту права дјеце и младих на приватност и слободу изражавања, компаније би требало да обезбиједе 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. |
| | Обезбјеђивањем приступа правном лијеку успостављањем могућности жалби на оперативном нивоу и кроз механизме пријављивања било каквих кршења права дјетета (нпр. материјал сексуалног злостављања дјеце, непримјерен садржај или контакт или кршење приватности). |
| | Именовањем руководиоца политике заштите дјеце или друге одређене особе која се може контактирати у вези са питањима заштите дјеце на интернету. Ако је дијете у опасности од штете, руководилац политике заштите дјеце треба одмах упозорити одговарајуће власти. |
| | Уредничке смјернице ББЦ-а (2019.), на примјер, одређују именовање руководиоца политике заштите дјеце, што се у јавним медијима сматра обавезним. |
| **Развој стандарда ИКТ компанија за заштиту дјеце на интернету** | Направити и примијенити стандарде за компаније и ИКТ индустрију за заштиту дјеце и младих, с обзиром на специфичну индустрију и карактеристике. |
| **Развој стандардних поступака за руковање материјалима сексуалног злостављања дјеце** | 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 дјеце предузимањем сљедећих радњи: |
| | Забранити учитавање, објављивање, пренос, дијељење 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 дјеце чим провајдер сазна за њих. |
| | Обезбиједити 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), гдје се може извршити пријава на било којој међународној линији за подршку. |

| | |
|---|---|
| **Развој стандардних поступака за руковање материјалима сексуалног злостављања дјеце**<br>**(наставак)** | Успоставити интерне процедуре да би се обезбиједило поштовање локалних и међународних закона о борби против материјала сексуалног злостављања дјеце.<br>Основати виши положај или тим посвећен интеграцији ових поступака у организацију. Чланови ИКТ индустрије би затим требало да извјештавају о предузетим радњама и резултатима које је постигао овај тим у свом годишњем извјештају о корпорацији и одрживости.<br>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 дјеце.<br>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 извјештајима 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 дијељење материјала сексуалног злостављања дјеце и посљедицама било које злоупотребе. |
| | Развити поступке обавјештавања, уклањања и извјештавања који омогућавају корисницима да пријаве материјал сексуалног злостављања дјеце или непримјерен контакт и одређени профил / локацију гдје је откривен.<br>Успоставити извјештај о пратећем поступку, договорити се о процедурама за прикупљање доказа и брзо уклањање или блокирање приступа материјалу сексуалног злостављања дјеце.<br>Обезбиједити да провајдери услуга, по потреби, затраже мишљење стручњака (нпр. националних органа за борбу против материјала сексуалног злостављања дјеце) прије уништавања незаконитог садржаја.<br>Обезбиједити да релевантне треће стране са којима је компанија у уговорном односу имају успостављене исто тако снажне процесе обавјештавања и уклањања. |
| | Треба да буду спремне за руковање материјалом сексуалног злостављања дјеце 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 безбједност, 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 дјетета / дјеце и младих. Позабавити се ситуацијама у којима особље може да буде изложено изопаченом материјалу, провести политику или програм за пружање подршке за развој отпорности, безбједности и добробити особља. |

| | |
|---|---|
| **Развој стандардних поступака за руковање материјалима сексуалног злостављања дјеце**<br>**(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 дјеце, почевши од праћења и настављајући се до коначног преноса и уништавања садржаја. У документацију укључити списак цијелог особља одговорног за руковање материјалом. |
| | Промовисати механизме пријављивања материјала сексуалног злостављања дјеце и обезбиједити да корисници знају како поднијети 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 спријечили ширење познатог садржаја сексуалног злостављања дјеце путем својих услуга или платформи. |
| | Редовно активно процјењивати 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 дјеце, софтвер за препознавање слика или блокирање интернет адреса за борбу против материјала сексуалног злостављања дјеце. |
| **Стварање безбједнијег окружења на интернету прилагођеног узрасту** | ИКТ компаније могу помоћи у стварању безбједнијег, угоднијег дигиталног окружења за дјецу и младе свих узраста предузимањем сљедећих радњи: |
| | Усвојити принципе безбједности и приватности по дизајну у технологијама и услугама компанија и дати приоритет рјешењима која смањују количину података који се односе на дјецу на минимум. |
| | Примијенити дизајне прилагођене узрасту у понуђеним услугама.<br>Представити дјеци информације о правилима интернет странице на приступачан начин и примјерено њиховом узрасту, пружајући одговарајућу количину детаља.<br>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, посљедице кршења било којих правила, специфичности услуге и оно на шта корисник пристаје пријављивањем. Такве информације треба да буду посебно усмјерене на младе кориснике и њихове родитеље и старатеље. |
| | Користити услове услуге или услове и одредбе да бисте скренули пажњу корисницима на садржај на интернетским услугама компаније који можда није примјерен за све узрасте. Услови и одредбе такође треба да укључују јасне механизме за пријављивање и поступање у случају кршења таквих правила. |

| | |
|---|---|
| **Стварање безбједнијег окружења на интернету прилагођеног узрасту**<br>**(наставак)** | Размотрити могућност пружања механизама као што су софтвер за родитељску контролу и други алати који омогућавају родитељима и старатељима да управљају приступом дјеци интернетским ресурсима, истовремено им пружајући смјернице о њиховој одговарајућој употреби да се не би кршила дјечја 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 дјеца 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 дјететову способност да унаприједи своје дигиталне вјештине и на смањивање његових могућности на интернету, ове контроле би требало да буду дизајниране за врло малу дјецу у складу са њиховим развојним контекстом и са одговарајућим смјерницама за родитеље. |
| | Тамо гдје 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. |
| | Избјегавати штетне или непримјерене 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 дјецу и младе. Штетно оглашавање такође може да укључује оглашавање хране и пића која садрже пуно масти, шећера или соли.<br>Ускладити пословне праксе са прописима и савјетима о маркетингу и оглашавању за дјецу и младе. Пратити гдје, када и како дјеца и млади могу наићи на потенцијално штетне рекламне поруке намијењене другом сегменту тржишта. |
| | Обезбиједити да се политике прикупљања података придржавају релевантних закона који се тичу приватности дјеце и младих, укључујући разматрање да ли је потребан пристанак родитеља прије него што комерцијална предузећа могу да прикупи личне податке од дјетета или о дјетету. |
| | Прилагодити и примијенити 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. Подразумијевана подешавања приватности и информације о важности приватности требало би да одговарају узрасту корисника и природи услуге. |
| | Примијенити техничке мјере, као што су одговарајући алати за родитељску контролу, безбједност 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 спријечио приступ и изложеност малољетника непримјереном садржају или услугама.<br>Примијенити технологију која може идентификовати узраст корисника и представити им верзију апликације која одговара узрасту.<br>За садржај или услуге осјетљиве на узраст, интересне стране у ИКТ индустрији би требало да предузму кораке за провјеру старости корисника. Тамо гдје 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.<br>Компаније би такође требало да препознају потенцијал злоупотребе таквих технологија са циљем ограничавања права дјеце и младих на слободу изражавања и приступа информацијама или угрожавања њихове приватности. |

