ԵՐԵԽԱՆԵՐԻ ԱՌՑԱՆՑ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՈՒՂԵՑՈՒՅՑ՝ ՆԱԽԱՏԵՍՎԱԾ ՈՒԼՈՐՏԻ ՀԱՄԱՐ

2020

UNION OF OPERATORS

Երեխաների առցանց պաշտպանության ուղեցույց՝ նախատեսված ոլորտի համար

2020

ԳՄՍՀ (ISBN)

«Երեխաների առցանց պաշտպանության ուղեցույց՝ նախատեսված ոլորտի համար» հրատարակության անգլերեն տարբերակի համար:

978-92-61-30081-4 (Թղթային տարբերակ)

978-92-61-30411-9 (Էլեկտրոնային տարբեակ)

978-92-61-30071-5 (EPUB տարբերակ)

978-92-61-30421-8 (Mobil տարբերակ)

Այս թարգմանությունն իրականացվել է «Հայաստանի օպերատորների միություն» ՀԿ-ի կողմից՝ Հեռահաղորդակցության միջազգային միության «Երեխաների առցանց պաշտպանություն» համաշխարհային ծրագրի շրջանակներում: Սույն ուղեցույցում ներկայացված տեսակետների համար «Հայաստանի օպերատորների միություն» ՀԿ-ն պատասխանատվություն չի կրում:

Հեռահաղորդակցության միջազգային միության «Երեխաների առցանց պաշտպանություն» համաշխարհային ծրագրի մասին մանրամասն տեղեկատվություն կարող եք ստանալ հետևյալ հղումով:

ՀՄՄ-ի «Երեխաների առցանց պաշտպանության ուղեցույց՝ նախատեսված ոլորտի համար» ուղեցույցի պաշտոնական տարբերակը ՄԱԿ-ի վեց պաշտոնական լեզուներով հասանելի է հետևյալ հղումով:

Բովանդակություն

Շնորհակալագրեր

Այս ուղեցույցները մշակվել են Հեռահաղորդակցության միջազգային միության, (ՀՄՄ) տեղեկատվական և հեռահաղորդակցության տեխնոլոգիաների (ՏՀՏ) ոլորտում, ինչպես նաև երեխաների (առցանց) պաշտպանության ոլորտում գործող առաջատար հաստատությունների հեղինակներից կազմված աշխատանքային խմբի կողմից և ներառել են հետևյալ կազմակերպությունները.

Եվրոպական հեռարձակման միություն (EBU), «Վերջ երեխաների հանդեպ բռնությանը» գլոբալ գործընկերություն, ՋԻԷՍԷՄԷՅ (GSMA), Հաշմանդամների միջազգային դաշինք (International Disability Alliance), «Ինտերնետի դիտման հիմնադրամ» (IWF), Փրայվիթլի բաժնետիրական ընկերություն և ՅՈՒՆԻՍԵՖ:

Աշխատանքային խումբը ղեկավարում էր Անժան Բոսեն (ՅՈՒՆԻՍԵՖ) և համակարգում էր Ֆենի Ռոտինոն (ՀՄՄ):

Այս ուղեցույցների իրականացումն անհնար կլիներ առանց հեղինակների շահագրգռվածության և մեծ նվիրումի:

Անգնահատելի ներդրում են ունեցել նաև էլեկտրոնային համաշխարհային խմբի (ԷՀԽ), Ֆեյսբուկի, Թենսենթ խաղերի, Թվիթերի, Ուոլթ Դիսնեյ ընկերության, ինչպես նաև ոլորտի այլ շահագրգիռ կողմերը, որոնք ունեն մեկ ընդհանուր նպատակ, այն է՝ համացանցը երեխաների և երիտասարդների համար ավելի լավ և ապահով վայր դարձնելը:

ՀՄՄ-ն երախտապարտ է հետևյալ գործընկերներին, ովքեր ներդրել են իրենց արժեքավոր ժամանակն ու պատկերացումները/մոտեցումները՝ (կազմակերպությունները ներկայացված են այբբենական կարգով).

- Ջիաքոմո Մազոն (Եվրոպական հեռարձակման միություն (EBU))
- Սալմա Աբասի (էլեկտրոնային համաշխարհային խումբ)
- Դեյվիդ Մայլս և Քարոլին Հուրստ (Ֆեյսբուկ)
- Էմի ԿրոկերևՍերենաԹոմազինո («Վերջ երեխաների հանդեպ բռնությանը» գլոբալ գործընկերություն)
- Ջենի Ջոնս (ՋԻԷՍԷՄԷՅ)
- ԼյուսիՌիչարդսոն (Հաշմանդամների միջազգային դաշինք)
- ՖենիՌոտինո (ՀՄՄ)
- ԹեսԼեյլանդ («Ինտերնետի դիտման հիմնադրամ» (ԻԴՀ))
- ԴիպակԹեվարի (Փրայվիթլի ԷսԷյ)
- Ադամ Լիու (Թենսենթ խաղեր)

- Կեյթի Մինշել (Թվիթեր)
- Անժան Բոս, Քարդֆելտ Վինթեր, էմմա Դեյ, Ժոսիան Գելեա Բարոն, Սարա Ժաքովսթեյն և Սթիվեն Էդվին Ոսլու (ՅՈՒՆԻՍԵՖ)
- Ամի Ի. Քանինգհեմ (Ուոլթ Դիսնեյ ընկերություն)

Նախաբան

Թվային տեխնոլոգիաների առաջընթացն աննախադեպ հնարավորություններ է ստեղծել երեխաների և երիտասարդների՝ շփվելու, միանալու, կիսվելու, սովորելու, տեղեկատվություն ստանալու համար, ինչպես նաև արտահայտելու սեփական կարծիքն իրենց կյանքին, համայնքներին առնչվող և ազդեցություն ունեցող հարցերի վերաբերյալ: Սակայն առցանց ծառայությունների ավելի լայն և հեշտ հասանելիությունը նաև զգալի մարտահրավերներ է ստեղծում երեխաների անվտանգության համար՝ ինչպես առցանց, այնպես էլ անցանց: Երեխաներն այսօր բախվում են բազմաթիվ լուրջ ռիսկերի՝ գաղտնիության, հասակակիցների նկատմամբ բռնության, և/կամ տարիքի համար անհամապատասխան բովանդակության խնդիրներից մինչև համացանցային խաբեբաներ և երեխաների դեմ ուղղված հանցագործություններ, ինչպիսիք են՝ առցանց գրումինգը, սեռական բռնությունն ու շահագործումը: Սպառնալիքները բազմապատկվում են, և հանցագործներն ավելի ու ավելի շատ են գործում նաև սահմաններից այն կողմ, ինչը դժվարացնում է նրանց հետևելը և էլ ավելի դժվար պատասխանատվության ենթարկելը:

Բացի այդ, ՔՈՎԻԴ-19 գլոբալ համաճարակի պատճառով, գրանցվել է երեխաների թվի աճ, որոնք առաջին անգամ միանում են առցանց աշխարհին՝ կրթվելու և սոցիալական շփումը պահպանելու համար: Վիրուսի պատճառով դրված սահմանափակումները, մեծահասակների աշխատանքային պարտավորություններին ձեռնամուխ լինելու անհրաժեշտությունը, պատճառ հանդիսացավ, որ շատ երեխաներ սկսեցին առցանց շփվել ավելի վաղ տարիքում և շատ ծնողներ չկարողացան վերահսկել իրենց երեխաներին՝ թողնելով նրանց վտանգի տակ և/կամ հայտնվելու հանցագործների թիրախում, ովքեր զբաղվում են մանկական սեռական բռնության նյութերի արտադրությունով:

Հանցագործներն օգուտներ են քաղում տեխնոլոգիական առաջընթացներից, ինչպիսիք են՝ հավելվածների և խաղերի փոխկապակցումը, ֆայլերի արագ փոխանակումն, ուղիղ հեռարձակումը, կրիպտոարժույթները և գաղտնագրման ծրագրերը:

Զարգացող տեխնոլոգիաները կարող են լինել լուծման մի մասը, օրինակ՝ Ինտերպոլի արհեստական ինտելեկտի վրա հիմնված երեխաների սեռական բռնության տվյալների բազան, որն օգտագործում է պատկերների և տեսանյութերի համեմատման ծրագրակազմ՝ զոհերի, բռնարարների և վայրերի միջև արագ կապեր ստեղծելու համար: Սակայն միայն տեխնոլոգիան խնդրին լուծում չի կարող տալ:

Կառավարությունները, քաղաքացիական հասարակությունը, տեղական համայնքները, միջազգային կազմակերպությունները և ոլորտի շահագրգիռ կողմերը պետք է համախմբվեն ընդհանուր նպատակի համար:

Գիտակցելով դա՝ 2018թ.-ին ՀՄՄ անդամ երկրները խնդրել են երեխաների առցանց պաշտպանության վերաբերյալ մեր ուղեցույցների համապարփակ թարմացում: ՀՄՄ-ի այս նոր ուղեցույցները վերանայվել են, վերաշարադրվել և վերանախագծվել՝ արտացոլելու թվային լանդշաֆտի շատ կարևոր տեղաշարժերը, որում հայտնվում են այս սերնդի երեխաները:

Ի լրումն թվային տեխնոլոգիաների և հարթակների նոր զարգացումներն արտացոլելուն, այս նոր հրատարակությունն անդրադառնում է մի կարևոր բացթողման. իրավիճակին, որին բախվում են հաշմանդամություն ունեցող երեխաները, որոնց համար հատկապես առցանց աշխարհը կարևոր փրկարար օղակ է առաջարկում լիարժեք սոցիալական մասնակցության համար:

Տեխնոլոգիական ոլորտը կարևոր և ակտիվ դերակատարում ունի այսօրվա երեխաների և ապագա սերունդների համար, քանի որ համացանցի վրա հիմնված ծառայությունները և այլ տեխնոլոգիաներն օգտագործման համար ավելի անվտանգ և ապահով են:

Բիզնեսի աշխատանքի հիմքում պետք է մեծապես դրվեն երեխաների շահերը ՝ հատուկ ուշադրություն դարձնելով երիտասարդ օգտատերերի անձնական տվյալների գաղտնիության պաշտպանությանը, նրանց խոսքի ազատության իրավունքի պահպանմանը, մանկական սեռական բռնության նյութերի արտադրության աճող պատուհասի դեմ պայքարին և երեխաների իրավունքների խախտումներին անմիջապես արձագանքելու համար անհրաժեշտ համապատասխան արդյունավետ համակարգերի առկայությանը:

Այնտեղ, որտեղ ներպետական օրենքները դեռ չեն համընկնում միջազգային իրավունքին, յուրաքանչյուր ձեռնարկություն ունի հնարավորություն և պատասխանատվություն՝ համապատասխանեցնելու իր գործառնական շրջանակներն ամենաբարձր չափանիշներին և լավագույն փորձին:

Մենք հուսով ենք, որ անտաբերության համար այս ուղեցույցները կծառայեն որպես ամուր հիմք՝ բիզնես քաղաքականության և նորարար լուծումների մշակման համար: Հպարտ եմ, որ այս ուղեցույցները համաշխարհային համատեղ ջանքերի արդյունք են և համահեղինակվել են միջազգային լայն հանրության փորձագետների կողմից:

Ուրախ եմ ներկայացնելու նաև մեր նոր Երեխաների առցանց անվտանգության (COP) թալիսման Սանգոյին, ընկերասեր, աշխույժ և անվախ կերպար, որը ստեղծվել է մի խումբ երեխաների կողմից՝ երիտասարդների հետ աշխատանքի միջազգային նոր ծրագրի շրջանակներում:

Մի դարաշրջանում, որտեղ ավելի ու ավելի շատ երիտասարդներ են հայտնվում առցանց, ՀՄՄ-ի երեխաների պաշտպանության ուղեցույցներն ավելի կարևոր են դառնում, քան երբևէ: Ոլորտը, կառավարությունները, ծնողներն ու մանկավարժները, ինչպես նաև իրենք՝ երեխաները, բոլորն էլ կենսական դեր ունեն: Ես, ինչպես միշտ, երախտապարտ եմ աջակցության համար և անհամբերությամբ սպասում եմ մեր սերտ համագործակցության շարունակությանն այս կարևոր խնդրի շուրջ:

Տնօրեն՝ Դորին Բոգդան-Մարտին

Հեռահաղորդակցության Զարգացման Գրասենյակ

1. Ամփոփագիր

Այս փաստաթղթի նպատակն է ուղղորդել ՏՀՏ ոլորտի շահագրգիռ կողմերին՝ ստեղծելու երեխաների առցանց պաշտպանության (COP) սեփական ռեսուրսները: Ոլորտի համար նախատեսված «Երեխաների առցանց պաշտպանության» այս ուղեցույցներն ապահովելու են նաև ինչպես կազմակերպությունների տեսլականներն, այնպես էլ օգտատերերին պաշտպանելու նրանց պատասխանատվության վերաբերյալ օգտակար, ճկուն և օգտագործողին հարմար շրջանակ: Դրանք նաև ուղղված են համացանցի ծառայություններն ու հարակից տեխնոլոգիաները երեխաների և ապագա սերունդների համար ավելի անվտանգ և ապահով օգտագործման հիմքեր ստեղծելուն:

Որպես գործիքակազմ՝ այս ուղեցույցները նաև նպատակ ունեն խթանել բիզնեսի հաջողությունը, օգնել խոշոր և փոքր կազմակերպություններին և շահագրգիռ կողմերին, մշակել և պահպանել գրավիչ և կայուն բիզնես մոդել՝ միաժամանակ հասկանալով երեխաների և հասարակության հանդեպ իրավական և բարոյական պարտականությունները:

Ի պատասխան տեխնոլոգիաների զգալի առաջընթացի՝ ՀՄՄ-ն, ՅՈՒՆԻՍԵՖ-ը և երեխաների առցանց պաշտպանության գործընկերները մշակել և թարմացրել են ուղեցույցներն ընկերությունների լայն շրջանակի համար, ովքեր զարգացնում, տրամադրում կամ օգտագործում են հեռահաղորդակցությունը կամ հարակից տեխնոլոգիաներն իրենց ապրանքների և ծառայությունների տրամադրման համար:

Այս փաստաթղթի նպատակն է.

- ՏՀՏ և առցանց ոլորտների և համապատասխան շահագրգիռ կողմերի համար ստեղծել ընդհանուր հղման վայր և ուղեցույց,
- Տրամադրել ուղեցույց ընկերություններին՝ երեխաների իրավունքների, իրենց արտադրանքի և ծառայությունների ցանկացած բացասական ազդեցությունը բացահայտելու, կանխելու և մեղմելու վերաբերյալ,
- Տրամադրել ուղեցույց ընկերություններին՝ բացահայտելու ուղիներ, որոնցով կարող են խթանել երեխաների իրավունքները և նրանց շրջանում թվային քաղաքացիության պատասխանատվությունը,
- առաջարկել ընդհանուր սկզբունքներ՝ բոլոր համապատասխան ոլորտներում ազգային կամ տարածաշրջանային պարտավորությունների հիմքը ստեղծելու համար՝ միաժամանակ գիտակցելով, որ տարբեր բիզնեսներ կօգտագործեն իրականացման տարբեր մոդելներ:

Շրջանակը

Երեխաների առցանց պաշտպանությունը բարդ մարտահրավեր է, որը ներառում է կառավարման, քաղաքականության, գործառնական, տեխնիկական և իրավական բազմաթիվ տարբեր ասպեկտներ: Այս ուղեցույցները փորձում են անդրադառնալ, կազմակերպել և առաջնահերթություն տալ այս ոլորտներից շատերին՝ հիմնվելով առկա և լավ ճանաչված մոդելների, շրջանակների և այլ հղումների վրա:

Ուղեցույցները կենտրոնանում են բոլոր ոլորտների, այդ թվում՝ թվային աշխարհի բոլոր ռիսկերի վրա, որոնք առնչվում են երեխաների պաշտպանությանը և, որպես այդպիսին, ընդգծում ոլորտի շահագրգիռ կողմերի լավագույն փորձը, որը կարող է դիտարկվել կազմակերպության համար երեխաների առցանց պաշտպանության քաղաքականության մշակման և կառավարման գործընթացում: Նրանք ուղղորդում են ոլորտի դերակատարներին ոչ միայն կառավարել անօրինական առցանց գործունեությունը (օրինակ՝ առցանց երեխաների սեռական ոտնձգության նյութերի տարածում), որի դեմ նրանք պարտավոր են գործել իրենց ծառայությունների միջոցով, այլև կենտրոնանում են այլ հարցերի վրա, որոնք կարող են ոչ բոլոր իրավասություններում սահմանվել որպես հանցագործություն: Դրանք ներառում են հասակակիցների միջև բռնություն, կիբերհարձակում և առցանց ոտնձգություն, ինչպես նաև գաղտնիության կամ ընդհանուր բարեկեցության, խարդախության կամ այլ սպառնալիքների հետ կապված հարցեր, որոնք կարող են վնասել երեխաներին միայն որոշակի համատեքստերում:

Այդ նպատակով, այս ուղեցույցները ներառում են առաջարկություններ թվային աշխարհում երեխաների առջև ծառացած ռիսկերին դիմակայելու լավագույն փորձի վերաբերյալ և ինչպես գործել՝ երեխաներին առցանց անվտանգ միջավայր ապահովելու համար: Այս ուղեցույցները խորհուրդներ են տալիս, ինչպես կարող է ոլորտն աշխատել՝ ապահովելով երեխաների անվտանգությունը տեղեկատվական և հաղորդակցական տեխնոլոգիաներից, համացանցից կամ հարակից տեխնոլոգիաներից և սարքերից, ներառյալ բջջային հեռախոսները, խաղային կոնսուլները, համացանցին միացված խաղալիքները, ժամացույցները, իրերի ինտերնետը և արհեստական բանականության վրա հիմնված համակարգերը: Հետևաբար, դրանք ներկայացնում են երեխաների առցանց պաշտպանության հիմնական խնդիրների ու մարտահրավերների ընդհանուր պատկերը և առաջարկում ձեռնարկություններին և շահագրգիռ կողմերին գործողությունների շրջանակ երեխաների առցանց անվտանգության տեղական և ներքին քաղաքականության մշակման համար: Այս ուղեցույցները չեն ներառում այնպիսի ասպեկտներ, ինչպիսիք են՝ քաղաքականության մշակման իրական գործընթացը կամ տեքստը, որը կարող է ներառել ոլորտի համար երեխաների առցանց անվտագության քաղաքականությունը:

Կառուցվածքը

Բաժին 1 – Ընդհանուր պատկերացում.