| | |
|---|---|
| **Стварање безбједнијег окружења на интернету прилагођеног узрасту** **(наставак)** | Обезбиједити да су садржај и услуге који нису прикладни за кориснике свих старосних група:<br>• класификовани у складу са националним стандардима и културним нормама;<br>• у складу са постојећим стандардима у еквивалентним медијима;<br>• идентификовани са истакнутим опцијама приказа за контролу приступа;<br>• у понуди заједно са провјером старости, гдје 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 провјере.<br><br>На примјер, 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 примијене смјернице 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 непримјереном садржају, контактима и злоупотребама, а корисницима услуга пружити детаљне повратне информације о процесу који се односи на пријаву. |
| | Обезбиједити предмодерацију интерактивних простора дизајнираних за дјецу и младе на начине који се подударају са правима дјеце на приватност и њиховим развојним капацитетима. Активна модерација може да подстакне атмосферу у којој насиље и узнемиравање нису прихватљиви. Неприхватљиво понашање укључује:<br>• објављивање неугодних или пријетећих коментара на нечијем профилу;<br>• отварање лажних профила или интернет страница мржње ради понижавања жртве;<br>• слање ланчаних порука и прилога са штетном намјером;<br>• хаковање нечијег профила ради слања увредљивих порука другима. |
| | Предузети посебне мјере опреза са члановима особља или сарадницима који раде са дјецом и младима, за које може бити потребна претходна провјера 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:<br>• пријавити врбовање извршном руководећем тиму и именованом руководиоцу политике заштите дјеце, гдје је то могуће;<br>• омогућити корисницима да директно пријаве надлежним органима случајеве врбовања;<br>• успоставити могућност директног контакта путем адреса е-поште ради упозорења и пријављивања. |
| | У сваком тренутку дати приоритет безбједности и добробити дјетета. Дјеловати увијек у професионалним границама и обезбиједити да је сваки контакт са дјецом важан за услугу, програм, догађај, активност или пројекат. Никада не преузимајте искључиву одговорност за дијете. Ако је дјетету потребна њега, упозорити родитеља, старатеља или пратиоца. Слушати и поштовати дјецу у свако доба.<br>Ако се неко понаша непримјерено у близини дјеце, пријавите то понашање локалном контакту за заштиту дјеце. |

| | |
|---|---|
| **Стварање безбједнијег окружења на интернету прилагођеног узрасту (наставак)** | Успоставити јасан скуп правила која су на видном мјесту и осликавају кључне тачке из услова услуге и смјерница прихватљиве употребе. Језиком који је разумљив за кориснике ова правила би требало да дефинишу:<br>• природу услуге и шта се очекује од њених корисника;<br>• шта је прихватљиво а шта није у смислу садржаја, понашања и језика, као и забрана незаконите употребе;<br>• посљедице пропорционалне кршењу, на примјер, 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 рјешавање различитих проблема, као што је примање нежељених комуникација (нпр. нежељене СМС поруке). |
| | Бити транспарентан и пружити корисницима јасне информације о природи понуђених услуга, на примјер:<br>• врста садржаја / услуге и трошкови;<br>• минимална старосна граница потребна за приступ;<br>• доступност родитељског надзора, укључујући оно што контроле покривају (нпр. интернет) или не покривају (нпр. Wi-Fi) и обуку о томе како их користити;<br>• врста прикупљених корисничких података и како се користе. |
| | Промовисати националне службе подршке које омогућавају дјеци и младима да пријаве и потраже подршку у случају злостављања или искоришћавања (погледати, на примјер, Child Helpline International). |
| **Едукација дјеце, родитеља и едукатора о безбједности дјеце и њиховој одговорној употреби ИК технологија** | ИКТ компаније могу да допуне техничке мјере образовним активностима и активностима оснаживања предузимањем сљедећих 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 дјецу, родитеље и старатеље, посебно у односу на одредбе и услове, трошкове укључене у употребу садржаја или услуга, политике приватности, безбједносне информације и механизме пријављивања. |
| | Обучити кориснике о начину рјешавања проблема у вези са употребом интернета, укључујући нежељену пошту, крађу података и непримјерен контакт, попут малтретирања и врбовања, и описати које радње корисници могу да предузму и како могу да изнесу забринутост због непримјерене употребе. |
| | Успоставити механизме и едуковати родитеље да се укључе у ИКТ активности своје дјеце и младих, посебно оних који имају млађу дјецу, тако што ће, на примјер, омогућити родитељима да прегледају поставке приватности дјеце и младих. |
| | Сарађивати са владом и едукаторима да би изградили капацитете родитеља за подршку и разговор са својом дјецом и младима о томе да буду одговорни дигитални грађани и корисници ИК технологија. |

| | |
|---|---|
| **Едукација дјеце, родитеља и едукатора о безбједности дјеце и њиховој одговорној употреби ИК технологија**<br>**(наставак)** | На основу локалног контекста, треба обезбиједити образовне материјале за употребу у школама и домовима да би побољшали употребу ИК технологија код дјеце и младих и развили критичко размишљање да би им омогућили да се понашају безбједно и одговорно када користе услуге ИК технологија. |
| | Подржите кориснике ширењем смјерница о породичној безбједности на интернету које подстичу родитеље и старатеље да:<br>• се упознају са производима и услугама које користе дјеца и млади;<br>• обезбиједе умјерену употребу електронских уређаја од стране дјеце и младих као дијела здравог и уравнотеженог начина живота;<br>• пажљиво обрате пажњу на понашање дјеце и младих да би утврдили промјене које би могле указивати на сајбер злостављање или узнемиравање. |
| | Пружити родитељима потребне информације да би разумјели како њихова дјеца и млади користе услуге ИК технологија, рјешавали проблеме у вези са штетним садржајем и понашањем и били спремни да уче дјецу и младе одговорној употреби. То се може олакшати употребом алата и интеракцијом са школским дистриктима за пружање наставних планова и програма за дјецу и образовних материјала за родитеље у вези са безбједности на интернету. |
| **Коришћење технолошког напретка за заштиту и образовање дјеце** | Вјештачка интелигенција која чува приватност, а која разумије текстове, слике, разговоре и контекст, може да открије и ријеши читав низ штета и пријетњи на интернету и да користи те информације за оснаживање и образовање дјеце 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 дјеце и њихово освјешћивање о ризицима и могућностима интернетског свијета |
| **Промовисање дигиталне технологије као начина за повећање грађанског ангажмана** | ИКТ компаније могу да охрабре и оснаже дјецу и младе подржавајући њихово право на учешће кроз сљедеће радње: |
| | Пружање информација о услузи да би истакли користи које дјеца остварују понашајући се примјерно и одговорно, попут употребе услуге у креативне сврхе. |
| | Успоставити писане поступке који обезбјеђују досљедно провођење политика и процеса који штите слободу изражавања за све кориснике, укључујући дјецу и младе, као и документацију о усклађености са тим политикама. |