Այս բաժինը ընդգծում է այս ուղեցույցների նպատակը, շրջանակը և թիրախային լսարանը:

Բաժին 2 – Երեխաների առցանց պաշտպանության ներածություն.

Այս բաժինը ներկայացնում է երեխաների առցանց պաշտպանության հիմնախնդրի ակնարկ՝ ուրվագծելով որոշ նախնական տեղեկություններ, ներառյալ հաշմանդամություն ունեցող երեխաների հատուկ իրավիճակը: Ավելին, այն ներկայացնում է գոյություն ունեցող միջազգային և ազգային մոդելների օրինակներ՝ երեխաներին առցանց անվտանգ պահելու համար՝ որպես ոլորտի շահագրգիռ կողմերի միջամտության հնարավոր ոլորտներ:

Բաժին 3 – Երեխաների իրավունքների պաշտպանության և խթանման հիմնական ոլորտները.

Այս բաժինն ուրվագծում է հինգ հիմնական ոլորտները, որտեղ ընկերությունները կարող են քայլեր ձեռնարկել՝ երեխաների կողմից ՏՀՏ-ներն անվտանգ և ապահով կիրառելու համար:

Բաժին 4 – Ընդհանուր ուղեցույցներ.

Այս բաժինը տալիս է առաջարկություններ ոլորտի բոլոր շահագրգիռ կողմերին՝ ՏՀՏ-ների օգտագործման ժամանակ երեխաների անվտանգությունը պահպանելու և տեխնոլոգիաները դրական կերպով օգտագործելու, ինչպես նաև երեխաների շրջանում պատասխանատու թվային քաղաքացիություն զարգացնելու համար:

Բաժին 5 – Առանձնահատկություններին առնչվող ստուգաթերթեր.

Այս բաժինը շահագրգիռ կողմերին ներկայացնում է հատուկ առաջարկություններ երեխաների իրավունքները հարգելու և աջակցելու կոնկրետ գործողությունների վերաբերյալ՝ հետևյալ հատկանիշներով.

- Առանձնահատկություն Ա. Տրամադրել կապի, տվյալների պահպանման և հոսթինգի ծառայություններ
- Առանձնահատկություն Բ. Առաջարկել ընտրված թվային բովանդակություն
- Առանձնահատկություն Գ. Աջակցել օգտվողների կողմից ստեղծված բովանդակությանը և կապ ապահովել օգտվողների համար
- Առանձնահատկություն Դ. Արհեստական բանականության վրա հիմնված համակարգեր

Թիրախային լսարան

Հիմնվելով Միավորված ազգերի կազմակերպության բիզնեսի և մարդու իրավունքների ուղեցույցույցի[1] վրա՝ երեխաների իրավունքների և բիզնեսի սկզբունքները կոչ են անում ձեռնարկություններին կատարել երեխաների իրավունքները հարգելու պատասխանատվությունը և խուսափել իրենց գործունեության, արտադրանքի կամ ծառայությունների հետ կապված ցանկացած անբարենպաստ ազդեցությունից: Ձեռնարկությունները պետք է ապահովեն երեխաների իրավունքը ինչպես առցանց պաշտպանության, այնպես էլ տեղեկատվության հասանելիության և խոսքի ազատության՝ միաժամանակ խթանելով երեխաների կողմից ՏՀՏ-ների օգտագործումը:

Հեռահաղորդակցության և բջջային հեռախոսների արդյունաբերության տարբեր մասերի, ինտերնետ ընկերությունների և հեռարձակողների միջև ավանդական տարբերություններն արագորեն քանդվում և դառնում են մշուշոտ: Կոնվերգենցիան այս նախկինում տարբեր թվային հոսքերը ներառում է մեկ հոսանքի մեջ, որն աշխարհի բոլոր մասերում հասնում է միլիարդավոր մարդկանց: Համագործակցությունը և գործընկերությունը համացանցի ու հարակից տեխնոլոգիաների ավելի անվտանգ և ապահով օգտագործման հիմքերի ստեղծման բանալին են: Կառավարությունները, մասնավոր հատվածը, քաղաքականություն մշակողները, մանկավարժները, քաղաքացիական հասարակությունը, ծնողներն ու խնամակալները ու բոլորը կենսական դեր ունեն այս նպատակին հասնելու գործում: Ոլորտը կարող է գործել հինգ հիմնական ուղղություններում, ինչպես նկարագրված է 3-րդ բաժնում:

1 Միավորված ազգերի կազմակերպություն «Բիզնեսի և մարդու իրավունքների ուղեցույց սկզբունքներ»

2. Ինչ է երեխաների առցանց անվտանգությունը

Վերջին 10 տարիներին մարդկանց կյանքում զգալիորեն փոխվել է համացանցի օգտագործումն ու դերը: Սմարթֆոնների և պլանշետների տարածվածության, ՎայՖայի (WiFi) և 4G տեխնոլոգիաների հասանելիության, սոցիալական մեդիա հարթակների և հավելվածների զարգացումների հետ մեկտեղ, ավելի ու ավելի շատ մարդիկ են մուտք գործում համացանց տարաբնույթ պատճառներով:

2019 թվականին աշխարհի բնակչության կեսից ավելին օգտվել է համացանցից: Համացանցից օգտվողների ամենամեծ մասնաբաժինը մինչև 44 տարեկան մարդիկ են, ընդ որում համացանցի օգտագործումը հավասարապես բարձր է 16-24 և 35-44 տարեկանների շրջանում: Համաշխարհային մակարդակում համացանցից յուրաքանչյուր երրորդ օգտվողը երեխա է (0-18) տարեկան, և ՅՈՒՆԻՍԵՖ-ի գնահատմամբ՝ երիտասարդների 71 տոկոսն արդեն առցանց է:[2] Համացանցին հասանելիության կետերի տարածումը, շարժական տեխնոլոգիաները և համացանցի միջոցով աշխատող սարքերի աճող զանգվածը, զուգորդված կիբերտարածությունում առկա հսկայական ռեսուրսներն աննախադեպ հնարավորություններ են տալիս սովորելու, կիսվելու և շփվելու:

ՏՀՏ-ի օգտագործման առավելությունները ներառում են սոցիալական ծառայությունների, կրթական ռեսուրսների և առողջապահական խորհրդատվության տեղեկատվության ավելի լայն հասանելիություն: Երեխաները, երիտասարդները և ընտանիքներն օգտագործում են համացանցը և բջջային հեռախոսները՝ տեղեկատվություն, աջակցություն փնտրելու և չարաշահումների դեպքերի մասին զեկուցելու համար, ինչպես նաև այս տեխնոլոգիաները կարող են օգնել երեխաներին և երիտասարդներին պաշտպանել բռնությունից և շահագործումից: Երեխաների պաշտպանության ծառայություններ մատուցողները նույնպես օգտագործում են ՏՀՏ, որպեսզի կարողանան տվյալներ հավաքել, փոխանցել և դրանով իսկ հեշտացնեն ծննդյան գրանցումը, բռնության դեպքերի կառավարումը, տվյալների հավաքագրումը, բռնության քարտեզագրումը և այլն:

Ավելին, համացանցը մեծացրել է տեղեկատվության հասանելիությունն աշխարհի բոլոր աննկյուններում և հնարավորություն ընձեռել երեխաներին ու երիտասարդներին հետազոտել իրենց հետաքրքրությունների շրջանակում գրեթե ցանկացած բան, մուտք գործել համաշխարհային լրատվամիջոցներ, հետապնդել մասնագիտական հեռանկարներ և ձևավորել գաղափարներ ապագայի համար:

2 ՏՀՁԿ, «Նոր տեխնոլոգիաները և 21-րդ դարի երեխաները. վերջին միտումները և արդյունքները», Կրթության աշխատանքային փաստաթուղթ թիվ 179:

ՏՀՏ-ի օգտագործումն երեխաներին և երիտասարդներին հնարավորություն է տալիս պաշտպանել իրավունքներն ու կարծիքն արտահայտել, ինչպես նաև թույլ է տալիս նրանց կապվել և շփվել ընտանիքների ու ընկերների հետ: ՏՀՏ-ները նաև ծառայում են որպես մշակութային փոխանակման և ժամանցի աղբյուր:

Չնայած համացանցի առավելություններին, այնուամենայնիվ, երեխաները և երիտասարդները կարող են նաև հանդիպել մի շարք ռիսկերի ՏՀՏ-ներն օգտագործելիս: Նրանք կարող են ենթարկվել տարիքին անհամապատասխան բովանդակության կամ անպատշաճ շփման, այդ թվում՝ սեռական բռնության պոտենցիալ հանցագործների կողմից: Նրանք կարող են առցանց զգայուն անձնական տեղեկություններ հրապարակելու կամ «սեքսթինգ»-ի միջոցով վնասվել, հաճախ չհասկանալով իրենց և ուրիշների գործողությունների հետևանքներն ու երկարաժամկետ «թվային հետքերը»:

Նրանք նաև բախվում են առցանց գաղտնիության հետ կապված ռիսկերի՝ անձնական տվյալների, գտնվելու վայրի մասին տեղեկատվության հավաքագրում և օգտագործում:

Երեխայի իրավունքների մասին կոնվենցիան հանդիսանում է մարդու իրավունքների ամենալայն միջազգային վավերացված պայմանագիրը[3], որտեղ ներկայացված են երեխաների քաղաքացիական, քաղաքական, տնտեսական, սոցիալական և մշակութային իրավունքները: Այն սահմանում է, որ բոլոր երեխաներն ու երիտասարդներն ունեն կրթության, ժամանցի, խաղի, մշակույթի, ինչպես նաև համապատասխան տեղեակտվության, մտքերի և արտահայտման ազատության, գաղտնիության, տեսակետներն ազատ արտահայտելու իրավունք այն հարցերի վերաբերյալ, որոնք առնչվում են իրենց կարողությունների զարգացմանը:

Կոնվենցիան նաև պաշտպանում է երեխաներին և երիտասարդներին ցանկացած տեսակի բռնությունից, շահագործումից, չարաշահումից, խտրականությունից և սահմանում է, որ երեխայի լավագույն շահը պետք է լինի առաջնային, ուշադրության կենտրոնում: Ծնողները, խնամակալները, մանկավարժները և համայնքի անդամները, ներառյալ համայնքի ղեկավարները և քաղաքացիական հասարակության դերակատարները, պարտավոր են դաստիարակել, աջակցել երեխաներին և երիտասարդներին մինչ նրանց հասուն տարիքը: Կառավարությունները կարևոր դեր ունեն՝ ապահովելու, որ բոլոր շահագրգիռ կողմերը կատարեն այդ դերը:

Ինչ վերաբերում է առցանց երեխաների իրավունքների պաշտպանությանը, ապա արդյունաբերությունները պետք է աշխատեն միասին՝ երեխաների պաշտպանության և տեղեկատվության հասանելիության

3 Միավորված ազգերի կազմակերպության Երեխայի իրավունքների կոնվենցիա. Բոլոր երկրները, բացի երեքից, (Սոմալի, Հարավային Սուդան և ԱՄՆ) վավերացրել են Երեխաների իրավունքների մասին կոնվենցիան:

իրավունքի և խոսքի ազատության միջև մանրակրկիտ հավասարակշռություն հաստատելու համար: Հետևաբար, ընկերությունները պետք է առաջնահերթություն տան երեխաներին և երիտասարդներին առցանց պաշտպանելու միջոցառումներին, որոնք թիրախավորված են և անտեղի չեն սահմանափակում ինչպես երեխայի, այնպես էլ այլ օգտատերերի իրավունքները: Ավելին, աճող կոնսենսուս կա, որ երեխաների և երիտասարդների շրջանում թվային քաղաքացիության խթանումը, ինչպես նաև ապրանքների ու հարթակների մշակումը, որոնք նպաստում են երեխաների կողմից ՏՀՏ-ների դրական օգտագործմանը, պետք է առաջնահերթություն լինեն մասնավոր հատվածի համար:

Թեև առցանց տեխնոլոգիաները երեխաների և երիտասարդների համար շփվելու, նոր հմտություններ սովորելու, ստեղծագործելու և հասարակության բարելավմանը նպաստելու բազմաթիվ հնարավորություններ են ստեղծում, սակայն դրանք կարող են նաև նոր վտանգներ ներկայացնել երեխաների և երիտասարդների անվտանգության համար: Նրանք կարող են երեխաներին և երիտասարդներին ենթարկել պոտենցիալ ռիսկերի և վնասների՝ գաղտնիություն, անօրինական բովանդակություն, ոտնձգությունների, կիբերհարձակում, անձնական տվյալների չարաշահում կամ սեռական նպատակներով վարվելու և նույնիսկ երեխաների սեռական բռնություն և շահագործում: Նրանք կարող են նաև ենթարկվել հեղինակությանը հասցված վնասի, ներառյալ «վրեժ պոռնո» (revenge porn), որը կապված է առցանց կամ «սեքսթինգ»-ի միջոցով զգայուն անձնական տեղեկատվության հրապարակման հետ և օգտատերերի համար բջջային հեռախոսների միջև սեռական բնույթի հաղորդագրություններ, լուսանկարներ կամ պատկերներ ուղարկելուն: Նրանք նաև համացանցից օգտվելիս բախվում են առցանց գաղտնիության հետ կապված ռիսկերի: Երեխաները, իրենց տարիքի և զարգացող հասունության բնույթով, հաճախ չեն կարողանում լիովին հասկանալ առցանց աշխարհի հետ կապված ռիսկերը և իրենց ոչ պատշաճ վարքագծի հնարավոր բացասական հետևանքներն ուրիշների և իրենց վրա:

Չնայած առավելություններին, կան նաև զարգացող և առաջադեմ տեխնոլոգիաների կիրառման բացասական կողմեր: Արհեստական բանականության և մեքենայական ուսուցման, վիրտուալ և ընդլայնված իրականության, մեծ տվյալների, ռոբոտաշինության և իրերի ինտերնետի զարգացումներն էլ ավելի են փոխակերպելու երեխաների և երիտասարդների մեդիա պրակտիկան: Թեև այս տեխնոլոգիաները հիմնականում մշակվում են ծառայությունների մատուցման շրջանակն ընդլայնելու և հարմարավետությունը բարձրացնելու համար (օրինակ՝ ձայնային աջակցության, հասանելիության և թվային ներթափանցման նոր ձևերի միջոցով), սակայն որոշ նման տեխնոլոգիաներ կարող են ունենալ ոչ միտումնավոր ազդեցություն և նույնիսկ չարաշահվել երեխաների սեռական հանցագործների կողմից՝ իրենց մտադրություններն իրականացնելու համար:

Երեխաների և երիտասարդների համար անվտանգ և ապահով առցանց միջավայրի ստեղծումը պահանջում է կառավարությունների, մասնավոր հատվածի և բոլոր շահագրգիռ կողմերի արդյունավետ մասնակցություն: Ծնողների և մանկավարժների թվային հմտությունների և գրագիտության կենտրոնացումը նույնպես պետք է լինի առաջնային թիրախներից մեկը, որին հասնելու գործում ոլորտը կարող է կենսական և էական դեր ունենալ:

Որոշ երեխաներ կարող են լավ պատկերացում ունենալ առցանց ռիսկերի մասին և թե ինչպես արձագանքել դրանց: Այնուամենայնիվ, սա չի կարելի ասել բոլոր երեխաների վերաբերյալ, ամենուր, հատկապես խոցելի խմբերում: Միավորված ազգերի կազմակերպության Կայուն զարգացման նպատակների 16.2-րդ թիրախի համաձայն, որի նպատակն է վերջ դնել չարաշահմանը, շահագործմանը, թրաֆիքինգի և երեխաների նկատմամբ բռնության և խոշտանգումների բոլոր ձևերին, երեխաների առցանց պաշտպանությունը կենսական նշանակություն ունի:

2009 թ.-ին ՀՄՄ-ի կողմից և միջազգային բազմաշահառու ջանքերի արդյունքում ստեղծվել է «Երեխաների առցանց անվտանգություն» նախաձեռնությունը, որը նպատակ ունի բարձրացնել երեխաներին առցանց սպառնացող ռիսկերի և այդ ռիսկերին արձագանքելու իրազեկվածությունը: Նախաձեռնությունը համախմբում է ոլորտի գործընկերներին և գլոբալ հանրության բոլոր հատվածներին՝ ամենուր ապահովելով անվտանգ և ապահով առցանց փորձառություն երեխաների համար: 2009 թ.-ին ՀՄՄ-ն հրապարակեց Երեխաների առցանց անվտանգության ուղեցույցների մի շարք՝ որպես նախաձեռնության մի մաս, որը նախատեսված էր երեք խմբերի համար՝ *երեխաներ, ծնողներ, խնամակալներ և մանկավարժներ, ոլորտ, և քաղաքականություն մշակողներ:* Երեխաների առցանց պաշտպանությունն այս ուղեցույցներում հասկացվում է որպես համապարփակ մոտեցում՝ արձագանքելու բոլոր պոտենցիալ սպառնալիքներին և վնասներին, որոնց կարող են հանդիպել երեխաներն ու երիտասարդներն առցանց տեխնոլոգիաների միջոցով: Այս փաստաթղթում երեխաների առցանց պաշտպանությունը ներառում է նաև երեխաներին հասցված վնասը, որը տեղի է ունենում անցանց ռեժիմում, բայց կապված է առցանց բռնության և ոտնձգության փաստի հետ:

Բոլոր համապատասխան շահագրգիռ կողմերն իրենց համապատասխան դերն ունեն, որպեսզի օգնեն երեխաներին ու երիտասարդներին օգտվել համացանցի հնարավորություններից, միաժամանակ ձեռք բերել թվային գրագիտություն և ճկունություն՝ կապված նրանց առցանց բարեկեցության և պաշտպանության հետ:

Երեխաների և երիտասարդների պաշտպանությունը բոլոր շահագրգիռ կողմերի ընդհանուր պատասխանատվությունն է: Քաղաքականություն մշակողները, ոլորտը, ծնողները, խնամակալները, մանկավարժները և այլ շահագրգիռ կողմերը պետք է ապահովեն,

որ երեխաները և երիտասարդները կարողանան առցանց և անցանց իրենց ներուժն իրականացնել:

Թեև չկա համընդհանուր սահմանում, սակայն Երեխաների առցանց պաշտպանությունը համապարփակ մոտեցում է ցուցաբերում երեխաների և երիտասարդների համար՝ անվտանգ, տարիքային, ներառական և մասնակցային թվային տարածքներ կառուցելով, որոնք բնութագրվում են.

- պատասխան, աջակցություն և ինքնօգնություն սպառնալիքների դեպքում,
- վնասների կանխարգելում,
- դինամիկ հավասարակշռություն պաշտպանություն ապահովելու և երեխաների համար թվային քաղաքացի դառնալու հնարավորություն ընձեռելու միջև,
- պահպանել ինչպես երեխաների, այնպես էլ հասարակության իրավունքներն ու պարտականությունները:

Ավելին, տեխնոլոգիաների և հասարակության արագ առաջընթացի և համացանցի առանց սահմանների բնույթի պատճառով երեխաների առցանց պաշտպանությունը պետք է լինի ճկուն և հարմարեցվող՝ արդյունավետ լինելու համար: Նաև տեխնոլոգիական նորարարությունների զարգացման հետ մեկտեղ ի հայտ կգան նոր մարտահրավերներ և կտարբերվեն ըստ տարածաշրջանների: Սրանք լավագույնս կլուծվեն՝ որպես գլոբալ համայնք միասին աշխատելով, քանի որ այս մարտահրավերներին նոր լուծումներ պետք է գտնել:

2.1 Նախապատմություն

Անհնար է թվային և ֆիզիկական աշխարհներն առանձին դիտարկել:

Նման կապը ահռելի ուժ է տվել, քանի որ համացանցը լիովին ինտեգրված է երեխաների և երիտասարդների կյանքում:

Առցանց աշխարհը թույլ է տալիս երեխաներին ու երիտասարդներին հաղթահարել անլիարժեքությունը, հաշմանդամությունը և նոր ասպարեզներ տրամադրել զվարճանքի, կրթության, մասնակցության և հարաբերությունների կառուցման համար: Ընթացիկ թվային հարթակները օգտագործվում են տարբեր գործողությունների համար և հաճախ մուլտիմեդիա փորձառություններ են:

Երիտասարդների զարգացման համար կարևոր է համարվում հասանելիություն ունենալ և սովորել տեխնոլոգիան օգտագործել, հատկապես, երբ ՏՀՏ-ներն առաջին անգամ օգտագործվում են վաղ տարիքում:

Ուստի շատ կարևոր է, որ բոլոր դերակատարները տեղյակ լինեն, որ երեխաները և երիտասարդները հաճախ սկսում են օգտագործել հարթակներ և ծառայություններ, նախքան կհասնեն սահմանված նվազագույն տարիքին, որին տեխնոլոգիական ոլորտը պետք է համապատասխանի, և, հետևաբար, կրթությունը, պաշտպանական միջոցների հետ մեկտեղ, պետք է ինտեգրվի բոլոր առցանց ծառայությունների մեջ, որոնք օգտագործվում են երեխաների կողմից:

2.1.1 Երեխաները թվային աշխարհում

Համացանցի հասանելիություն

2019 թվականին աշխարհի բնակչության կեսից ավելին օգտվել է ինտերնետից (53,6 տոկոս), մոտ 4,1 միլիարդ օգտատեր: Համաշխարհային մակարդակում համացանցից յուրաքանչյուր երրորդ օգտվողը մինչև 18 տարեկան երեխա է[4]: ՅՈՒՆԻՍԵՖ-ի տվյալներով՝ ամբողջ աշխարհում երիտասարդների 71 տոկոսն արդեն առցանց է[5]: Չնայած նվազագույն տարիքային պահանջներին՝ Ofcom-ը (Միացյալ Թագավորություն Կապի կարգավորող մարմին) գնահատում է, որ 10-12 տարեկան երեխաների գրեթե 50 տոկոսն արդեն ունի սոցիալական մեդիայի հաշիվ[6]: Երեխաներն ու երիտասարդներն այժմ զգալի և մշտական ներկայություն ունեն համացանցում: Համացանցը ծառայում է սոցիալական, տնտեսական, քաղաքական նպատակների և դարձել է ընտանեկան սպառողական ապրանք կամ ծառայություն, որը հանդիսանում է ընտանիքների, երեխաների և երիտասարդների ապրելակերպի անբաժանելի մաս:

2017 թվականին, տարածաշրջանային մակարդակով, երեխաների և երիտասարդների համացանցին հասանելիությունը խիստ կապված էր ազգային եկամտի մակարդակին: Ցածր եկամուտ ունեցող երկրները հակված են ունենալ համացանցից օգտվող երեխաների ավելի ցածր մակարդակ, քան բարձր եկամուտ ունեցող երկրները: Շատ երկրներում երեխաները և երիտասարդներն ավելի շատ ժամանակ են անցկացնում առցանց հանգստյան օրերին, քան աշխատանքային օրերին, ընդ որում 15-17 տարեկան դեռահասներն ամենաերկար ժամանակն են անցկացնում առցանց՝ 2,5- 5,3 ժամ՝ կախված երկրից:

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

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

6 BBC, "Under-age social media use 'on the rise', says Ofcom".

Համացանցից օգտվելը

Երեխաների և երիտասարդների շրջանում համացանց մուտք գործելու ամենատարածված սարքը բջջային հեռախոսն է, որին հաջորդում են անհատական կամ դյուրակիր համակարգիչները: Երեխաները և երիտասարդները շաբաթվա ընթացքում օրական միջինում երկու ժամ են անցկացնում առցանց, իսկ հանգստյան օրերին չորսական ժամ: Թեև ոմանք մշտապես համացանցին հասանելիություն ունեն, սակայն շատերը դեռևս տանը համացանցից օգտվելու հնարավորություն չունեն: Գործնականում համացանցից օգտվող երեխաների և երիտասարդների մեծ մասը համացանցին հասանելիություն ունի մեկից ավելի սարքերի միջոցով, իսկ նրանք, ովքեր միանում են առնվազն շաբաթական, երբեմն օգտագործում են մինչև երեք տարբեր սարքեր: Հարուստ երկրներում ավելի տարիքով երեխաները՝ հատկապես տղաներն ավելի շատ սարքեր են օգտագործում, քան աղջիկները հետազոտված յուրաքանչյուր երկրում:

Թե՛ աղջիկների, թե՛ տղաների շրջանում ամենատարածված գործունեությունը տեսահոլովակներ դիտելն է: Համացանցից օգտվող երեխաների և երիտասարդների ավելի քան երեք քառորդը նշում է, որ շաբաթն առնվազն մեկ տեսանյութ է դիտում առցանց՝ միայնակ կամ իրենց ընտանիքի այլ անդամների հետ: Շատ երեխաներ և երիտասարդներ կարող են համարվել «ակտիվ սոցիալիզատոր»՝ օգտագործելով մի քանի սոցիալական մեդիա հարթակներ, ինչպիսիք են՝ Ֆեյսբուքը, Թվիթերը, Տիկ տոկը կամ Ինստագրամը: Երեխաներն ու երիտասարդները նաև առցանց քաղաքականությամբ են զբաղվում՝ իրենց ձայնը լսելի դարձնելով բլոգավարության միջոցով:

Առցանց խաղերին մասնակցության ընդհանուր մակարդակը տատանվում է ըստ երկրների՝ մոտավորապես համահունչ երեխաների և երիտասարդների համացանցին հասանելիությանը:

Շաբաթական կտրվածքով համացանցից օգտվող երեխաների և երիտասարդների 10-30 տոկոսը ներգրավված է ստեղծագործական առցանց գործունեության մեջ[7]: Տարբեր տարիքի շատ երեխաներ և երիտասարդներ օգտվում են համացանցից կրթություն ստանալու նպատակով, որպեսզի կատարեն տնային աշխատանքները, լրացնեն բաց թողած դասերը կամ փնտրեն բժշկական տեղեկատվություն: Ավելի մեծ երեխաները, կարծես, ավելի մեծ ախորժակ ունեն տեղեկատվության ստանալու, քան փոքր երեխաները:

7 Livingstone, S., KardefeltWinther, D., and Hussein, M. (2019). Global Kids Online Comparative Report, Innocenti Research Report. UNICEF Office of Research - Innocenti, Florence, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html.

Երեխաների առցանց սեռական շահագործում և բռնություն

Երեխաների առցանց սեռական շահագործումը և չարաշահումն աճում է ցնցող տեմպերով: Մեկ տասնամյակ առաջ կար ավելի քան մեկ միլիոն թղթապանակ երեխաների սեռական բռնության նյութերի մասին: 2019-ին այդ թիվը հասել էր 70 միլիոնի, ինչը 2018թ.-ի համեմատ աճել է գրեթե 50 տոկոսով: Բացի այդ, իշխանություններին տրված զեկույցներում չարաշահումների մասին տեսագրություններն առաջին անգամ գերազանցել են լուսանկարներին, ինչը ցույց է տալիս, որ անհրաժեշտ են նոր գործիքներ՝ այս միտումին լուծում տալու համար: Առցանց սեռական չարաշահման և շահագործման զոհերը պատկանում են բոլոր տարիքային խմբերին, բայց գնալով ավելի երիտասարդների են ներքաշում:

2018թ.-ին INHOPE թեժ գծերի ցանցը նշել է զոհերի պրոֆիլների փոփոխություն՝ սեռական հասուն տարիքից մինչև նախասեռական տարիք:

Բացի այդ, 2018 թվականին ECPAT International-ի և ԻՆՏԵՐՊՈԼԻ կողմից իրականացված հետազոտությունը ցույց է տվել, որ փոքր երեխաները ավելի հավանական է, որ ենթարկվեն ծանր բռնությունների, ներառյալ խոշտանգումները, բռնաբարությունները կամ սադիզմը: Սա ներառում է նորածիններ, ովքեր ընդամենը օրական, շաբաթական կամ ամսական են: Չնայած աղջիկներն ավելի շատ են տուժում, սակայն տղաների նկատմամբ բռնությունը կարող է ավելի դաժան լինել: Նույն զեկույցը ցույց է տալիս, որ զեկույցներում նշված զոհերի 80 տոկոսը եղել են աղջիկներ, իսկ 17 տոկոսը՝ տղաներ: Գնահատված զեկույցների 3 տոկոսում հիշատակվել են երկու սեռերի երեխաներ:[8]

Տվյալների պատկերը[9]

- Աշխարհում համացանցի յուրաքանչյուր երրորդ օգտատերը երեխա է:
- Յուրաքանչյուր կես վայրկյանը մեկ երեխան առաջին անգամ միանում է համացանցին:
- 800 միլիոն երեխա օգտվում է սոցիալական ցանցերից:
- Մոտ 750,000 անձ ցանկացած պահի առցանց, ըստ հաշվարկների, ցանկանում է կապ հաստատել երեխաների հետ սեռական նպատակներով:
- ԵՎՐՈՊՈԼ-ի պահոցում կան երեխաների սեռական շահագործման և բռնության (ԵՍՇԲ) ավելի քան 46 միլիոն եզակի լուսանկարներ կամ տեսանյութեր:

8 ECPAT and Interpol, "Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: summary report", 2018.
9 End Violence Against Children, "Safe Online".

- Զոհերի ավելի քան 89 տոկոսը 3-13 տարեկան են:

Առցանց ԵՍՇԲ-ի մասշտաբների և արձագանքների մասին լրացուցիչ տեղեկությունների համար տե՛ս WePROTECT Global Alliance.