| | |
|---|---|
| **Промовисање дигиталне технологије као начина за повећање грађанског ангажмана**<br>**(наставак)** | Избјегавајте прекомјерно блокирање легитимног и развојно одговарајућег садржаја. Да се захтјеви и алати за филтерисање не би злоупотребљавали за ограничавање приступа информацијама дјеци и младима, обезбиједити транспарентност блокираног садржаја и успоставити поступак за кориснике који пријављују ненамјерно блокирање. Овај поступак требало би да буде доступан свим потрошачима, укључујући вебмастере. Сваки поступак извјештавања треба пружити јасне, одговорне и процијењене услове пружања услуге. |
| | Развити онлајн платформе које промовишу право дјеце и младих на изражавање; олакшати њихово учешће у јавном животу; и подстицати њихову сарадњу, предузетништво и грађанско учествовање. |
| | Развити образовни садржај за дјецу и младе који подстиче учење, креативно размишљање и рјешавање проблема. |
| | Промовисати дигиталну писменост, изградњу капацитета и ИКТ вјештине да би се дјеца и млади, посебно они у руралним подручјима и подручјима са недовољно високим нивоом услуга, опремили за коришћење ИКТ ресурса и потпуно безбједно учешће у дигиталном свијету. |
| | 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. |
| | Обавијестите и укључите купце, укључујући родитеље, његоватеље, дјецу и младе, о понуђеним услугама, попут:<br>• врсте садржаја и одговарајуће родитељске контроле;<br>• механизама пријављивања случајева погрешне употребе, злоупотребе и непримјереног или незаконитог садржаја;<br>• поступака праћења извјештаја;<br>• врсте услуга које су старосно ограничене;<br>• безбједног и одговорног коришћења интерактивних услуга „властитог бренда“. |
| | Бавите се ширим питањима у вези са безбједним и одговорним дигиталним грађанством, на примјер интернетском репутацијом и дигиталним отиском, штетним садржајем и његом. Размислите о партнерству са локалним стручњацима, попут дјечјих невладиних организација, добротворних организација и родитељских група, да бисте помогли обликовати поруку компаније и имали жељену публику. |
| | Ако компанија већ ради с дјецом или школама, на примјер, кроз програме корпоративне друштвене одговорности, истражите могућност да се овај ангажман прошири на образовање и интеракцију са дјецом и младима као и на едукаторе о порукама у вези са заштитом дјеце на интернету. |
| **Инвестирање у дигитално истраживање** | Уложите у истраживање засновано на доказима и у дубинску анализу технологија, утицај технологија на дјецу, разматрање заштите дјеце и права дјетета с обзиром на дигитално окружење, интегрисање онлајн система заштите у услуге које користе дјеца и млади и боље разумијевање које врсте интервенција су најефикасније у побољшању дјечјих онлајн искустава. |

### Типологија ИКТ компанија

Иако су ове смјернице Међународне уније за телекомуникације усмјерене на ИКТ индустрију у цјелини, 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 усмјерени директно или индиректно на дјецу може да има користи од раније наведених општих принципа и може да се прилагоди на основу свог специфичног подручја дјеловања. Основна идеја је подржати и водити ИКТ индустрију у предузимању правих мјера за бољу заштиту дјеце на интернету од опасности наношења штете, истовремено оснажујући дјецу да се крећу онлајн свијетом на најбољи могући начин. Типологија у наставку ће помоћи да се пружи јасније разумијевање неких из циљне публике и како се исти уклапају у контролне листе у сљедећем одјељку. Треба напоменути да су ово само неки специфични примјери 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 размјену 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 дјечје 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 дјечјих 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 пресијецају и неколико контролних листа специфичних за карактеристике може да буде релевантно за исту компанију.

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

### 5.1 Карактеристика А: Обезбиједити повезивање, услуге складиштења података и хостинга

Приступ интернету је основни за остваривање дјечјих права, а повезаност може дјеци отворити читав свијет. Провајдери услуга повезивања, складиштења података и хостинга имају огромне могућности да у своје понуде за дјецу и младе угради безбједност 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 дјеце на интернету и нуде низ алата и информативних извора ради подршке својој посвећености заштити дјеце на интернету.

Већина провајдера интернетских услуга дјелује 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 дјеце 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 обезбиједи доступност интернета у одређеном подручју. Међутим, треба водити рачуна када је такав приступ омогућен у јавним просторима у којима је вјероватно да ће дјеца 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 увијек бити у могућности да подрже или надзиру употребу интернет конекције коју је испоручио и корисници зато морају да предузму мјере предострожности да избјегавају дијељење осјетљивих информација путем јавно доступне Wi-Fi мреже.

У јавним просторима, провајдери Wi-Fi мреже ће можда размислити о увођењу додатних мјера за заштиту дјеце 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 дјеце.
- 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 дјеца. Одредбе и услови такође треба да садрже јасне механизме у вези са посљедицама кршења таквих правила.
- Предузимање свих мјера 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.
- Обезбјеђење процедура и софтвера за путоказ и нуђење опционе родитељске контроле која се односи на приступ дјеце и младих интернетским садржајима.

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

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

## Табела 2. Контролна листа заштите дјеце на интернету за Карактеристику А: Обезбиједити уређаје за повезивање, складиштење и хостинг података

| | |
|---|---|
| **Увртавање питања права дјетета у све одговарајуће корпоративне политике и процесе управљања** | Провајдери услуга повезивања, складиштења података и хостинга могу да идентификују, спријече и ублаже негативне ефекте ИК технологија на права дјеце и младих и да идентификују могућности за подршку напретку дјеце и младих. |
| | *Види опште смјернице у Табели 1.* |
| **Развој стандардних процеса ради рјешавања проблема материјала сексуалног злостављања дјеце** | 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 дјеце предузимањем сљедећих радњи: |
| | Сарадња са владом, органима за провођење закона, цивилним друштвом и организацијама СОС сервиса у борби против материјала сексуалног злостављања дјеце 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) гдје 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 обавјештавања, уклањања и пријављивања те повезати пријаве злоупотребе са тим процесима путем споразума о јавној служби о поступку одговора и времену уклањања. |
| | Погледајте, на примјер, УНИЦЕФ-ов и ГСМА водич о политикама и пракси обавјештавања и уклањања. |
| | Успоставите механизам пријављивања са јасним информацијама о његовој употреби, на примјер, давањем смјерница о илегалном садржају и понашању које треба пријавити и појашњавањем тога који се материјали не могу приложити уз извјештај да би се избјегла даљна дистрибуција на интернету. |

| | |
|---|---|
| **Развој стандардних процеса ради рјешавања проблема материјала сексуалног злостављања дјеце** (***наставак***) | Подржите провођење закона у случају кривичних истрага кроз активности као што је прикупљање доказа.<br>Користите услове и одредбе услуге да бисте посебно забранили употребу услуга за складиштење, дијељење или дистрибуцију материјала сексуалног злостављања дјеце. Обавезно наведите да ови услови јасно наводе да се материјал сексуалног злостављања дјеце неће толерисати.<br>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 дјеце. |
| | Тренутно постоје два рјешења за пријављивање материјала сексуалног злостављања дјеце на интернету на националном нивоу: вруће линије и портали за пријављивање. Потпуну ажурну листу свих постојећих телефонских линија и портала можете пронаћи на веб-страници INHOPE.<br>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 смјернице о томе како развити интерне процесе за особље за бригу о клијентима које ће подносити извјештаје сумњивог садржаја полицији и мрежи INHOPE.<br>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 дјеце 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 обавјештавања и уклањања. |
| **Стварање безбједнијег и старосно прикладног дигиталног окружења** | Провајдери услуга интернет конекције, складиштења података и хостинга могу помоћи у стварању безбједнијег, угоднијег дигиталног окружења за дјецу свих узраста предузимањем сљедећих 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 извјештајима 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 примијенити и понудити могућност блокирања или филтерисања приступа интернету путем корпоративне мреже. Обезбиједите 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 дјеце, родитеља и наставника о дјечјој безбједности и њиховој одговорној употреби ИК технологија** | Провајдери услуга повезивања, складиштења података и хостинга требало би да понове кључне поруке из одредби и услова из смјерница заједнице написаних на језику прилагођеном корисницима да подрже дјецу и њихове родитеље и старатеље. У оквиру саме услуге, у тренутку преношења садржаја, уврстити подсјетнике на теме као што је врста садржаја која се сматра неприкладном. |
| | Пружите дјеци и младима информације о безбједнијој употреби интернета. Размотрите креативне начине за промоцију кључних порука, као што су сљедеће:<br>"Никада не дијелите никакве контакт-информације са непознатим лицима, укључујући вашу физичку локацију и телефонски број.<br>„Никада немојте пристати да се сами састанете са неким кога сте упознали на мрежи без претходног савјетовања са одраслом особом. Увијек реците поузданом пријатељу гдје се налазите "<br>„Не одговарајте на малтретирање, непристојне или увредљиве поруке. Али сачувајте доказе - не бришите поруку.“<br>"Реците одраслој особи или пријатељу од повјерења ако вам је због нечега или некога непријатно."<br>“Никада не дајте лозинку или корисничко име налога! Имајте на уму да други људи на мрежи могу давати лажне податке да би вас увјерили да подијелите своје приватне податке." |
| | Провајдери услуга могу да се удруже са организацијама које су у добром положају ради едукације и подршке дјеци о безбједнијој употреби интернета и о сродним питањима.<br>Погледајте International Helpline за дјецу и практични водич за ГСМА за дјечје линије за подршку и мобилне операторе: Заједнички рад на заштити дјечјих права. |
| **Промовисање дигиталне технологије као начина за повећање цивилног ангажмана** | *Види опште смјернице у Табели 1.* |

## 5.2 Карактеристика Б: Понудити организовани дигитални садржај

Интернет пружа све врсте садржаја и активности, од којих су многи намијењени дјеци и младима. Сервиси који нуде професионално уређен садржај имају огромне могућности да у своје понуде за дјецу и младе угради безбједност 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 вијести и мултимедије, националну и јавну радиодифузију и индустрију игара на срећу.

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

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

| | |
|---|---|
| **Увртавање питања права дјетета у све одговарајуће корпоративне политике и процесе управљања** | Сервиси који нуде професионално уређен садржај могу да помогну да се идентификују, спријече и ублаже негативни утицаји ИК технологија на права дјеце и младих и да идентификују могућности за подршку напретку дјеце и младих предузимањем сљедећих радњи: |
| | Развити политике које штите добробит дјеце 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, вијести итд. без обзира на пристанак који је могао дати родитељ или друго одрасло лице. |
| **Развијање стандардних процеса за борбу против материјала сексуалног злостављања дјеце** | 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 сљедећих активности:<br>У случајевима МСЗД, на примјер 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:<br>• одмах упозорити националне агенције за провођење закона;<br>• упозорити руководство агенције и пријавити материјал менаџеру политике заштите дјеце;<br>• контактирати службу интерне истраге телефоном или е-поштом са детаљима инцидента и затражити савјет;<br>• прије брисања материјала, складиштења у заједнички простор или прослеђивања причекајте савјет надлежне агенције; |
| | • имплементирати брзу и ефикасну стратегију ескалације ако је материјал сексуалног злостављања дјеце објављен или се сумња на незаконито понашање; у ту сврху:<br>• понудити корисницима једноставан и лако доступан начин упозоравања произвођача садржаја на кршење било којих правила онлајн заједнице;<br>• уклонити садржај којим се крше правила;<br>• понудити корисницима једноставан и лако доступан начин упозоравања произвођача садржаја на кршење било којих правила онлајн заједнице;<br>• уклонити садржај којим се крше правила.<br>• Прије слања професионално уређеног садржаја са старосним ограничењем на друштвене мреже, припазите на услове и одредбе веб-странице. Пратите минималне старосне захтјеве на различитим страницама за друштвено умрежавање.<br>• Одредбе и услови сваког интернетског простора треба такође да садрже јасне механизме извјештавања о кршењу таквих правила. |