2.1.2 Տարբեր հարթակների ազդեցությունը երեխաների թվային փորձի վրա

Համացանցը և թվային տեխնոլոգիաները երեխաների և երիտասարդների համար ներկայացնում են հնարավորություններ և ռիսկեր: Դրանցից մի քանիսը ներկայացված են ստորև:

Երբ երեխաները օգտվում են սոցիալական ցանցերից, ապա նրանք օգտվում են ուսումնասիրելու, սովորելու, հաղորդակցվելու և հիմնական հմտությունները զարգացնելու բազմաթիվ հնարավորություններից: Սոցիալական ցանցերը երեխաների կողմից դիտվում են որպես հարթակներ, որոնք թույլ են տալիս բացահայտել անձնական ինքնությունն անվտանգ միջավայրում: Երիտասարդների համար կարևոր է համապատասխան հմտություններ ունենալը և իմանալ, թե ինչպես լուծել գաղտնիության և հեղինակության հետ կապված խնդիրները:

«Ես գիտեմ, որ այն ամենը, ինչ դուք տեղադրում եք համացանցում, մնում է այնտեղ, և դա կարող է ազդել ձեր կյանքի վրա ապագայում», *14-ամյա տղա, Չիլի:*

Այնուամենայնիվ, հարցումները ցույց են տալիս, որ երեխաների մեծ մասն օգտվում է սոցիալական ցանցերից մինչև 13 տարեկանը դառնալը, և տարիքի ստուգման ծառայությունները հիմնականում թույլ են կամ բացակայում են, ապա երեխաների առջև ծառացած ռիսկերը կարող են լուրջ լինել: Ավելին, մինչ երեխաները ցանկանում են սովորել թվային հմտություններ, դառնալ թվային քաղաքացիներ և վերահսկել գաղտնիության կարգավորումները, նրանք հակված են հաշվի առնել գաղտնիությունն իրենց ընկերների և ծանոթների հետ կապված՝ «Ինչ կարող են տեսնել իմ ընկերները», և ավելի քիչ՝ կապված անծանոթների և երրորդ անձանց հետ: Սա զուգորդված է երեխաների բնական հետաքրքրասիրությանը, ընդհանուր առմամբ, ռիսկը չգնահատելով, ինչը կարող է նրանց խոցելի դարձնել գրումինգի, շահագործման, ահաբեկման կամ այլ տեսակի վնասակար բովանդակության կամ շփման նկատմամբ:

Բջջային հավելվածների միջոցով լուսանկարների և տեսանյութերի փոխանակման լայն տարածվածությունը, մասնավորապես, երեխաների կողմից ուղիղ հեռարձակման հարթակների օգտագործումը, ավելացնում է գաղտնիության վերաբերյալ մտահոգությունները և ռիսկերը: Որոշ երեխաներ ստեղծում են իրենց, ընկերների և եղբայրների սեռական լուսանկարները և դրանք տարածում են համացանցում:

2019թ.-ին Համացանցի դիտման հիմնադրամի (IWF) կողմից դիտարկված բոլոր վեբ էջերի գրեթե մեկ երրորդը (29 տոկոսը) պարունակում էր ինքնուրույն ստեղծված լուսանկարներ: Նրանցից 76 տոկոսում ներկայացված են եղել 11-13 տարեկան աղջիկներ, որոնց մեծ մասը իրենց ննջասենյակներում կամ տան այլ սենյակներում են: Ոմանց, հատկապես, ավելի մեծ երեխաների դեպքում, կարող է այդ վարքը դիտարկվել որպես սեռականության և սեռական ինքնության բնական ուսումնասիրություն, մինչդեռ մյուսների, հատկապես՝ փոքր երեխաների դեպքում, կա հաճախ հարկադրանք մեծահասակի կամ այլ երեխայի կողմից: Ինչ էլ որ լինի, արդյունքում ստացված բովանդակությունը շատ երկրներում անօրինական է և կարող է երեխաներին ենթարկել հետապնդման ռիսկի կամ օգտագործվել երեխային հետագա շահագործման, գրումինգի կամ շորթման համար:

Նմանապես, առցանց խաղերը երեխաներին հնարավորություն են տալիս իրականացնելու իրենց խաղալու հիմնարար իրավունքը, ինչպես նաև ստեղծել կապեր, ժամանակ անցկացնել ընկերների հետ, ձեռք բերել նոր ընկերներ և զարգացնել կարևոր հմտություններ: Թեև դա կարող է լինել ճնշող մեծամասնությամբ դրական, որոշ դեպքերում չվերահսկվող և պատասխանատու չափահասների կողմից չաջակցվող, սակայն խաղային հարթակները կարող են նաև վտանգներ ներկայացնել երեխաների համար: Սա ներառում է չափից ավելի խաղի վրա ժամանակ ծախսելը, ֆինանսական ռիսկեր, որոնք կապված են խաղի մեջ չափից դուրս գնումներին, ինչպես նաև ոլորտի դերակատարների կողմից երեխաների անձնական տվյալների հավաքագրման և դրամայնացման, կիբերհարձակման, ատելության խոսքի, բռնության և անպատշաճ պահվածքի կամ բովանդակության ենթարկվելու, գրումինգի, իրական կամ համակարգչով ստեղծած կամ նույնիսկ վիրտուալ իրականության պատկերներ և տեսանյութեր, որոնք պատկերում են ԵՍԾԲ-ն: Այս ռիսկերը միայն խաղային միջավայրի համար չեն, այլ վերաբերում են նաև թվային միջավայրերին, որտեղ երեխաները ժամանակ են անցկացնում:

Ավելին, տեխնոլոգիայի զարգացումները հանգեցրել են «Իրերի ինտերնետի» առաջացմանը, որտեղ համացանցին միացված մի շարք սարքեր կարող են հաղորդակցվել և կապվել համացանցի միջոցով: Սա ներառում է խաղալիքներ, մանկական մոնիտորներ և արհեստական ինտելեկտով աշխատող սարքեր, որոնք կարող են վտանգ ներկայացնել գաղտնիության և անցանկալի շփման տեսանկյունից:

Լավագույն փորձ. հետազոտություն

Առցանց կամ կիբերհարձակման համատեքստում Մայքրոսոֆթը հետազոտություն է անցկացրել թվային անվտանգության և կիբերհարձակման վերաբերյալ: 2012 թվականին այն 25 երկրներում 8-17 տարեկան երեխաների հարցում է անցկացրել առցանց բացասական վարքագծի վերաբերյալ: Արդյունքները ցույց են տվել, որ միջին հաշվով մասնակիցների 54 տոկոսը նշել է, որ անհանգստացած է, որ կենթարկվի առցանց բռնության: 37 տոկոսը նշել է, որ իրենք ենթարկվել են կիբերհարձակման, իսկ 24 տոկոսը բացահայտել է, որ իրենք ինչ-որ մեկին ահաբեկել են: Նույն հարցումը ցույց է տվել, որ 10 ծնողից երեքն են իրենց երեխաների հետ քննարկել առցանց ահաբեկման հարցերը: 2016 թվականից ի վեր Մայքրոսոֆթը կանոնավոր հետազոտություն է անցկացնում առցանց ռիսկերի վերաբերյալ՝ տրամադրելով Digital Civility Index տարեկան հաշվետվություններ:

FACES-ը մուլտիմեդիա ծրագիր է, որը արտադրվել է ՆՀԿ Ճապոնիայի (NHK Japan) և հանրային ծառայությունների տարբեր հեռարձակողների կոնսորցիումի կողմից՝ ամբողջ աշխարհում առցանց և անցանց ահաբեկման զոհերի պատմություններով: Այն դեռահասների վերաբերյալ տեսաշարք է, որոնցում հերոսները տեսախցիկի առաջ բացատրում են, թե ինչպես են նրանք արձագանքում համացանցի միջոցով հարձակումներին: Շարքը, որը պատրաստվել է նաև երկու րոպեանոց հոլովակներով, ընդունվել է ՖԵՅՍԲՈՒՔ-ի, ՅՈՒՆԵՍԿՕ-ի և Եվրոպայի խորհրդի կողմից և հասանելի է բազմաթիվ լեզուներով:

2019-ին ՅՈՒՆԻՍԵՖ-ը հրապարակեց «Երեխայի իրավունքներ և առցանց խաղեր. հնարավորություններ և մարտահրավերներ երեխաների և ոլորտի համար» թեմայով քննարկման փաստաթուղթ՝ երեխաների համար ամենաարագ զարգացող ժամանցային ոլորտներից մեկի հնարավորություններն ու մարտահրավերները լուծելու համար: Փաստաթուղթն ուսումնասիրում է հետևյալ թեմաները.

- Երեխաների խաղալու իրավունքը և արտահայտվելու ազատությունը (խաղի ժամանակը և առողջության հետևանքները).
- Խտրականության բացակայություն, մասնակցություն և պաշտպանություն չարաշահումներից (սոցիալական փոխազդեցություն և ներառում, թունավոր միջավայրեր, տարիքային սահմանափակումներ և ստուգում, պաշտպանություն գրումինգից և սեռական բռնությունից);
- Գաղտնիության և տնտեսական շահագործումից ազատվելու իրավունք (տվյալների համար մատչելի բիզնես մոդելներ, անվճար խաղեր և դրամայնացում, առևտրային բովանդակության թափանցիկության բացակայություն)

Լավագույ փորձ. Տեխնոլոգիա

Գուգլի Վիրտուալ Իրականության Գործողությունների Լաբորատորիան ուսումնասիրում է, թե ինչպես կարող է վիրտուալ իրականությունն օգնել խրախուսել երիտասարդներին դիմակայել անցանց և առցանց սպառնալիքներին[10]:

2019 թվականի սեպտեմբերին «ԲիԲիՍի»-ն գործարկեց «**Own IT**» կոչվող բջջային հավելվածը, որը բարեկեցության ծրագիր է և ուղղված է 8-13 տարեկան երեխաներին, ովքեր ստանում են իրենց առաջին սմարթֆոնը: Հավելվածը «Բիբիսի»-ի հանձնառության մի մասն է՝ աջակցելու երիտասարդներին այսօրվա փոփոխվող մեդիա միջավայրում և հետևում է Own IT կայքի հաջող գործարկմանը 2018 թվականին: Հավելվածը համատեղում է մեքենայական ուսուցման գերժամանակակից տեխնոլոգիան՝ սմարթֆոն օգտագործող երեխաների գործունեությանը հետևելու համար՝ երեխաների հուզական վիճակի մասին ինքնուրույն զեկուցելու հնարավորությամբ:

Այն օգտագործում է այս տեղեկատվությունը հարմարեցված բովանդակություն տրամադրելու և միջամտելու համար, որոնք օգնում են երեխաներին երջանիկ և առողջ մնալ առցանց՝ առաջարկելով ընկերական և աջակցող մղումներ, երբ նրանց վարքագիծը նորմայից շեղվում է: Օգտատերերը կարող են մուտք գործել հավելված, երբ նրանք օգնություն են փնտրում, բայց այն նաև պատրաստ է ակնթարթային, էկրանային խորհուրդներ տալու և աջակցելու, երբ դրա կարիքն ունեն՝ հատուկ մշակված ստեղնաշարի միջոցով: Հատկանիշները ներառում են.

- Հիշեցնել օգտատերերին մտածել երկու անգամ, նախքան սոցիալական ցանցերում անձնական տվյալներ տարածելը, օրինակ՝ բջջային հեռախոսի համարները:
- Օգնել նրանց հասկանալ թե ինչպես հաղորդագրությունները կարող են ընկալվել ուրիշների կողմից «նախքան ուղարկել» կոճակը սեղմելը:
- Հետևել նրանց տրամադրությանը ժամանակի ընթացքում և առաջարկել ուղեցույց, թե ինչպես բարելավել իրավիճակը, եթե անհրաժեշտ է:
- Տեղեկատվության տրամադրում այնպիսի թեմաների վերաբերյալ, ինչպիսիք են մինչև ուշ գիշերը հեռախոսներից օգտվելը և դրանց ազդեցությունն օգտատերերի բարեկեցության վրա:

Հավելվածը պարունակում է հատուկ պատվիրված բովանդակություն «ԲիԲիՍի»-ից: Այն տրամադրում է օգտակար նյութեր և ռեսուրսներ՝ օգնելու երիտասարդներին առավելագույն օգուտ քաղել առցանց ժամանակից և ձևավորել առողջ առցանց վարքագիծ և սովորություններ:

10 Հավելյալ տեղեկատվության համար, տե՛ս Alexa Hasse et al., "Youth and Cyberbullying: Another Look", Berkman Klein Center for Internet & Society, 2019.

Այն օգնում է երիտասարդներին և ծնողներին առցանց ավելի կառուցողական զրույցներ վարել փորձառությունների մասին, սակայն ծնողներին հաշվետվություններ կամ հետադարձ կապ չի տրամադրի, և օգտատերերի սարքերից որևէ տվյալ չի թողնի: Հավելվածը չի հավաքում օգտատիրոջ կողմից ստեղծված որևէ անձնական տվյալ կամ բովանդակություն, քանի որ ամբողջ մեքենայական ուսուցումն իրականացվում է հավելվածում և օգտատիրոջ սարքում: Մեքենաները վերապատրաստվում են առանձին՝ վերապատրաստման տվյալների վերաբերյալ, որպեսզի համոզվեն, որ գաղտնիության խախտումներ չկան:

2.1.3 Հաշմանդամություն ունեցող երեխաների հատուկ իրավիճակը[11]

Հաշմանդամություն ունեցող երեխաներն ու երիտասարդներն, ինչպես հաշմանդամություն չունեցողներն, առցանց բախվում են ռիսկերի, բացի այդ, նրանք կարող են բախվել իրենց հաշմանդամության հետ կապված հատուկ ռիսկերի: Հաշմանդամություն ունեցող երեխաներն ու երիտասարդները հաճախ բախվում են իրենց շրջապատում մասնակցելու բացառման, խարանման և խոչընդոտների (ֆիզիկական, տնտեսական, հասարակական և վերաբերմունքի): Այս փորձառությունները կարող են բացասական ազդեցություն ունենալ հաշմանդամություն ունեցող երեխայի վրա և ստիպել նրան փնտրել սոցիալական փոխազդեցություններ և ընկերական հարաբերություններ առցանց տարածություններում: Թեև նման փոխազդեցությունները կարող են դրական լինել՝ աջակցելով ինքնագնահատականի ձևավորմանը և աջակցող կապերի ստեղծմանը, բայց դրանք կարող են նաև նման երեխաներին գրումինգի, առցանց բռնության և/կամ սեռական ոտնձգության դեպքերի ավելի մեծ ռիսկի ենթարկել: Հետազոտությունները ցույց են տալիս, որ այն երեխաները և երիտասարդները, ովքեր դժվարություններ են ունենում իրական կյանքում, և նրանք, ովքեր տառապում են հոգեսոցիալական դժվարություններից, նման միջադեպերի մեծ ռիսկի են ենթարկվում:[12]

Ընդհանուր առմամբ, այն երեխաները, ովքեր զոհ են դարձել իրական կյանքում, ամենայն հավանականությամբ, կարող են զոհ դառնալ նաև առցանց: Սա հաշմանդամություն ունեցող երեխաներին ավելի մեծ վտանգի տակ է դնում առցանց, սակայն նրանք առցանց լինելու ավելի մեծ կարիք ունեն:

11 Տես Եվրոպայի խորհուրդ, "Two clicks forward and one click back: report on children with disabilities in the digital environment", 2019.
12 Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content", Berkman Center for Internet & Society, 2008.

Հետազոտությունները ցույց են տալիս, որ հաշմանդամություն ունեցող երեխաներն ավելի հավանական է, որ ենթարկվեն ցանկացած տեսակի բռնության[13], մասնավորապես՝ սեռական բնույթի:[14] Վիկտիմիզացիան կարող է ներառել բուլինգ, ոտնձգություն, բացառում և խտրականություն՝ հիմնված երեխայի փաստացի կամ ընկալվող հաշմանդամության կամ նրա հաշմանդամության հետ կապված ասպեկտների վրա, ինչպես, օրինակ, նրանց վարքագծի կամ խոսելու ձևն, այնպես էլ օգտագործվող սարքավորումներն ու ծառայությունները:

Հաշմանդամություն ունեցող երեխաների և երիտասարդների նկատմամբ գրումինգի, առցանց ոտնձգությունների և/կամ սեռական բնույթի բռնությունների հեղինակները կարող են լինել ոչ միայն հանցագործները, որոնք թիրախ են դարձնում երեխաներին և երիտասարդներին, այլև նրանք, ովքեր թիրախ են դարձնում հենց հաշմանդամություն ունեցող երեխաներին և երիտասարդներին: Նման հանցագործները կարող են լինել «նվիրյալներ»՝ հաշմանդամություն չունեցող մարդիկ, ովքեր սեքսուալ հետաքրքրություն ունեն հաշմանդամություն ունեցող անձանց նկատմամբ (առավել հաճախ անդամահատվածներ և շարժունակության սարքեր օգտագործող անձինք), որոնցից ոմանք նույնիսկ հաշմանդամ են ձևանում:[15] Նման մարդկանց գործողությունները կարող են ներառել հաշմանդամություն ունեցող երեխաների և երիտասարդների, (որոնք իրենց բնույթով անվնաս են) լուսանկարներ և տեսանյութեր ներբեռնելը և/կամ դրանց տարածումը հատուկ ֆորումների կամ սոցիալական մեդիայի միջոցով: Ֆորումներում և սոցիալական ցանցերում զեկուցման գործիքները հաճախ չունեն համապատասխան ուղի նման գործողությունների դեմ պայքարելու համար:

Մտահոգություններ կան, որ «կիսվելը» (ծնողներն իրենց երեխաների և երիտասարդների մասին տեղեկություններ և լուսանկարներ են տարածում առցանց) կարող է խախտել երեխայի գաղտնիության իրավունքը, հանգեցնել բուլինգի և ամաչելու կամ բացասական հետևանքներ ունենալ հետագա կյանքում:[16] Հաշմանդամություն ունեցող երեխաների որոշ ծնողներ կարող են կիսվել իրենց երեխայի մասին տեղեկատվությամբ սոցիալական ցանցերով՝ փնտրելով աջակցություն կամ խորհուրդ, արդյունքում՝ իրենց երեխային գաղտնիության խախտման վտանգի ենթարկելով ինչպես հիմա, այնպես էլ ապագայում: Նման ծնողները նաև վտանգի են ենթարկվում անտեղյակ կամ անբարեխիղճ մարդկանց կողմից, ովքեր առաջարկում են բուժում, թերապիա կամ «բուժումներ» երեխայի հաշմանդամության համար:

13 UNICEF, "State of the World's Children Report: Children with Disabilities," 2013.
14 Katrin Mueller-Johnson et al., "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors", Journal of Interpersonal Violence, 2014.
15 Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder", Sexuality and Disability, 1997.
16 UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy", Innocenti Discussion Paper 2017-03 .