**Развој стандардних процеса ради рјешавања проблема материјала сексуалног злостављања дјеце**

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

| | |
|---|---|
| **Стварање безбједнијег и старосно прикладног дигиталног окружења** | Компаније које нуде професионално уређени дигитални садржај могу помоћи у стварању безбједнијег и пријатнијег дигиталног окружења за дјецу и младе свих узраста предузимањем сљедећих радњи: |
| | Сарађујте са другима из бранше да бисте развили системе класификације/оцјењивања садржаја који се заснивају на прихваћеним националним или међународним стандардима и у складу са приступима који се заузимају у еквивалентним медијима.<br>Гдје је то могуће, класификација садржаја требало би да буде конзистентна на различитим медијским платформама, на примјер, најава филма у биоскопу и на паметном телефону корисницима би приказивала исте класификације. |
| | Развити производе прилагођене дјеци и старосно прилагођене садржаје за дјецу и младе који су осмишљени као безбједни и надограђени поузданим системом провјере старости. |
| | Да бисте помогли родитељима и другима да одлуче да ли је садржај старосно примјерен за дјецу и младе, изградите апликације и услуге на свим медијима да би се ускладили са системима оцјењивања садржаја.<br>Усвојите одговарајуће методе провјере старости да бисте спријечили дјецу и младе да приступају старосно осјетљивом садржају, веб-локацијама, производима или интерактивним услугама.<br>Пружите савјете и подсјетнике 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 дјецу и младе. |
| | Обезбиједите транспарентност цијена за производе и услуге и прикупљене информације о корисницима. Побрините се да се политике прикупљања података придржавају релевантних закона који се тичу приватности дјеце и младих, укључујући и то да ли је потребан пристанак родитеља прије него што комерцијална предузећа могу прикупљати личне податке од дјетета или о њему. |
| | Побрините се да оглашавање или комерцијална комуникација буду јасно препознатљиви као такви.<br>Надгледајте садржај који је доступан онлајн и прилагодите га корисничким групама које ће му вјероватно приступити, на примјер, успостављањем одговарајућих правила за онлајн оглашавање дјеци и младима.<br>Ако понуда садржаја подржава интерактивни елемент, као што је коментарисање, онлајн форуми, друштвене мреже, платформе за игре, чат собе или огласне плоче, успоставите јасан скуп „кућних правила“ на језику прилагођеном купцима у оквиру услуга и корисничких смјерница. |
| | Одлучите који је ниво ангажмана потребан прије покретања онлајн услуге. Услуге усмјерене на привлачење дјеце требало би да представљају само садржаје који су прикладни за младу публику. Ако постоје сумње, могу се консултовати државни органи надлежни за заштиту дјеце. |
| | Обезбиједити јасно и истинито означавање садржаја. Имајте на уму да корисници могу доћи до непримјереног садржаја слиједећи везе на веб-локацијама трећих страна које заобилазе странице за контекстуализацију садржаја. |

| | |
|---|---|
| **Едукација дјеце, родитеља и едукатора о дјечјој безбједности и њиховој одговорној употреби ИК технологија** | Компаније које нуде професионално уређен дигитални садржај могу да допуне техничке мјере образовним активностима које оснажују дјецу предузимањем сљедећих радњи: |
| | Пружите купцима конкретне и јасне информације о садржају, као што су врста садржаја, старосне оцјене односно ограничења, увредљив језик или насиље и одговарајуће доступне родитељске контроле; и информације о томе како пријавити злоупотребу и непримјерен или незаконит садржај и како ће се поступати с извјештајима.<br>У интерактивном свијету 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 дјеце и младих да би могли помоћи и усмјеравати дјецу и младе у избору садржаја приликом куповине и помоћи у успостављању правила понашања.<br>Помозите дјеци (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 дјецу и младе на опрез и одговорност када сурфају интернетом. |
| | Креирајте алате прилагођене старости, попут туторијала и центара за помоћ. По потреби сарађујте са интернетским или личним превентивним програмима и терапеутским клиникама. На примјер, ако постоји ризик да се дјеца 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.<br>Нека безбједносне информације, попут линкова за савјете, буду истакнуте, лако доступне и јасне када буде велика могућност да ће онлајн садржај привући велики број дјеце 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 безбједни да их информације објављене на интернету о дјеци не излажу ризику. Начин препознавања дјеце у професионално уређеном садржају захтијева пажљиво разматрање и варира у зависности од контекста. Прибавите информисани пристанак дјеце када их приказујете у програмима, филмовима, видео-записима итд. гдје 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 дјецу 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 дјеци и младима да схвате свијет у којем живе. Осим што је атрактиван и употребљив, поуздан и безбједан, такав садржај може да допринесе физичком, менталном и социјалном развоју дјеце и младих пружајући нове могућности за забаву и образовање.<br>Потребно је снажно подстицати садржаје који дјеци омогућавају да прихвате различитост и буду позитивни узори. |

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

Раније су интернет свијетом доминирали одрасли, али сада је јасно да су дјеца и млади главни учесници на више платформи у стварању и дијељењу 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 подијеле у три категорије:

- Првенствено апликације за размјену 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 дијеле 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 захтијевају минималну старост за пријаву на платформе, али то је тешко провести јер се провјера старости ослања на пријављену старост. Већина услуга које међусобно повезују нове кориснике такође омогућавају функције дијељења локације, што чини дјецу и младе који користе ове услуге још осјетљивијима на опасности ван интернета.

Табела 4. која је прилагођена правилима која примјењује једна од највећих друштвених мрежа, пружа смјернице 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 дјеце.

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

| | |
|---|---|
| **Увртавање питања права дјетета у све одговарајуће корпоративне политике и процесе управљања** | Сервиси који врше хостинг садржаја који генеришу корисници и који повезују кориснике могу да идентификују, спријече и ублаже негативне ефекте ИК технологија на права дјеце и младих и да идентификују могућности за подршку напретку дјеце и младих. |
| | *Види опште смјернице у Табели 1.* |
| **Развој стандардних процеса ради рјешавања проблема материјала сексуалног злостављања дјеце** | 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 дјеце предузимањем сљедећих 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 забиљежите 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 безбједност да бисте били безбједни да компанија може подносити извјештаје 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 дијете/дјецу и младе. Да бисте се позабавили ситуацијама у којима особље може да буде изложено насилном материјалу, имплементирајте политику или програм за подршку отпорности, безбједности и добробити особља. |
| | Примијените услове из уговора о вршењу услуге и услове за забрану илегалног садржаја и понашања, истичући да:<br>• штетни садржаји, укључујући сумњу на педофилско зближавање са дјецом са намјером било физичког или нефизичког злостављања, неће бити толерисани:<br>• противзаконити садржај, укључујући аплод или даљне ширење материјала сексуалног злостављања дјеце, неће бити толерисан;<br>• 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 дјеце. |
| | Документујте праксу компаније за руковање материјалом сексуалног злостављања дјеце, 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 захтјев 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 посљедице, укључујући:<br>• уклањање садржаја, суспензију или затварање налога прекршиоца;<br>• опозив опције дијељења одређених врста садржаја или коришћења одређених опција;<br>• спречавање контакта са дјецом;<br>• пријављивање случаја надлежним органима. |
| **Успостављање стандардних процеса за борбу против МСЗД** | Промовишите механизме извјештавања за МСЗД или било који други илегални садржај и обезбиједите услове да клијенти знају поднијети пријаву ако открију такав садржај.<br>Успоставите системе и обезбиједите обучено особље за процјену појединачних случајева и предузимање одговарајућих мјера. Успоставите добро организоване и свеобухватне оперативне тимове за корисничку подршку.<br>Идеално би било да се ови тимови обуче за рјешавање 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.<br>Компанија би такође могла да успостави посебне тимове за рјешавање жалби корисника у случајевима када су извјештаји можда поднесени грешком. |
| | Успоставите процесе за тренутно уклањање или блокирање приступа материјалу сексуалног злостављања дјеце, укључујући процесе обавјештавања и уклањања илегалног садржаја одмах након идентификовања истог. Побрините се да треће стране са којима је компанија у уговорном односу имају сличне ефикасне поступке обавјештавања и уклањања.<br>Ако законодавство дозвољава, материјал се може чувати као доказ кривичног дјела 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 мјере заштите сервиса од злоупотребе у погледу хостинга, дистрибуирања или креирања материјала сексуалног злостављања дјеце.<br>Гдје је то могуће, успоставите проактивне техничке мјере за анализу предмета и метаподатака повезаних са профилом ради откривања криминалног понашања или образаца и предузмите одговарајуће мјере. |
| | 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 дјеце. Размотрите проактивне технике идентификације као што су технологија скенирања или људски преглед. |