Հաշմանդամություն ունեցող երեխաների և երիտասարդների որոշ ծնողներ կարող են չափազանց «պաշտպանող» լինել, քանի որ նրանք չգիտեն, թե ինչպես լավագույնս առաջնորդեն իրենց երեխային համացանցից օգտվելիս կամ գրումինգից ու ոտնձգություններից:[17]

Հաշմանդամություն ունեցող որոշ երեխաներ և երիտասարդներ կարող են դժվարություններ ունենալ առցանց միջավայրերում կամ անհասանելի դիզայնի պատճառով (օրինակ՝ հավելվածներ, որոնք թույլ չեն տալիս մեծացնել տեքստի չափը), կամ էկրանի ընթերցման ծրագրակազմի բացակայությունը կամ համապատասխան աջակցության անհրաժեշտություն, (օրինակ՝ ուսուցում, թե ինչպես օգտագործել սարքավորումներն, անհատական աջակցություն սոցիալական փոխազդեցությունների նավարկության համար):18

2.2 Երեխաների առցանց պաշտպանության գոյություն ունեցող ազգային և անդրազգային մոդելներ

Համաշխարհային մակարդակում մի քանի մոդելներ են ընդունվում՝ երեխաներին և երիտասարդներին առցանց անվտանգ պահելու համար: Ոլորտի շահագրգիռ կողմերը պետք է դրանք դիտարկեն որպես միջազգային նախաձեռնությունների ուղեցույց և որպես հենք՝ երաշխավորելու, որ նրանք ջանք չեն խնայում երեխաներին և երիտասարդներին առցանց պաշտպանելու համար: Ինտերնետային ոլորտը բազմազան և բարդ ասպարեզ է, որը կազմված է տարբեր չափերի և գործառույթների ընկերություններից: Կարևոր է, որ երեխաների պաշտպանությանն ուղղված լինի ոչ միայն բովանդակության վրա հիմնված հարթակներն ու ծառայությունները, այլ նաև համացանցի ենթակառուցվածքներին աջակցող հարթակները:

Պետք է նշել, որ ոլորտի կարողությունները երեխաների պաշտպանության համապարփակ քաղաքականություն ներդնելու համար սահմանափակված են առկա ռեսուրսներով: Հետևաբար, այս ուղեցույցները խորհուրդ են տալիս, որ ոլորտները միասին աշխատեն՝ օգտվողներին պաշտպանելու ծառայություններ տեղակայելու համար: Կիսելով ռեսուրսները և ինժեներական փորձը, ոլորտները կկարողանան ավելի արդյունավետ կերպով ստեղծել «անվտանգ տարածքներ»՝ չարաշահումները կանխելու համար:

17 UNICEF, "Is there a ladder of children's online participation?", Innocenti Research Brief, 2019.
18 Ուղեցույցները տե՛ս.United Nations Convention on the Rights of Persons with Disabilities and Optional Protocol, հատկապես մատչելիության մասին 9-րդ հոդվածը և խոսքի և կարծիքի ազատության և տեղեկատվության հասանելիության մասին 21-րդ հոդվածը:

Ոլորտային համագործակցություն

Տեխնոլոգիական կոալիցիան (The Technology Coalition) ոլորտի շահագրգիռ կողմերի հաջողված համագործակցության և ԵՍՇԲ-ի դեմ պայքարի օրինակ է:

Անդրազգային մոդելներ

Ոլորտներն իրենց կառուցվածքային ծրագրում պետք է ներառեն համապատասխան միջազգային ուղեցույցներ, ինչպես նաև հետևեն իրենց գործունեության վայրի երկրում կիրառվող ցանկացած համապատասխան ազգային կամ անդրազգային օրենսդրությանը: Ոլորտները ոչ միայն պետք է հաշվի առնեն այն գործողությունները, որոնք նրանք պետք է ձեռնարկեն օրինական մակարդակում, այլ նաև, թե ինչ գործողություններ կարող են իրականացնել, իսկ հնարավորության դեպքում, ձգտեն իրականացնել նախաձեռնություններ ամբողջ աշխարհում: Որոշ մոդելներ, որոնք ապահովում են նման նախաձեռնությունների սկզբունքները, ներառում են.

- Հինգ երկրի նախարարական կամավոր սկզբունքներ՝ առցանց ԵՍՇԲ-ին դիմակայելու համար (2020 թ.);
- Լայնաշերտ ինտերնետի կայուն զարգացման հանձնաժողով, երեխաների առցանց անվտանգություն. բռնության, չարաշահման և շահագործման առցանց ռիսկի նվազեցում (2019);
- WePROTECT գլոբալ դաշինք, գլոբալ ռազմավարական պատասխան երեխաների առցանց սեռական շահագործման և չարաշահման նկատմամբ (2019 թ.);
- Համաշխարհային գործընկերություն երեխաների նկատմամբ բռնությանը վերջ դնելու համար, Անվտանգ է սովորել. Գործողության կոչ;
- Երեխաների արժանապատվությունը թվային աշխարհում, Երեխաների արժանապատվության դաշինք, տեխնոլոգիական աշխատանքային խմբի հաշվետվություն (2018);
- Եվրոպական խորհրդարանի և Խորհրդի 2018/1808 դիրեկտիվ (ԵՄ). Աուդիո վիզուալ մեդիա ծառայությունների դիրեկտիվ
- Եվրոպական հանձնաժողովի տվյալների պաշտպանության ընդհանուր կանոնակարգ (2018 թ.);
- ՏՀՀԿ-ի խորհուրդները առցանց երեխաների պաշտպանության վերաբերյալ (2012 թ.):

Ազգային մոդելներ

Գոյություն ունեն մի շարք ազգային և միջազգային մոդելներ, որոնք սահմանում են տեխնոլոգիական ոլորտի հստակ դերերն ու պարտականությունները երեխաների առցանց պաշտպանությանն առնչվող հարցերում:

Սրանցից մի քանիսը հենց հատուկ երեխաների համար չեն, բայց կարող են կիրառվել նրանց համար որպես համացանցի օգտատերեր: Նրանք ոլորտի համար ընդհանուր ուղեցույցներ են տրամադրում՝ կապված կարգավորող քաղաքականության, ստանդարտների և այլ ոլորտների հետ համագործակցության վերաբերյալ: Այս փաստաթղթի նպատակների համար ընդգծված են նման մոդելների հիմնական սկզբունքները, որոնք վերաբերում են ՏՀՏ ոլորտին:

Տարիքին համապատասխան մոտեցումներ, Միացյալ Թագավորություն

2019 թվականի սկզբին Տեղեկատվության հանձնակատարի գրասենյակը առաջարկներ է հրապարակել երեխաների՝ տարիքին համապատասխան տվյալների պաշտպանության վերաբերյալ: Առաջարկվող օրենսգիրքը հիմնված է երեխայի լավագույն շահերի վրա, ինչպես ամրագրված է Միավորված ազգերի կազմակերպության՝ Երեխայի իրավունքների կոնվենցիայում, և ոլորտի համար մի շարք ակնկալիքներ է սահմանում: Առաջարկները բաղկացած են տասնհինգ ստանդարտներից, օրինակ՝ տեղորոշման ծառայությունները երեխաների համար պետք է անջատված լինեն, ոլորտը պետք է հավաքի և պահպանի երեխաների անձնական տվյալների նվազագույն քանակություն, արտադրանքը լինի նախագծված, անհատական, իսկ բացատրությունները՝ տարիքին համապատասխան և հասանելի:

Վնասակար թվային հաղորդակցության մասին օրենքը, Նոր Զելանդիա

2015 թվականին ընդունված օրենքը կիբեր չարաշահումը դարձրեց հատուկ հանցագործություն և կենտրոնացած է վնասների լայն շրջանակի վրա՝ կիբերհարձակումից մինչև «վրեժ-պոռնոգրաֆիա»: Այն նպատակ ունի բացահայտելու, կանխելու և նվազեցնելու վնասակար թվային հաղորդակցությունը՝ անօրինական դարձնելով թվային հաղորդակցության հրապարակումը՝ մեկ ուրիշին հուզական լուրջ անհանգստություն պատճառելու նպատակով և սահմանում է հաղորդակցման 10 սկզբունքներ: Այն հնարավորություն է տալիս օգտատերերին բողոքել անկախ կազմակերպությանը, եթե այդ սկզբունքները խախտվեն, կամ եթե խնդիրը չլուծվի, հայց ներկայացնել դատարան՝ հեղինակի կամ հաղորդակցության պատասխանատուի դեմ:

Էլեկտրոնային Անվտանգության (eSafety) հանձնակատար, Ավստրալիա

Ավստրալիայի Էլեկտրոնային Անվտանգության հանձնակատարը, որը հիմնադրվել է 2015 թվականին, աշխարհում առաջին պետական գործակալությունն է, որը նվիրված է առցանց չարաշահումների դեմ պայքարին և իր քաղաքացիներին՝ առցանց տիրույթում անվտանգ

պահելուն: Որպես առցանց անվտանգության անկախ ազգային կարգավորող՝ Էլեկտրոնային Անվտանգության հանձնակատարն ունի գործառույթների հզոր համադրություն: Դրանք տատանվում են՝ կանխարգելումից մինչև իրազեկման բարձրացում, կրթություն, հետազոտություն և խորհուրդներ լավագույն փորձի վերաբերյալ, վաղ միջամտություն և վնասի փոխհատուցում՝ բազմաթիվ կանոնադրական կարգավորող ռեժիմների միջոցով, որոնք Էլեկտրոնային Անվտանգության հանձնակատարին հնարավորություն են տալիս արագորեն հեռացնել կիբերհարձակումը, պատկերի վրա հիմնված չարաշահումը և անօրինական առցանց բովանդակությունը: Այս լայն առաքելությունը Էլեկտրոնային Անվտանգության հանձնակատարը հնարավորություն է տալիս բազմակողմանի, ամբողջական և ակտիվ կերպով մոտենալ առցանց անվտանգությանը:

2018 թվականին Էլեկտրոնային Անվտանգության հանձնակատարը մշակել է Անվտանգությունը Դիզայնով (SbD) նախաձեռնությունը, որն անվտանգությունն ու օգտատերերի իրավունքները դնում է առցանց ապրանքների և ծառայությունների նախագծման, մշակման և տեղակայման կենտրոնում: Նախաձեռնության հիմքում ընկած է անվտանգության նախագծման սկզբունքների մի շարք, որոնք սահմանում են իրատեսական, գործող և հասանելի քայլեր, որոնք պետք է ձեռնարկվեն ոլորտում՝ քաղաքացիներին առցանց տիրույթում ավելի լավ պահպանելու և պաշտպանելու համար: Երեք ընդհանուր սկզբունքներն են.

1. **Ծառայություններ մատուցողի պարտականությունները**. անվտանգության բեռը երբեք չպետք է ընկնի միայն վերջնական օգտագործողի վրա: Կարելի է կանխարգելիչ քայլեր ձեռնարկել՝ ապահովելու համար, որ առցանց ծառայության նախագծման և տրամադրման ժամանակ գնահատվեն հայտնի և ակնկալվող վնասները, ինչպես նաև կանխարգելվի անօրինական և ոչ պատշաճ վարքագիծը:
2. **Օգտագործողների հզորացում և ինքնավարություն.** օգտատերերի արժանապատվությունը և նրանց լավագույն շահերն առանցքային նշանակություն ունեն: Մարդկային գործոնը և ինքնավարությունը պետք է աջակցություն ստանան, ուժեղացվեն և ամրապնդվեն ծառայությունների նախագծման մեջ՝ թույլ տալով օգտվողներին ավելի շատ վերահսկել, կառավարել և կարգավորել իրենց փորձը:
3. **Թափանցիկություն և հաշվետվողականություն.** սրանք անվտանգության ոլորտում հետևողական մոտեցմանը բնորոշ նշաններ են, որոնք ապահովում են երաշխիքներ, որ ծառայությունները գործում են իրենց հրապարակած անվտանգության նպատակներին համապատասխան, ինչպես նաև հանրությանը կրթելով և տեղեկացնելով այն քայլերի մասին, որոնք կարող են ձեռնարկվել՝ անվտանգության խնդիրները լուծելու համար:

Մենք Պաշտպանում ենք (We PROTECT) **գլոբալ դաշինք**

Մենք Պաշտպանում ենք գլոբալ դաշինքի ռազմավարության հիմքում ընկած է երկրներին աջակցելը՝ մշակելու համակարգված բազմաշահառու արձագանքներ երեխաների առցանց սեռական շահագործման դեմ պայքարելու համար՝ առաջնորդվելով նրա Ազգային արձագանքման մոդելով, որը գործում է որպես ազգային գործողությունների նախագիծ: Այն երկրներին տրամադրում է գործողությունների առցանց այնպիսի շրջանակ, որը պետք է օգտագործվի երեխաների սեռական շահագործման դեմ պայքարելու համար:

Մենք Պաշտպանում ենք գլոբալ դաշինքի ազգային արձագանքման մոդելի շրջանակներում ՏՀՏ ընկերությունների կողմից կան հստակ պարտավորություններ, որոնք վերաբերում են.

- ծանուցման և հեռացման ընթացակարգերին.
- զեկուցել երեխաների առցանց սեռական շահագործման և բռնության մասին (ԵՍԾԲ)
- մշակել տեխնոլոգիական լուծումներ
- ներդրումներ կատարել երեխաների առցանց պաշտպանության արդյունավետ կանխարգելիչ ծրագրերում և արձագանքման ծառայություններում:

Գլոբալ գործընկերություն և երեխաների հանդեպ բռնությանը վերջ տալու հիմնադրամ (Global Partnership and Fund to End Violence against Children)

Գլոբալ գործընկերություն և երեխաների նկատմամբ բռնությանը վերջ դնելու հիմադրամը մեկնարկել է ՄԱԿ-ի Գլխավոր քարտուղարի կողմից 2016թ.-ին Հիմադրամի նպատակը մեկն է՝ մշակել գործողությունների, քայլերի որոշակի փաթեթ և մինչև 2030 թվականը վերջ դնել երեխաների հանդեպ բռնության բոլոր ձևերին: Այս աշխատանքում ներառել, համագործակցել են տարբեր ոլորտներից ավելի քան 400 գործընկերների հետ:

Աշխատանքի գլխավոր ուղղություններն են. զոհերի փրկությունն ու աջակցությունը, վիրավորանքը հայտնաբերելու և կանխելու տեխնոլոգիական լուծումները, իրավապահ մարմինների աջակցությունը, օրենսդրական և քաղաքական բարեփոխումները, ինչպես նաև՝ առցանց ԵՍԾԲ-ի մասշտաբի և բնույթի վերաբերյալ տվյալների ու ապացույցների հավաքագրումը, երեխաների պաշտպանվածության մասին պատկերացում կազմելը:[19]

19 Հավելյալ տեղեկատվության համար տես «Վերջ երեխաների հանդեպ բռնությանը», "Grantees of the End Violence Fund".