| | |
|---|---|
| **Стварање безбједнијег и старосно прикладног дигиталног окружења** | Провајдери услуга који нуде садржај креиран од стране корисника могу помоћи у стварању безбједнијег, угоднијег дигиталног окружења за дјецу свих узраста предузимањем сљедећих радњи: |
| | На језику прилагођеном купцима, а у оквиру услуге и корисничких смјерница, дефинишите јасан скуп „кућних правила“ којима се дефинише сљедеће:<br>• природа услуге и оно што се очекује од њених корисника;<br>• шта јесте, а шта није прихватљиво у смислу садржаја, понашања и језика, као и забрану илегалне употребе;<br>• посљедице кршења, као на примјер пријављивање полицији и суспензија корисничког рачуна. |
| | Кључне безбједносне 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 рјешавање различитих проблема, попут примања нежељених комуникација (нежељене поште, малтретирања) или гледања непримјереног садржаја. |
| | Омогућите подешавања видљивости и подјеле садржаја прилагођена узрасту. На примјер, нека поставке приватности и видљивости за дјецу и младе буду по дифолту рестриктивније од поставки за одрасле. |
| | Успоставите минималне старосне захтјеве 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.<br>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 гдје постоје релевантне мјере за заштиту приватности података дјеце. Функција извјештавања или служба за помоћ/центар која може подстакнути кориснике да пријаве људе који су погрешно приказали своју старост. |

| | |
|---|---|
| **Стварање безбједнијег и старосно прикладног дигиталног окружења** (***наставак***) | Заштитите млађе кориснике од нежељене комуникације и обезбиједите да се успоставе смјернице 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 дјецу, фотографије и видео-записи могу се претходно провјерити да би се обезбиједило да дјеца не објављују осјетљиве личне податке о себи или другима. |
| | Бројне мјере могу да се користе за контролу приступа садржају који генеришу корисници и за заштиту дјеце и младих на мрежи од неприкладног или илегалног садржаја. Обавезно користите безбједне лозинке као корак у циљу заштите дјеце и младих у играма и другим поставкама друштвених медија. Остале технике укључују:<br>• преглед дискусионих група ради утврђивања штетних предмета, говора мржње и незаконитог понашања и брисање таквог садржаја када се утврди да крши услове коришћења;<br>• премодерисање огласних плоча са тимом специјализованих модератора за дјецу и младе који проверавају садржај који је у супротности с објављеним "кућним редом". Свака порука се може провјерити прије објављивања, а модератори такође могу да уоче и означе сумњиве кориснике, као и кориснике у невољи;<br>• 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 дјеце, родитеља и едукатора о безбједности дјеце и њиховој одговорној употреби ИК технологија** | Провајдери услуга који нуде садржај који генеришу корисници могу допунити техничке мјере образовним активностима и активностима оснаживања предузимањем сљедећих радњи: |
| | Креирајте дио посвећен безбједносним савјетима, 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 примјер, објашњење веб локација друштвених<br>мрежа и услуга заснованих на локацији, начин приступа интернету путем мобилних уређаја и опције доступне родитељима за примјену контрола. |
| | Обавијестите родитеље о начину пријављивања злоупотребе, погрешне употребе и непримјереног или незаконитог садржаја као и о начину на који ће пријава бити рјешавана. Обавијестите их које су услуге ограничене на старост и друге начине за безбједно и одговорно понашање приликом коришћења интерактивних услуга. |
| | Успоставите систем заснован на „повјерењу и угледу“ да би се подстакло добро понашање и омогућило вршњацима да примјером преносе најбоље праксе. Промовишите важност друштвеног извјештавања, које омогућава људима да се обрате другим корисницима или поузданим пријатељима да би помогли у рјешавању сукоба или започели разговор о забрињавајућем садржају. |
| | Пружите савјете и подсјетнике о природи дате услуге или садржаја и о томе како безбједно уживати у њему. Уградите смјернице заједнице у интерактивне услуге, на примјер, са поп-ап обавјештењима која подсјећају кориснике на одговарајуће и безбједно понашање, попут недавања њихових контакт информација. |
| | Сарађујте са родитељима да бисте били сигурни да их информације објављене на интернету о дјеци не излажу ризику. Прибавите информисани пристанак дјеце када их приказујете у програмима, филмовима, видео-записима итд. гдје 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 дјецу и младе подржавајући њихово право на учешће. |
| | *Види опште смјернице 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 дијелу 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 вјештачкој интелигенцији у посљедњих неколико година, тренутни међународни оквир који штити дјечја права не бави се изричито многим питањима која су покренута развојем и употребом вјештачке 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 дјечја права, попут права на приватност, образовање и играње, као и права на недискриминацију."

Примјена вјештачке интелигенције може да измијени утицај на дјецу 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 дјеци да прегледају и крећу се овим садржајем. Посебна је забринутост да алгоритми који користе препоручене видео-записе могу да заробе дјецу у „филтер мјехурићима“ лошег или неприкладног садржаја. Како су дјеца посебно подложна препорукама за садржај, шокантни "повезани видео-записи" им могу привући пажњу и одвратити их од програмирања прилагођенијег дјеци.

Вјештачка интелигенција такође има утицаја на онлајн заштиту дјеце 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 дјететом), мобилном апликацијом која се користи као приступна тачка за Wi-Fi везу и персонализованим онлајн налогом играчке, односно потрошача, гдје се подаци чувају. Такве играчке комуницирају са серверима заснованим на облаку који чувају и обрађују податке које пружају дјеца која комуницирају с играчком. Овај модел има безбједносне проблеме ако се безбједност не примјењује 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 пријетње дјеци која користе ове уређаје, на примјер, давањем савјета 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 дјеце.

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

УНИЦЕФ и УЦ Беркелеу, “Завршни извјештај: Вјештачка интелигенција и дјечја права”, 2018.

19 Ibid.

20 Ibid.

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

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

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

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

### Унапређење приступа Facebook-а садржају повезаном са самоубиством и самоповређивањем

У 2019. години, Facebook је почео организовати редовне консултације са стручњацима из цијелог свијета 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 Безбједносном центру. Ове консултације за резултат су имале неколико побољшања у начину на који Facebook обрађује ову врсту садржаја. На примјер, ојачана је политика у вези са самоповређивањем да би се забранило графичко резање слика ради избјегавања ненамјерног промовисања или изазивања самоповређивања. Чак и када неко тражи подршку или тврди да помаже опоравак, Facebook сада приказује упозорење преко слика залијечених посјекотина од самоповређивања. Ова врста садржаја сада се открива примјеном вјештачке интелигенције, при чему се аутоматски могу предузети радње на потенцијално штетном садржају, укључујући уклањање истог или додавањем упозорења да се ради о осјетљивом садржају. Од априла до јуна 2019. године, Facebook је нтервенисао код више од
1,5 милиона садржаја самоубистава и самоповређивања на својој веб-локацији и открио више од 95 посто истих прије 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 прије него што их је корисник пријавио.

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

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

24 Ibid.

## Добра пракса: Употреба вјештачке интелигенције у идентификацији материјала сексуалног злостављања дјеце

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

Познате као PDQ и TMK + PDQF, ове технологије су дио 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 вјештачке 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 двије датотеке исте или сличне, чак и без оригиналне слике или видео-записа. Хашеви се такође могу лакше дијелити 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 рјешења намијењених дјеци, а заснованих на вјештачкој интелигенцији.

Ове препоруке се заснивају на УНИЦЕФ-овом раду на изради глобалних смјерница политике о вјештачкој интелигенцији и дјеци, које ће бити намијењене 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 вјештачкој интелигенцији и правима дјетета.

УНИЦЕФ и УЦ Berkeley, “Завршни извјештај: Вјештачка интелигенција и дјечја права”, 2018.

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

| | |
|---|---|
| **Увртавање питања права дјетета 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 дјеце и младих и да идентификују могућности за подршку напретку дјеце и младих. |
| | Системи вјештачке интелигенције треба да се дизајнирају, развијају, имплементирају и истражују да би се поштовала, промовисала и испуњавала дјечја права, како је утврђено у Конвенцији о правима дјетета. Дјетињство, које се све више одвија у дигиталном окружењу, вријеме је посвећено посебној њези и помоћи. Системе вјештачке интелигенције треба искористити тако да ову подршку пруже у пуном потенцијалу. |
| | Уврстите инклузивни приступ дизајну при развоју производа за дјецу, чиме се посвећује максимална пажња родној, географској и културној разноликости и укључује широк спектар интересних страна, попут родитеља, наставника, дјечјих психолога и, према потреби, саме дјеце. |
| | Требало би успоставити оквире управљања, укључујући етичке смјернице, законе, стандарде и регулаторне органе ради надзора процеса којима се спречава да се примјена система вјештачке интелигенције не крше дјечја права. |
| **Развој стандардних процеса ради рјешавања проблема материјала сексуалног злостављања дјеце** | 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 дјеце предузимањем сљедећих радњи: |
| | *Види опште смјернице у Табели 1.* |

| | |
|---|---|
| **Стварање безбједнијег и старосно прикладног дигиталног окружења** | Провајдери система вођених вјештачком интелигенцијом могу да помогну у стварању безбједнијег, угоднијег дигиталног окружења за дјецу свих узраста предузимањем сљедећих радњи: |
| | Усвојите мултидисциплинарни приступ приликом развијања технологија које утичу на дјецу и консултујте се са цивилним друштвом, укључујући академску заједницу, да би се идентификовали потенцијални утицаји ових технологија на права различитих врста потенцијалних крајњих корисника. |
| | Примијените планирану безбједност и планирану приватност за производе и услуге којима се дјеца баве или их често користе. |
| | Како су системи вјештачке интелигенције "гладни" података, компаније које користе вјештачку интелигенцију за своје услуге требало би да користе посебну будност у погледу прикупљања, обраде, складиштења, продаје и објављивања личних података дјеце.<br>Системи вјештачке 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 дјеце.<br>Побрините се да постоје функционални и законски механизми за помоћ ако дјеца јесу или ако тврде да су оштећена системима вјештачке интелигенције.<br>Потребно је успоставити процесе за благовремено исправљање свих дискриминаторних резултата и успоставити надзорне органе за жалбе и континуирано праћење дјечје безбједности и заштите.<br>Одговорност и механизми за обештећење иду руку под руку. |
| | Сачинити планове за руковање посебно осјетљивим подацима, укључујући откривања злоупотребе или друге штете која може да се подијели са компанијом путем њених производа.<br>Дигиталне платформе и системи вјештачке интелигенције требало би да смање прикупљање података о дјеци и повећају дјечју контролу над подацима које креирају. Услови употребе треба да буду разумљиви дјеци да би оснажили своју свијест и способност. |
| **Едукација дјеце, родитеља и едукатора о дјечјој безбједности и њиховој одговорној употреби ИК технологија** | Пружаоци система вођених вјештачком интелигенцијом могу да допуне техничке мјере образовним активностима и активностима оснаживања. |
| | Требало би бити могуће објаснити сврху система са вјештачком интелигенцијом дјеци 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 вјештачком интелигенцијом могу да охрабре и оснаже дјецу и младе подржавајући њихово право на учешће.<br>*Види опште смјернице у Табели 1.* |
| Коришћење технологије | Системи вођени вјештачком интелигенцијом требало би да се развијају да би подржали дјечји напредак у заштити развоја и благостања као резултат у цијелом дизајну система, те едуковали дјецу о развоју и имплементацији. Њихове референте тачке требало би да буду најбоље доступне и широко прихваћене метрике развоја и благостања.<br>Компаније би требало да улажу у истраживање и развој етичких алата заснованих на вјештачкој интелигенцији за откривање радњи онлајн материјала сексуалног злостављања дјеце и онлајн узнемиравања и малтретирања и то у сарадњи са кључним стручњацима за дјечја права и дјецом.<br>Напредак у технологији вјештачке интелигенције требало би да се примијени на циљани, старосно прилагођени *messaging* сервис за дјецу и то без угрожавања њиховог идентитета, локације и личних података. |

## Референце

Текст Опште уредбе о заштити података (Уредба (ЕУ) 2016/679 Парламента и Савјета 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.

Измијењена 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 промјену тржишне стварности и Текста објављеног у Службеном листу ЕУ.

ББЦ политика:

- Политика заштите дјеце и провођења мјера заштите дјеце, 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 дјеце;
- Смјернице: Интеракција са дјецом и младима на мрежи путем уредничких смјерница 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 дјетета, 1989. године, као и од Међуагенцијске радне групе за сексуално искоришћавање дјеце у Терминолошким смјерницама за заштиту дјеце од сексуалног искоришћавања и сексуалног злостављања, 2016. (Луксембуршке смјернице), Конвенције Савјета Европе о заштити дјеце 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 дјецом, док се 18-годишњаци сматрају одраслима осим ако је праг пунољетности нижи према раније прописаном националном закону.

### Вјештачка интелигенција

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

### Системи вјештачке интелигенције

Систем вјештачке 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 вјештачке интелигенције су осмишљени за функционисање на различитим нивоима аутономије.

### Алекса

Амазон Алекса, познат једноставно као Алекса, виртуелни је асистент заснован на вјештачкој 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 вијести. Алекса такође може да контролише неколико паметних уређаја користећи самог себе као систем за аутоматизацију куће. Корисници могу да прошире Алексине могућности инсталирањем "вјештина" (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, “Смјернице за ИКТ компаније у погледу безбједности дјеце на интернету”, 2014.
Савјет Европе, “Шта је вјештачка интелигенција?”.
ОЕЦД (2019), Препоруке Савјета о вјештачкој интелигенцији, https://webcache.googleusercontent
УНИЦЕФ и ИТУ, “Смјернице за ИКТ компаније у погледу безбједности дјеце на интернету”, 2014.

### Најбољи интерес дјетета

Описује све елементе потребне за доношење одлуке у одређеној ситуацији за одређено дијете или групу дјеце.

### Дијете

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

### Сексуално искоришћавање и злостављање дјеце

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

### Сексуално искоришћавање и злостављање дјеце

Брза еволуција ИК технологија створила је нове облике сексуалног искоришћавања и злостављања дјеце на интернету, који могу да се одвијају виртуелно и не морају укључивати физички сусрет лицем у лице са дјететом. Иако правни системи у великом броју држава још увијек означавају слике и видео-записе дјетета сексуалног злостављања као „дјечју порнографију" или „недоличне слике дјеце", ове смјернице се колективно односе на субјекте као материјал за сексуално злостављање дјеце. Ово је у складу са Смјерницама Комисије за широкопојасну мрежу и одговором глобалне сарадње у борби против сексуалног искоришћавања и злостављања дјеце "WePROTECT Global Alliance Model National Response ". Овај појам прецизније описује садржај. Порнографија се односи на закониту, комерцијализовану индустрију, а како Луксембуршке смјернице 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 дјеце […] Овај термин ризици „дјечје порнографије" инсинуира да се дјела врше уз пристанак дјетета и представљају „легитимни сексуални материјал". Израз материјал за сексуално злостављање дјеце односи се на материјал који представља дјела која су сексуално насилна, односно израбљивачка по дијете. То између осталог укључује материјале којима се снима сексуално злостављање дјеце од стране одраслих; слике дјеце укључене у сексуално експлицитно понашање; полни органи дјеце када се слике производе или користе првенствено у сексуалне сврхе.

Види Луксембуршке смјернице за изразе попут „компјутерски или дигитално генерисан материјал сексуалне злоупотребе дјеце".

---

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

### Дјеца и млади

Описује лица млађа од 18 година, при чему појам "дјеца", која се у смјерницама такође називају и млађом дјецом, 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 дјеци 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 дјеце, укључујући имена, геолокацију, адресе, фотографије, аудио и видео-записе.

### Сајбер малтретирање

Термином сајбер малтретирање се описује намјерни 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, намјерно дијељење приватних података, информација, фотографија или видео-записа на штетан начин, слање пријетећих или увредљивих порука (путем е-поште, размјене тренутних порука, чата, текстова), ширење гласина и лажних података о жртви или њихово намјерно 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 вјештине 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 дјечје приватности и лоша безбједност", 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 дјецу и младе, 2019.

Луксембуршке смјернице 2016 и Извјештај 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 вјештине 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 вјештине и критичко размишљање.

### Дигитална отпорност

Овај појам описује способност дјетета да се емоционално носи са повређивањем на интернету. Такође се односи на емоционалну интелигенцију потребну да би се разумјело када је дијете 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 дјететом 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 дјететом ... ,са циљем наговарања дјетета 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 вишенамјенске комерцијалне дигиталне игре путем било ког уређаја повезаног на интернет, укључујући намјенске конзоле, десктоп компјутере, лаптопе, 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 размјену 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 дјетета", Virgin Media and Parent Zone, 2014.
УНИЦЕФ и ИТУ, "Смјернице за ИКТ компаније у погледу безбједности дјеце на интернету", 2014.
(како је наведено изнад)
УНИЦЕФ, Дјечја права и онлајн играње: Прилике и изазови за дјецу 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 снимају све текстове послане 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 обезбјеђења 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 дјетету 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 мјери у смислу дијељења личних података на мрежи, посједовања јавног профила на друштвеним мрежама, дијељења информација са људима које су дјеца упознала на мрежи, коришћења поставки приватности, дијељења лозинки са пријатељима и бриге о приватности.

### Јавни сервиси

Ријеч 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 посљедица дигиталне трансформације путем медија и програма дигиталне писмености и обавеза рјешавања дигиталне подјеле.

### Секстинг

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

---

УНИЦЕФ и ИТУ, “Смјернице за ИКТ компаније у погледу безбједности дјеце на интернету”, 2014. (како је наведено изнад)

Комисија за трговину САД (1998), Закон о заштити приватности дјеце на дигиталним мрежама, 1998. Луксембуршке смјернице, 2016 (како је наведено изнад).

### Сексуално изнуђивање дјеце („sextortion“)

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

### Интернет ствари

Интернет ствари представља сљедећи корак ка дигитализацији друштва и економије, гдје су предмети и људи међусобно повезани комуникационим мрежама и извјештавају о свом статусу односно окружењу.

### УРЛ

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

### Виртуелна стварност

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

### WI-FI

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

---

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

With the support of:









Међународна унија за телекомуникације
**Place des Nations**
**CH-1211 Geneva 20**
**Switzerland**

ISBN: 978-92-61-30411-9

Објављено у Швајцарској
Женева, 2020
Фотографије: Shutterstock