3. Երեխաների իրավունքների պաշտպանության և խթանման հիմնական ոլորտները

Այս բաժինը նախանշում է հինգ հիմնական ոլորտներ, որտեղ ընկերությունները կարող են գործողություններ ձեռնարկել՝ պաշտպանելու երեխաների և երիտասարդների անվտանգությունը ՏՀՏ օգտագործելիս և խթանելու՝ ՏՀՏ-ի դրական կիրառումը:

3.1 Երեխաների իրավունքների ինտեգրում կորպորատիվ քաղաքականության և կառավարման բոլոր համապատասխան գործընթացներում

Երեխաների իրավունքների ինտեգրումը պահանջում է, որ ընկերությունները համապատասխան միջոցներ ձեռնարկեն՝ բացահայտելու, կանխելու, մեղմելու և, անհրաժեշտության դեպքում, վերացնելու հնարավոր և իրական բացասական ազդեցությունները երեխաների իրավունքների վրա: Միավորված ազգերի կազմակերպության՝ «Բիզնեսի և մարդու իրավունքների ուղեցույց»-ի սկզբունքները կոչ են անում բոլոր ձեռնարկություններին և ոլորտներին ձեռնարկել համապատասխան քաղաքականություն և գործընթացներ՝ մարդու իրավունքները հարգելու գործընթացին ուղղված:

Որպես խոցելի խմբի՝ ոլորտները պետք է հատուկ ուշադրություն դարձնեն երեխաներին և երիտասարդներին՝ նրանց տվյալների պաշտպանությանը և արտահայտվելու ազատությանը: Միավորված ազգերի կազմակերպության Գլխավոր ասամբլեայի 68/167 բանաձևը թվային դարաշրջանում գաղտնիության իրավունքի մասին՝ վերահաստատում է գաղտնիության և խոսքի ազատության իրավունքն՝ առանց անօրինական միջամտության: Ի հավելումն ՄԱԿ-ի՝ Մարդու իրավունքների խորհրդի 32/13 բանաձևը համացանցում մարդու իրավունքների խթանման և պաշտպանության մասին, ճանաչում է համացանցի գլոբալ և բաց բնույթը որպես շարժիչ ուժ՝ դեպի զարգացում առաջընթացն արագացնելու գործիք և հաստատում է, որ նույն իրավունքներն, ինչ մարդիկ ունեն անցանց կյանքում, պետք է ունենան և պաշտպանված լինեն նաև առցանց տիրույթում: Այն պետություններում, որտեղ բացակայում են երեխաների և երիտասարդների անձնական կյանքի և արտահայտվելու ազատության իրավունքների պաշտպանության համար համապատասխան իրավական շրջանակները, ընկերությունները պետք է հետևողական լինեն, ապահովեն, որ քաղաքականությունն ու գործելակերպը համահունչ լինեն միջազգային իրավունքին: Քանի որ երիտասարդների քաղաքացիական ներգրավվածությունը շարունակում է աճել առցանց հաղորդակցության միջոցով, ընկերությունները ավելի մեծ պատասխանատվություն ունեն հարգելու երեխաների և երիտասարդների

իրավունքները, նույնիսկ, եթե ներպետական օրենքները դեռ չեն համապատասխանում միջազգային չափանիշներին:

Ընկերությունները պետք է գործառնական մակարդակի բողոքարկման մեխանիզմ ունենան՝ խնդիրների հետ առնչված անձանց համար՝ հնարավոր խախտումների վերաբերյալ մտահոգությունները բարձրացնելու ձևաչափ տրամադրեն: Գործառնական մակարդակի մեխանիզմները պետք է հասանելի լինեն երեխաներին, նրանց ընտանիքներին և նրանց շահերը ներկայացնողներին: Բիզնեսի և մարդու իրավունքների ուղեցույցի 31-րդ սկզբունքը պարզաբանում է, որ նման մեխանիզմները պետք է լինեն օրինական, մատչելի, կանխատեսելի, արդարացի, թափանցիկ, իրավունքներին համապատասխան, շարունակական ուսուցման աղբյուր և հիմնված լինեն ներգրավվածության և երկխոսության վրա: Բացասական ազդեցությունները վերացնելու ներքին գործընթացների հետ մեկտեղ, բողոքարկման մեխանիզմները պետք է ապահովեն, որ ընկերություններն ունենան այնպիսի շրջանակներ, որոնք ապահովում են երեխաների և երիտասարդների համար համապատասխան միջոցներ, երբ նրանց իրավունքները վտանգված են:

Ընկերությունները ՏՀՏ անվտանգության հանդեպ ցուցաբերում են համապատասխանության վրա հիմնված մոտեցում, որը կենտրոնանում է ազգային օրենսդրության պահպանման վրա: Ազգային օրենսդրության բացակայության դեպքում՝ հետևելով միջազգային ուղեցույցներին և խուսափելով երեխաների և երիտասարդների իրավունքների վրա բացասական ազդեցություններից, ընկերությունները կամավոր գործողությունների միջոցով ակտիվորեն նպաստում են երեխաների և երիտասարդների զարգացմանը և բարեկեցությանը, որոնք ուղղված են երեխաների և երիտասարդների տեղեկատվության հասանելիության իրավունքին՝ խոսքի ազատությանը, մասնակցությանը, կրթությանը և մշակույթին:

Լավագույն փորձ. քաղաքականությանը և տարիքին համապատասխան նախագիծ

Հավելվածի մշակող Toca Boca ընկերությունը թվային խաղալիքներ է արտադրում՝ իր արտադրանքում արտացոլելով երեխաների հետաքրքրությունները, ցանկությունները: Ընկերության գաղտնիության քաղաքականության մեջ ներկայացնում է, թե ինչ տեղեկատվություն է հավաքում և ինչպես է այն օգտագործվում: TocaBoca-ն հանդիսանում է PRIVO Kids Privacy Assured COPPA Safe Harbor հավաստագրման ծրագրի անդամ:

LEGO® Life -ն անվտանգ սոցիալական մեդիա հարթակի օրինակ է 13 տարեկանից փոքր երեխաների համար՝ կիսվելու իրենց լեգո ստեղծագործություններով, ոգեշնչվելու և ապահով շփվելու համար:

Այստեղ հաշիվ ստեղծել հնարավոր է միայն ծնողի կամ խնամակալի էլեկտրոնային փոստի հասցեով: Այստեղ երեխաներից որևէ անձնական տեղեկատվություն չի պահանջվում: Հավելվածը հնարավորություն է տալիս երեխաներին և իրենց ընտանիքներին քննարկել առցանց անվտանգությունն ու գաղտնիությունը դրական միջավայրում:

Տարիքին համապատասխան նախագծերի օրինակները ներառում են որոշ խոշոր հանրային ծառայությունների հեռարձակողների հատուկ առաջարկներ՝ որոշակի տարիքային խմբերի համար: Օրինակ՝ գերմանական ARD-ն (Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland – Das Erste) և ZDF (Zweites) Deutsches Fernsehen-ը՝ 14 տարեկանից սկսած, առաջարկում է հարմարեցված բովանդակություն՝ funk.net՝ առցանց ալիքի միջոցով: Բի-Բի-Սի-ն (British Broadcasting Corporation) թողարկել է CBeebies-ը, որը նախատեսված է մինչև 6 տարեկան երեխաների համար: Կայքի բովանդակությունը հատուկ հարմարեցված է համապատասխան տարիքային խմբերի համար:

Լավագույն փորձ. քաղաքականություն և տեխնոլոգիա

Twitter-ը շարունակաբար ներդրումներ է կատարել սեփական տեխնոլոգիայի մեջ, ինչը նպաստել է մարդկանց կողմից բողոքներ ներկայացնելու բեռի կտրուկ նվազմանը:[20] Twitter-ը հետևողական մոտեցում է ցուցաբերում և բողոքների ավելի քան 50 տոկոսը, 2018-ի 20 տոկոսի հետ համեմատած, ներկայումս ակտիվորեն հայտնաբերբում են տեխնոլոգիայի միջոցով: Նոր տեխնոլոգիան օգտագործվում է անձնական տեղեկատվության, զգայուն մեդիայի, ատելությամբ լցված վարքագծի, չարաշահման խնդիրների դեպքերում:

20 Twitter, "15th Transparency Report: Increase in proactive enforcement on accounts".

3.2 ԵՍԸՆ-ի հետ աշխատանքի համար ստանդարտ գործընթացների մշակում

2019 թվականին IWF-ն հայտնաբերել է 132,676 վեբ էջ, որոնք հաստատվել են որպես երեխաների հանդեպ սեռական բռնություն պարունակող:[21] Ցանկացած ՄՌՈ (URL) կարող է պարունակել հարյուրավոր, եթե ոչ հազարավոր նկարներ և տեսանյութեր: IWF-ի կողմից հայտնաբերված նկարներից 45 տոկոսում ներկայացված են եղել 10 տարեկան և ավելի փոքր երեխաներ, և 1609 ինտերնետային էջերը ներկայացնում էին 0-2 տարեկան երեխաների, որոնց 71 տոկոսը պարունակում էր ամենածանր սեռական բռնություններ, ինչպիսիք են՝ բռնաբարությունները և սեռական խոշտանգումները: Այս մտահոգիչ փաստերն ընդգծում են ոլորտի, կառավարությունների, իրավապահ մարմինների և քաղաքացիական հասարակության միջև համագործակցության կարևորությունը՝ ԵՍԸՆ-ի դեմ պայքարելու համար:

Մինչ կառավարությունների մեծ մասը զբաղվում են ԵՍԸՆ-ի տարածման դեմ օրենսդրական ակտեր ընդունելով, հայտնաբերելով և հետապնդելով չարաշահողներին, բարձրացնելով իրազեկությունը և աջակցելով երեխաներին և երիտասարդներին՝ վերականգնվելու չարաշահման կամ շահագործման հետևանքներից, կան շատ երկրներ, որոնք դեռևս չունեն համապատասխան համակարգեր: Յուրաքանչյուր երկրի համար պահանջվում են մեխանիզմներ, որոնք հնարավորություն կտան լայն հանրությանն իրազեկել նման բնույթի վիրավորական և շահագործող բովանդակության մասին: Ոլորտը, իրավապահ մարմինները, կառավարությունները և քաղաքացիական հասարակությունը պետք է միասին աշխատեն՝ ապահովելու համար միջազգային չափանիշներին համապատասխան իրավական շրջանակների առկայությունը: Նման շրջանակները պետք է քրեականացնեն ԵՍԸԲ-ի բոլոր ձևերը, ներառյալ՝ ԵՍԸՆ-ն, և պաշտպանեն երեխաներին, ովքեր նման չարաշահման կամ շահագործման զոհ են դարձել: Այս շրջանակները պետք է ապահովեն բողոքների հետաքննության և բովանդակության հեռացման գործընթացները, հնարավորինս արդյունավետ կերպով աշխատելով:

Ոլորտը պետք է հղումներ տրամադրի ազգային թեժ գծերին կամ տեղական այլ հասանելի թեժ գծերի, ինչպիսիք են IWF-ի պորտալները որոշ երկրներում: Իսկ տեղական բողոքների ներկայացման մեխանիզմների բացակայության դեպքում հղումներ տրամադրի այլ միջազգային թեժ գծերի, ինչպիսին է Միացյալ Նահանգների անհայտ կորած և շահագործման ենթարկված երեխաների ազգային կենտրոնը (NCMEC) կամ Ինտերնետ Թեժ գծերի միջազգային ասոցիացիան (INHOPE), որտեղ միջազգային թեժ գծերից որևէ մեկը կարող է օգտագործվել հաշվետվություն ներկայացնելու համար:

21 IWF, "The why. The how. The who. And the results. Annual Report 2019".

Պատասխանատու ընկերությունները մի շարք քայլեր են ձեռնարկում, որոնք կօգնեն կանխել իրենց ցանցերով ու ծառայություններով ԵՍՇՄ-ի տարածմանը: Դրանք վարքագծի կանոնների մեջ[22] ներառում են հատուկ կետեր, որոնք բացահայտորեն արգելում են նման բովանդակությունը կամ վարքագիծը. ապահովում ծանուցման և հեռացման կայուն գործընթացների զարգացումը և սերտորեն համագործակցում տեղական ընկերությունների հետ:

Բացի այդ, որոշ ընկերություններ օգտագործում են տեխնիկական միջոցներ՝ կանխելու իրենց ծառայությունների կամ ցանցերի միջոցով ԵՍՇՆ-երով կիսվելը: Օրինակ, որոշ ինտերնետային ծառայությունների մատակարարներ արգելափակում են մուտքը համապատասխան մարմնի կողմից հաստատված ՄՌՈ-ներ (URL), որոնք հաստատված են որպես ԵՍՇՆ պարունակող: Եվ եթե վեբ կայքը տեղակայված է այնպիսի երկրում, որտեղ նման գործընթացներ չկան, չի ապահովվում դրանց արագ հեռացումը: Մյուսները կիրառում են հեշինգի տեխնոլոգիաներ՝ ավտոմատ կերպով հայտնաբերելու և հեռացնելու երեխաների սեռական բռնության նկարները, որոնք արդեն հայտնի են իրավապահներին կամ թեժ գծերին: Ոլորտի անդամները պետք է հաշվի առնեն և ներառեն բոլոր համապատասխան ծառայություններն իրենց գործունեության մեջ՝ կանխելու երեխաների հանդեպ սեռական բռնության տարածումը:

Լավագույն փորձ. տեխնոլոգիա

Մայքրոսոֆթը կիրառում է քառակողմ մոտեցում՝ խթանելու պատասխանատու և անվտանգ տեխնոլոգիաների օգտագործումը՝ կենտրոնանալով հենց տեխնոլոգիայի, ինքնակառավարման, գործընկերության, սպառողների կրթության և իրազեկման վրա: Մայքրոսոֆթը նաև ներդրել է գործառույթներ, որոնք օգնում են անհատներին ավելի արդյունավետ կերպով կառավարել իրենց առցանց անվտանգությունը: «Ընտանեկան անվտանգությունը» նման գործառույթներից մեկն է, որը թույլ է տալիս ծնողներին և խնամակալներին վերահսկել իրենց երեխաների համացանցից օգտելը:

Մայքրոսոֆթը կիրառում է քաղաքականություն իր հարթակներում ոտնձգությունների դեմ, և օգտատերերը, ովքեր չարաշահում են այս կանոնակարգերը, ենթակա են հաշվի դադարեցման կամ ավելի լուրջ խախտումների դեպքում՝ իրավապահ մարմինների կողմից միջամտության:

22 Հարկ է նշել, որ օգտվողների ոչ պատշաճ վարքագիծը չի սահմանափակվում միայն ԵՍՇՆ-ով, և որ ցանկացած տեսակի ոչ պատշաճ վարքագիծ կամ բովանդակություն պետք է համապատասխան արձագանք ստանա ընկերության կողմից:

Microsoft PhotoDNA-ն ստեղծում է նկարների հեշեր (կոդավորված արժեք) և դրանք համեմատում է արդեն իսկ հայտնաբերված և հաստատված ԵՍԲՆ հեշերի տվյալների բազայի հետ: Եթե դրանք համընկնում են, ապա պատկերն արգելափակվում է: Այս գործիքը հնարավորություն է տվել բովանդակության մատակարարներին համացանցից հեռացնել միլիոնավոր անօրինական լուսանկարներ. օգնել է դատապարտել երեխաների սեռական «գիշատիչներին», որոշ դեպքերում օգնել է իրավապահ մարմիններին փրկել պոտենցիալ զոհերին՝ նախքան նրանց ֆիզիկական վնաս պատճառելը:

Մայքրոսոֆթը պարտավորվել է պաշտպանել իր հաճախորդներին՝ իր արտադրանքի և ծառայությունների անօրինական բովանդակությունից, և ընկերության կողմից արդեն իսկ ստեղծված տեխնոլոգիայի կիրառումն՝ անօրինական տեսանյութերի այս աճի դեմ պայքարելու տրամաբանական հաջորդ քայլն էր: Սակայն, այս գործիքը չի օգտագործում դեմքի ճանաչման տեխնոլոգիա և չի կարող նույնականացնել նկարում պատկերված անձին կամ առարկան:

Այնուամենայնիվ, PhotoDNA for Video-ի հայտնագործմամբ ամեն ինչ նոր շրջադարձ է ստացել: PhotoDNA-ն for Video-ն բաժանում է տեսանյութն առանցքային շրջանակների և, ըստ էության, ստեղծում է հեշեր այդ էկրանի պատկերների (screenshot) համար: Նույն կերպ, ինչպես PhotoDNA-ը կարող է համընկնել այն նկարի հետ, որը փոփոխվել է՝ հայտնաբերումից խուսափելու համար, PhotoDNA for Video-ն կարող է գտնել երեխաների սեռական շահագործման բովանդակություն, որը խմբագրվել կամ միացվել է այլ տեսանյութի, որն այլ կերպ կարող է անվնաս թվալ:

Ավելին, Մայքրոսոֆթը վերջերս թողարկել է նոր գործիք՝ հայտնաբերելու համար հանցագործներին, ովքեր բռնության նպատակով սիրահետում են երեխաներին առցանց չաթերում: Project Artemis-ը, որը մշակվել է The Meet Group-ի, Roblox-ի, Kik-ի և Thorn-ի հետ համատեղ, հիմնված է Մայքրոսոֆթի արտոնագրված տեխնոլոգիայի վրա և Thorn-ի միջոցով անվճար հասանելի կլինի որակավորված առցանց ծառայություններ մատուցող ընկերություններին, որոնք առաջարկում են չաթի գործառույթ: Project Artemis-ը տեխնոլոգիական գործիք է, որն օգնում է բարձրացնել կարմիր դրոշ այն դեպքում, երբ կարիք է լինում ադմինիստրատորներին տեղյալ պահել չաթ սենյակներում չափավորություն պահելու և կարգ ու կանոն հաստատելու մասին: Գրումինգի հայտնաբերման այս տեխնիկայի միջոցով հնարավոր կլինի բացահայտել և տեղեկացնել «գիշատիչների» մասին, ովքեր փորձում են գայթակղել երեխաներին սեռական նպատակներով:

IWF-ն մի շարք ծառայություններ է տրամադրում ոլորտի անդամներին՝ պաշտպանելու իրենց օգտատերերին ԵՍՇՆ-ի գայթակղությունից:

3.3 Ապահով և տարիքին համապատասխան առցանց միջավայրի ստեղծում

Կյանքում շատ քիչ բաներ կարելի է միշտ համարել բացարձակապես անվտանգ և ռիսկերից զերծ: Նույնիսկ այն քաղաքներում, որտեղ երթևեկությունը խիստ կանոնակարգված և խստորեն վերահսկվում է, դեռևս տեղի են ունենում պատահարներ: Նույն սկզբունքով կիբերտարածությունն առանց ռիսկերի չէ՝ հատկապես երեխաների և երիտասարդների համար: Երեխաներին և երիտասարդներին իրենց առցանց միջավայրում կարելի է համարել ընդունողներ, մասնակիցներ և դերակատարներ: Ռիսկերը, որոնց նրանք բախվում են, կարելի է դասակարգել չորս ուղղությունների.[23]

- *Անպատշաճ բովանդակություն* – Երեխաները և երիտասարդները այլ բան որոնելիս կարող են պատահել անպատշաճ և անօրինական բովանդակության՝ ակնթարթային հաղորդագրության մեջ, բլոգում կամ ֆայլեր փոխանակելիս՝ սեղմելով ենթադրաբար անվնաս հղումը: Նրանք կարող են նաև փնտրել և կիսվել անպատշաճ կամ տարիքին անհամապատասխան զգայուն նյութերով: Այն, ինչը համարվում է վնասակար բովանդակություն, երկրից երկիր տարբեր է: Օրինակները ներառում են բովանդակություն, որը խթանում է թմրամիջոցների չարաշահումը, ռասայական ատելությունը, ռիսկային վարքագիծը, ինքնասպանությունը, անորեքսիան կամ բռնությունը:
- *Անպատշաճ վարքագիծ* – Երեխաները և մեծահասակները կարող են օգտագործել համացանցը՝ այլ մարդկանց հետապնդելու կամ նույնիսկ շահագործելու համար: Երեխաները երբեմն կարող են տեղադրել վիրավորական մեկնաբանություններ կամ ոչ պատշաճ նկարներ, գողանալ բովանդակություն կամ խախտել հեղինակային իրավունքները:
- *Անպատշաճ շփում* – Եվ մեծահասակները, և՛ երիտասարդները կարող են օգտվել համացանցից՝ փնտրելու երեխաների կամ երիտասարդների, ովքեր խոցելի են: Հաճախ նրանց նպատակն է համոզել թիրախին, որ նրանց միջև զարգացել են խորքային հարաբերություններ, սակայն հիմքում ընկած նպատակը մանիպուլյատիվ է: Նրանք կարող են փորձել համոզել երեխային՝ առցանց սեռական կամ այլ վիրավորական գործողություններ անել՝ օգտագործելով վեբ-տեսախցիկ կամ ձայնագրող այլ սարք, կամ կփորձեն կազմակերպել անձնական հանդիպում և ֆիզիկական շփում: Այս գործընթացը հաճախ կոչվում է «գրումինգ»:
- *Առևտրային ռիսկեր* – Այս կատեգորիան վերաբերում է տվյալների գաղտնիության ռիսկերին՝ կապված երեխաների տվյալների հավաքագրման և օգտագործման, ինչպես նաև թվային մարքեթինգի հետ:

---

23 Sonia Livingstone et al., "EU Kids Online: Final Report", Լոնդոնի տնտեսագիտության դպրոց, 2009.

Առցանց անվտանգությունը համայնքի մարտահրավեր է, հնարավորություն ոլորտի, կառավարությունների և քաղաքացիական հասարակության համար՝ համատեղ աշխատելու և անվտանգության սկզբունքներն ու գործելակերպը հաստատելու համար: Ոլորտը կարող է առաջարկել մի շարք տեխնիկական մոտեցումներ, գործիքներ և ծառայություններ ծնողների, երեխաների և երիտասարդների համար և նախ և առաջ պետք է ստեղծի այնպիսի արտադրանք, որը հեշտ է օգտագործել, անվտանգ է դիզայնով և օգտագործողների լայն շրջանակի համար համապատասխան տարիքին: Լրացուցիչ մոտեցումները ներառում են գործիքներ՝ մշակելու համապատասխան տարիքային ստուգման համակարգեր, որոնք հարգում են երեխաների գաղտնիության իրավունքները և մուտքի իրավունքը, կամ՝ սահմանափակումներ են դնում երեխաների և երիտասարդների՝ տարիքին անհամապատասխան բովանդակության հասանելիության վրա, կամ սահմանափակում են այն մարդկանց, ում հետ երեխաները կարող են շփվել կամ այն ժամանակահատվածը, որ նրանք կարող են անցկացնել առցանց:[24] Ամենակարևորը, «անվտանգությունն ըստ դիզայնի» շրջանակները, ներառյալ գաղտնիությունը, պետք է ներառվեն նորարարության և արտադրանքի նախագծման գործընթացներում: Երեխաների անվտանգությունը և տեխնոլոգիաների պատասխանատու օգտագործումը պետք է ուշադիր դիտարկվեն և չթողնել հետագային:

Որոշ ծրագրեր ծնողներին թույլ են տալիս վերահսկել տեքստերը և այլ հաղորդակցությունները, որոնք ուղարկում և ստանում են իրենց երեխաները, երիտասարդները: Եթե պետք է օգտագործվեն այս տեսակի ծրագրեր, ապա կարևոր է, որ դա բաց քննարկվի երեխայի հետ, այլապես նման պահվածքը կարող է ընկալվել որպես «լրտեսություն» և կարող է խաթարել վստահությունը ընտանիքում:

Հստակ և թափանցիկ ահազանգման մեխանիզմները պետք է հասանելի լինեն այն օգտատերերի համար, ովքեր մտահոգություններ ունեն բովանդակության և վարքագծի վերաբերյալ: Ավելին՝ բողոքին անհրաժեշտ է հետևել պատշաճ կերպով՝ դրա կարգավիճակի վերաբերյալ ժամանակին տեղեկատվության տրամադրմամբ: Թեև ընկերությունները կարող են յուրաքանչյուր դեպքի համար փոփոխել իրենց հետևողականության մեխանիզմները, կարևոր է հստակ ժամանակացույց սահմանել պատասխանների համար, հաղորդել բողոքի վերաբերյալ կայացված որոշումը և առաջարկել մեթոդ՝ հետևելու, եթե օգտագործողին պատասխանը չի բավարարում:

24 eSafety Commissioner, Safety by Design Overview, 2019.

Լավագույն փորձ. զեկուցում

Ֆեյսբուքը, փորձելով զսպել սեռական ոտնձգությունները թվային հարթակներում, Եվրոպական միության հետ համաֆինանսավորել է «Project deSHAME»-ը, որը համագործակցում է Childnet-ի, Save the Children-ի, Kek Vonal-ի և UCLan-ի հետ: Այս նախագիծը նպատակ ունի մեծացնել անչափահասների շրջանում առցանց սեռական ոտնձգությունների մասին բողոքներ ներկայացնելու մշակույթը և բարելավելու բազմոլորտ համագործակցությունը՝ կանխելու և արձագանքելու այս վարքագծին:

Քանի որ նախագծի հիմնական նպատակն է խրախուսել օգտատերերին բողոք ներկայացնել անհանգստացնող կամ անպատշաճ բովանդակության մասին, *ֆեյսբուքի Համայնքային ստանդարտները նույնպես* համապատասխան ուղեցույցներ են այն մասին, թե ինչն է թույլատրվում և ինչը չի թույլատրվում Ֆեյսբուքում:

Ֆեյսբուքը նաև ստեղծել է անվտանգության առանձնահատկություններ, ինչպիսիք են՝ «Ճանաչու՞մ եք այս անձին» առանձնահատկությունը, «այլ» փոստարկղի հնարավորությունը, որում տեղափոխվում են նոր հաղորդագրությունները այն մարդկանցից, որոնց օգտատերը չի ճանաչում, «հայտնվող պատուհան»-ը, որը հայտնվում է լրահոսում, եթե թվում է, թե անչափահասի հետ կապվում է մեծահասակը, որին նրանք չեն ճանաչում:

Առցանց բովանդակություն և ծառայություններ մատուցողները կարող են նաև նկարագրել իրենց կողմից տրամադրվող բովանդակության կամ ծառայությունների բնույթը և նպատակային տարիքային շրջանակը: Այս նկարագրությունները պետք է համապատասխանեցվեն նախկինում գոյություն ունեցող ազգային և միջազգային ստանդարտներին, համապատասխան կանոնակարգերին և երեխաներին տրամադրվող՝ մարքեթինգի և գովազդի վերաբերյալ խորհրդատվությանը, որոնք հասանելի են համապատասխան դասակարգման մարմինների կողմից:

Այս գործընթացն ավելի դժվար է դառնում ինտերակտիվ ծառայությունների աճող շրջանակի հետ, որոնք հնարավորություն են տալիս հրապարակել օգտվողների կողմից ստեղծված բովանդակությունն, օրինակ՝ հաղորդագրությունների տախտակների, զրուցարանների և սոցիալական ցանցերի ծառայությունների միջոցով: Երբ ընկերությունները հատուկ թիրախավորում են երեխաներին և երիտասարդներին, և երբ ծառայությունները ճնշող մեծամասնությամբ ուղղված են դեպի երիտասարդ լսարանները, օգտագործողի համար հարմար, հեշտ հասկանալի և մատչելի պայմանները և անվտանգության ակնկալիքները շատ ավելի մեծ են:

Ընկերություններին նաև խորհուրդ է տրվում պահպանել գաղտնիության ամենաբարձր չափանիշները, երբ խոսքը վերաբերում է երեխաների և երիտասարդների վերաբերյալ տվյալների հավաքագրմանը, մշակմանը և պահպանմանը, քանի որ երեխաները և

երիտասարդները կարող են չունենալ հասունություն՝ գնահատելու իրենց անձնական տվյալներով առցանց կիսվելու հետևանքները: Ծառայությունները, որոնք ուղղված են կամ կարող են ներգրավել երեխաների և երիտասարդների հիմնական լսարանին սպասարկելու գործում, պետք է հաշվի առնեն անձնական տեղեկատվության (ներառյալ գտնվելու վայրի մասին) հավաքման և օգտագործման հետևանքով նրանց սպառնացող ռիսկերը և ապահովեն, որ այդ ռիսկերը պատշաճ կերպով կանխվեն, և օգտագործողները տեղեկացված լինեն այդ մասին: Մասնավորապես, ընկերությունները պետք է ապահովեն ցանկացած նյութի, հաղորդակցության ձևի լեզուն և ոճը, որն օգտագործվում է ծառայությունները խթանելու, ծառայություններին հասանելիություն տրամադրելու համար, կամ որոնց միջոցով ունենում են հասանելիություն անձնական տեղեկատվությանը, հավաքում և օգտագործում դրանք, օգնի օգտատերերին հասկանալ և կառավարել իրենց գաղտնիությունը պարզ և հեշտ կերպով՝ մատչելի լեզվով բացատրելով, թե ինչին են նրանք համաձայնություն տալիս:

Լավագույն փորձ. նորարարություն

2018-2019 թվականներին ՅՈՒՆԻՍԵՖ-ի Արևելյան Ասիայի և Խաղաղօվկիանոսյան տարածաշրջանային գրասենյակը կազմակերպեց հինգ բազմաշահառու կլոր սեղաններ՝ փոխանակելու ոլորտի խոստումնալից փորձառությունները՝ առցանց ԵՍՇԲ-ի հասցեին: Կլոր սեղաններին մասնակցում էին մասնավոր հատվածի առաջատար ընկերություններ, ինչպիսիք են Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Մոնղոլիա), Mobifone+ (Վիետնամ), Globe Telecom (Ֆիլիպիններ), True (Թաիլանդ), GSMA և քաղաքացիական հասարակության գործընկերներ, այդ թվում՝ INHOPE, ECPAT International և Child Helpline International:

Որպես նույն ծրագրի մաս՝ 2020 թվականի փետրվարին ՅՈՒՆԻՍԵՖ-ը գործարկեց «ուղեղային կենտրոն» (Think Tank)՝ Արևելյան Ասիայի և Խաղաղ օվկիանոսի տարածաշրջանում ոլորտը հզորացնելու՝ առցանց աշխարհում երեխաների նկատմամբ բռնությունը կանխելու նպատակով: «Ուղեղային կենտրոն»-ը գաղափարների և նորարարության ինկուբատոր է, որը հիմնված է ոլորտի դերակատարների եզակի հեռանկարի վրա (ապրանքի ստեղծում, շուկայավարում և այլն)՝ ազդեցիկ կրթական նյութերի մշակման և ամենաարդյունավետ մատուցման հարթակների բացահայտման, ինչպես նաև՝ երեխաներին ուղղված այս կրթական նյութերի և հաղորդագրությունների ազդեցությունը չափելու համար գնահատման շրջանակի ստեղծմանը: «Ուղեղային կենտրոն»-ի մասնակից ընկերություններն են Ֆեյսբուքը (Facebook), Տելենորը (Telenor), ակադեմիական փորձագետներ, ՄԱԿ-ի գործակալություններ, ինչպիսիք են ՀՄՄ-ն, ՅՈՒՆԵՍԿՕ-ն և Միավորված ազգերի կազմակերպության թմրամիջոցների և հանցավորության դեմ պայքարի գրասենյակը՝ (UNODC)-ն, և այլք, ինչպիսիք են Ավստրալիայի Էլեկտրոնային

անվտանգության հանձնակատարը, ECPAT միջազգայինը, «Անհայտ կորած և շահագործման ենթարկված երեխաների միջազգային կենտրոն»-ը՝ (ICMEC)-ը, Ինտերպոլը և «Վերջ բռնությանը» համաշխարհային հիմնադրամը: «Ուղեղային կենտրոն»-ի անդրանիկ հանդիպումը, որը տեղի ունեցավ Հարավարևելյան Ասիայի երկրների ասոցիացիայի (ASEAN) երեխաների առցանց պաշտպանության տարածաշրջանային կոնֆերանսին զուգահեռ, իր շրջանակներում հավաքեց փորձագետներին՝ ներառյալ Մայքրոսոֆթի փորձագետներին: Նպատակը՝ ուսումնասիրելու տեխնոլոգիան և հետազոտական հնարավորությունները՝ առցանց վարքագծի փոփոխություններին ավելի լավ հետևելու համար՝ հիմնված առցանց անվտանգության նյութերի և հաղորդագրությունների ընդունման վրա:

3.4 Կրթել երեխաներին, խնամակալներին և դաստիարակներին՝ երեխաների անվտանգության և ՏՀՏ-ների պատասխանատու օգտագործման թեմայով

Տեխնիկական միջոցառումները կարող են կարևոր բաղադրիչ լինել՝ ապահովելու, որ երեխաները և երիտասարդներն առցանց պաշտպանված լինեն պոտենցիալ ռիսկերից, սակայն դրանք գործընթացի միայն մեկ տարրն են: Ծնողական վերահսկողության գործիքները, իրազեկության բարձրացումը և կրթությունը նույնպես հիմնական բաղադրիչներն են, որոնք կօգնեն հզորացնել և տեղեկացնել բոլոր տարիքի երեխաներին և երիտասարդներին, ինչպես նաև ծնողներին, խնամակալներին և մանկավարժներին: Թեև ընկերությունները կարևոր դեր ունեն երեխաներին և երիտասարդներին խրախուսելու ՏՀՏ-ները պատասխանատու և անվտանգ ձևով օգտագործելու հարցում, այս պատասխանատվությունը կիսում են ծնողների, դպրոցների, երեխաների և երիտասարդների հետ:

Շատ ընկերություններ ներդրումներ են կատարում կրթական ծրագրերում, որոնք նախատեսված են օգտատերերին բովանդակության և ծառայությունների վերաբերյալ տեղեկացված որոշումներ կայացնելու հնարավորություն տալու համար: Ընկերություններն օգնում են ծնողներին, խնամակալներին և մանկավարժներին՝ երեխաներին և երիտասարդներին առաջնորդելու դեպի ավելի անվտանգ, պատասխանատու և համապատասխան առցանց և բջջային հեռախոսների փորձառություններ: Սա ներառում է տարիքային զգայուն բովանդակության վերաբերյալ նշաններ փակցնելուն և ապահովելուն, որ ապրանքների մասին տեղեկությունները՝ ինչպիսիք են բովանդակության գները, բաժանորդագրության պայմանները և բաժանորդագրությունները չեղարկելու եղանակները, հստակորեն ներկայացված լինեն: Բոլոր երկրներում նվազագույն տարիքային պահանջների պահպանումը սոցիալական

մեդիայի կողմից, որտեղ հնարավոր է նաև տարիքի ստուգում, կօգնի նաև պաշտպանել երեխաներին՝ համապատասխան տարիքում թույլ տալով նրանց օգտվել ծառայություններից:

Կարևոր է նաև երեխաներին և երիտասարդներին ուղղակիորեն տեղեկատվություն տրամադրել ՏՀՏ-ի ավելի անվտանգ օգտագործման, դրական ու պատասխանատու վարքագծի վերաբերյալ: Անվտանգության մասին իրազեկվածության բարձրացումից բացի՝ ընկերությունները կարող են նպաստել դրական փորձին՝ երեխաների և երիտասարդների համար մշակելով բովանդակություն՝ հարգալից, բարի և բաց մտքով ՏՀՏ-ներ օգտագործելու վերաբերյալ: Նրանք կարող են տեղեկատվություն տրամադրել այն գործողությունների մասին, որոնք պետք է ձեռնարկեն, եթե նրանք ունեն բացասական փորձ, ինչպիսիք են առցանց ահաբեկումը կամ գրումինգը, ինչը հեշտացնում է նման միջադեպերի մասին բողոք ներկայացնելը և տրամադրում է անանուն հաղորդագրություններ ստանալուց հրաժարվելու գործառույթ:

Ծնողները երբեմն համացանցի և շարժական սարքերից ավելի քիչ են հասկանում և ավելի քիչ գիտեն, քան երեխաները և երիտասարդները: Ավելին, շարժական սարքերի և համացանցային ծառայությունների սերտաճումը դժվարացնում է ծնողական վերահսկողությունը: Ոլորտը կարող է համագործակցել կառավարության և մանկավարժների հետ՝ ամրապնդելու ծնողների կարողությունները՝ աջակցելու իրենց երեխաներին թվային ճկունություն ձեռք բերելու և որպես թվային պատասխանատու քաղաքացիներ գործելու համար: Նպատակը երեխաների և երիտասարդների՝ ՏՀՏ-ի օգտագործման պատասխանատվությունը միայն ծնողներին փոխանցելը չէ, այլ ավելի շուտ գիտակցելն է, որ ծնողներն ավելի լավ են հասկանում, թե ինչն է հարմար իրենց երեխաներին, և որ նրանք պետք է տեղյակ լինեն բոլոր ռիսկերի մասին՝ իրենց երեխաներին ավելի լավ պաշտպանելու և աջակցելու համար:

Տեղեկատվությունը կարող է փոխանցվել առցանց և անցանց բազմաթիվ մեդիաներով՝ հաշվի առնելով, որ որոշ ծնողներ չեն օգտվում համացանցային ծառայություններից: Կարևոր է համագործակցել դպրոցական համայնքների հետ՝ երեխաների և երիտասարդների համար առցանց անվտանգության և ՏՀՏ-ի պատասխանատու օգտագործման վերաբերյալ ուսումնական ծրագրեր, ծնողների համար կրթական նյութեր տրամադրելու համար: Օրինակները ներառում են մոնիտորինգի համար ծառայությունների մատչելի տեսակների, տարբերակների բացատրությունը, գործողությունները, որոնք պետք է ձեռնարկվեն, եթե երեխան ենթարկվում է առցանց ահաբեկման կամ գրումինգի: Ինչպես խուսափել անցանկալի նամակներից և կառավարել գաղտնիության կարգավորումները, ինչպես խոսել տարբեր տարիքային խմբերի տղաների և աղջիկների հետ զգայուն թեմաների շուրջ:

Հաղորդակցությունը երկկողմանի գործընթաց է, և շատ ընկերություններ հաճախորդներին հնարավորություն են տալիս կապ հաստատել իրենց հետ՝ խնդիրների մասին տեղեկացնելու կամ մտահոգությունները քննարկելու համար:

Քանի որ բովանդակությունն ու ծառայություններն ավելի ու ավելի են հարստանում, բոլոր օգտատերերը պետք է օգտվեն որոշակի ծառայության բնույթի և այն ապահով վայելելու վերաբերյալ խորհուրդներից և հիշեցումներից: Թեև կարևոր է երեխաներին սովորեցնել համացանցի պատասխանատու օգտագործման մասին, սակայն մենք գիտենք, որ երեխաները սիրում են փորձարկումներ անել, ռիսկի դիմել, իրենց էությամբ հետաքրքրասեր են և միշտ չէ, որ լավագույն որոշումներն են կայացնում: Նրանց հնարավորություն ենք տալիս դրսևորել իրենց ազատ կամքը, նպաստել նրանց աճին՝ զարգացնել ինքնավարություն և ճկունություն, քանի դեռ հակադարձումը չափազանց դաժան չէ: Թեև առցանց միջավայրում երեխաներին պետք է տրվի որոշակի ռիսկի դիմելու հնարավորություն, շատ կարևոր է, որ ծնողները և ընկերությունները կարողանան աջակցել նրանց, երբ ամեն ինչ սխալ է ընթանում, նվազեցնել բացասական ազդեցությունը և այն վերածել օգտակար դասի:

Լավագույն փորձ. կրթություն

Ճապոնիայի հեռարձակման կորպորացիան (NHK Japan) Թվիթերում երիտասարդների համար ինքնասպանությունների կանխարգելման արշավ է իրականացնում: Ճապոնիայում դեռահասների շրջանում ինքնասպանությունները հասնում են առավելագույնի: Իրավիճակը սրվում է, երբ ամառային արձակուրդից հետո նրանք վերադառնում են դպրոց: Ասում են՝ պատճառը վերադարձն է իրականություն: NHK Heart Net TV (NHK Japan) -ի պրոդյուսերական թիմը թողարկում է #Օգոստոսի 31-ի գիշերը անունով մուլտիմեդիա հաղորդում: Կապելով հեռուստատեսությունը, ուղիղ հեռարձակումը և սոցիալական մեդիաները՝ NKH-ն հաջողությամբ ստեղծեց մի «վայր», որտեղ դեռահասներն առանց վախի կարող էին կիսվել իրենց զգացմունքներով:

Լավագույն փորձ. կրթություն

Թվիթերը (Twitter) հրապարակել է նաև մանկավարժների համար մեդիա գրագիտության վերաբերյալ ուղեցույց: ՅՈՒՆԵՍԿՕ-ի հետ կազմված ձեռնարկը հիմնականում նպատակ ունի օգնել մանկավարժներին զինել երիտասարդ սերունդներին մեդիա գրագիտության հմտություններով: Թվիթերի անվտանգության աշխատանքի մեկ այլ ասպեկտը վերաբերում է նրանց տեղեկատվական գործողությունների բացահայտմանը: Սա պետության կողմից աջակցվող տեղեկատվական գործողությունների արխիվ է, որը Թվիթերը հրապարակայնորեն կիսում է: Նախաձեռնությունը մեկնարկել է ամբողջ աշխարհում այս խնդրին առնչվող արշավների

ակադեմիական և հանրային ըմբռնումն ուժեղացնելու և Թվիթերի հարթակում այս մարտավարությունների անկախ, երրորդ կողմի վերահսկման հնարավորություն տալու համար:

DeSHAME նախագիծը, որը համաֆինանսավորվում է Ֆեյսբուքի և Եվրոպական միության կողմից, նաև նպաստում է ռեսուրսների ստեղծմանը՝ տարիքային լայն խմբերի համար՝ հատուկ ուշադրություն դարձնելով 9-13 տարեկան երեխաներին: Որպես նախագծի մի մաս, որը կոչվում է «Քայլ արա, խոսիր» (Step Up, Speak Up!) մշակվել է գործիքակազմ՝ տրամադրելով մի շարք կրթական, վերապատրաստման և իրազեկման նյութեր, ինչպես նաև բազմոլորտային կանխարգելման և արձագանքման ռազմավարությունների գործնական գործիքներ: Ծրագրի շրջանակներում այս ուսումնական նյութերը կտեղափոխեն եվրոպական այլ երկրներ և, գործընկերների հետ համագործակցելով, կխթանեն երիտասարդների թվային իրավունքները:

Գուգլը (Google) մշակել է մի շարք կրթական նախաձեռնություններ, ռեսուրսներ և գործիքներ, որոնք կօգնեն խթանել առցանց անվտանգությունը երիտասարդների համար: Դրանցից մեկը թվային քաղաքացիության շուրջ Be Internet Awesome արշավն է, որը ստեղծվել է այնպիսի կազմակերպությունների հետ համագործակցությամբ, ինչպիսիք են՝ Միացիր Ապահովը (ConnectSafely), Ընտանիքի առցանց անվտանգության ինստիտուտը (Family Online Safety Institute) և Համացանցն անվտանգ պահիր կոալիցիան (Internet Keep Safe Coalition): Այս արշավը ուղղված է 8-11 տարեկան երիտասարդներին: Այն ներկայացնում է վեբի վրա հիմնված խաղ երիտասարդների համար (Interland), որը սովորեցնում է թվային անվտանգության հիմունքներ և ռեսուրսներ մանկավարժների համար, ինչպիսիք են թվային քաղաքացիությունը և անվտանգության ուսումնական ծրագիրը: Անվտանգության ուսումնական պլանն առաջարկում է դասապլաններ՝ քարոզարշավի հինգ հիմնական թեմատիկ ոլորտների համար, որոնցից մեկը կենտրոնանում է կիբերհարձակման վրա: Ի հավելումն սրա, Գուգլը ստեղծել է առցանց թվային քաղաքացիության և անվտանգության դասընթաց՝ բոլոր տարիքի ուսանողների, մանկավարժների համար՝ ապահովելով հետագա աջակցություն թվային քաղաքացիության և լսարանում անվտանգության առնչվող գործողությունների ինտեգրման համար: Գուգլն առաջարկում է նաև մի քանի ծրագրեր, որոնք կօգնեն երիտասարդներին ուղղակիորեն ներգրավվել առցանց անվտանգության և թվային քաղաքացիության աշխատանքներում: Համաշխարհային Վեբ Ռեյնջերս (Web Rangers) նախաձեռնությունը նման ծրագրերից մեկն է, որը երիտասարդներին սովորեցնում է առցանց անվտանգության կանոնները և խրախուսում է նրանց նախագծել իրենց սեփական արշավները համացանցի դրական և անվտանգ օգտագործման շուրջ: Ինչպես նաև կան տվյալ երկրին բնորոշ ծրագրեր երիտասարդների համար, օրինակ՝ Գուգլի կողմից գործարկված «Ինտերնետ քաղաքացիներ» և «Ինտերնետ լեգենդներ» ծրագրերը՝ Միացյալ Թագավորությունում:

Եվրատեսիլի երիտասարդական նորությունների կենտրոնում, Եվ-

րոպական հեռարձակողների միությունը հավաքում է 15 եվրոպական հեռուստատեսային հեռարձակողների՝ առցանց և անցանց ծրագրերով, ձևաչափերով և լուծումներով կիսվելու համար: Վերջին տարիներին թվային գրագիտության ուսուցումը և երեխաներին համացանցում ռիսկերի մասին զգուշացնելը դարձել են նրանց ծրագրերի առանցքային նշանակությունը: Վերջին տարիների ամենահաջող նախաձեռնություններից են սոցիալական մեդիայի գովազդը և երեխաների համար նախատեսված լրատվական հաղորդումները, որոնք արտադրվել են Super և Ultra nytt կողմից՝ Նորվեգիայի հանրային հեռարձակողի NRK-ի համար:

Լավագույն փորձ. ռազմավարական համագործակցություն
Ծրագրի մի մասն աջակցում է «Վերջ երեխաների նկատմամբ բռնությանը» հիմնադրամին: 2018 թվականին Capital Humano y Social Alternativo-ն սկսեց համագործակցությունը Telefónica-ի հետ՝ Պերուի ինտերնետ, կաբելային և հեռախոսային ծառայություններ մատուցող ամենամեծ մատակարարի, որն ունի 14,4 միլիոն հաճախորդ, այդ թվում՝ ավելի քան 8 միլիոնը Movistar-ի բջջային կապի օգտվողներ:

Այս արդյունավետ համագործակցության շրջանակներում իրականացվել են մի շարք աշխատանքներ.

- Telefónica-ի կողմից Capital Humano Social Alternativo-ի տեխնիկական աջակցությամբ մշակվել է **երեխաների առցանց պաշտպանության վերաբերյալ վիրտուալ դասընթաց:** Այս դասընթացն այժմ բաց և հասանելի է Telefónica-ի կայքում, և ընկերությունը հետևում է այն մարդկանց թվին, ովքեր գրանցվում և հաջողությամբ ավարտում են դասընթացը: Պերուի կրթության նախարարությունը համաձայնել է այս վիրտուալ դասընթացի հղումը տեղադրել իր պաշտոնական կայք էջում ևս:
- **Համացանցի անվտանգության մասին գրքույկ է** ստեղծվել Capital Humano y Social Alternativo-ի կողմից և տարածվել Telefónica-ի միջոցով՝ ավելի քան 300 բջջային կապի վաճառքի կենտրոններում: Նպատակն է բարձրացնել Telefónica-ի հաճախորդների իրազեկությունն՝ առցանց անվտանգության և առցանց ԵՍՇԲ-ի հետ կապված ռիսկերի վերաբերյալ:
- Telefónica-ի կողմից Capital Humano y Social Alternativo-ի տեխնիկական աջակցությամբ մշակվել է **ինտերակտիվ խաղ՝ առցանց ԵՍՇԲ-ից** խուսափելու վերաբերյալ, որը հաճախորդները կարող են խաղալ Telefónica-ի խանութներում՝ իրենց հերթին սպասելով:

Հիմնվելով Telefónica-ի հաջողության վրա՝ Capital Humano y Social Alternativo-ն համագործակցում է Econocable-ի՝ ինտերնետ և կաբելային ծառայությունների մատակարարի հետ, որն աշխատում է Պերուի հեռավոր և ցածր եկամուտ ունեցող վայրերում:

3.5 Թվային տեխնոլոգիաների խթանում՝ որպես քաղաքացիական ներգրավվածության բարձրացման եղանակ

Միավորված ազգերի կազմակերպության Երեխայի իրավունքների մասին կոնվենցիայի 13-րդ հոդվածը սահմանում է, որ «երեխան իրավունք ունի ունենալու արտահայտվելու ազատության. այս իրավունքը ներառում է ցանկացած տեսակի տեղեկատվություն և գաղափարներ փնտրելու, ստանալու և տարածելու ազատությունը՝ անկախ սահմաններից, բանավոր, գրավոր կամ տպագիր, արվեստի ձևով կամ երեխայի ընտրությամբ ցանկացած այլ միջոցներով»: Ընկերությունները կարող են կատարել երեխաների և երիտասարդների քաղաքացիական և քաղաքական իրավունքները հարգելու իրենց պարտականությունը՝ ապահովելով, որ տեխնոլոգիան և՛ երեխաներին, և՛ երիտասարդներին առցանց վնասից պաշտպանելու համար մշակված օրենսդրության և քաղաքականության կիրառումը չունենան անցանկալի հետևանքներ, չճնշեն նրանց մասնակցությունը և արտահայտվելու իրավունքը, նրանց բարօրության համար կարևոր տեղեկատվություն ստանալուն չխոչընդոտեն:[25] Կարևոր է երաշխավորել, որ տարիքային ստուգման համակարգերը չեն վտանգի որոշակի տարիքային խմբերի՝ իրենց զարգացման համար համապատասխան բովանդակություն մուտք գործելու իրական կարիքը:

Միևնույն ժամանակ, ձեռնարկությունները և ոլորտները կարող են նաև աջակցել երեխաների և երիտասարդների իրավունքներին՝ ապահովելով երիտասարդների մասնակցությունը հեշտացնելու մեխանիզմներ և գործիքներ: Նրանք կարող են ընդգծել համացանցի կարողությունը՝ նպաստելու քաղաքացիական կյանքում դրական ներգրավվածությանը, խթանելու սոցիալական առաջընթացը և ազդելու համայնքների կայունության և ճկունության վրա, օրինակ՝ մասնակցելով սոցիալական և բնապահպանական արշավներին: Ճիշտ գործիքների և տեղեկատվության առկայության դեպքում երեխաներն ու երիտասարդները ավելի լավ հնարավորություն ունեն օգտվելու առողջապահական խնամքի, կրթության և աշխատանքի հնարավորություններից, ինչպես նաև բարձրաձայնելու իրենց կարծիքներն ու կարիքները դպրոցներում, համայնքներում և երկրներում: Նրանք իրավունք են ստանում օգտվելու տեղեկատվություն փնտրելու իրենց իրավունքների և այն հարցերի մասին, որոնք ազդում են անձամբ իրենց վրա, օրինակ՝ իրենց սեռական առողջության, ինչպես նաև քաղաքական և կառավարության պատասխանատվության մասին:

Ընկերությունները կարող են նաև ներդրումներ կատարել երեխաների, երիտասարդների և ընտանիքների համար հարմար առցանց փորձառությունների ստեղծման գործում:

---

25 Երիտասարդների բջջային համայնքում մասնակցության վերաբերյալ տեղեկատվությունը տես այստեղ.

Նրանք կարող են աջակցել տեխնոլոգիայի և բովանդակության զարգացմանը, որը խրախուսում և հնարավորություն է տալիս երեխաներին և երիտասարդներին սովորել, նորարարություններ կատարել և ստեղծել լուծումներ: Նրանք միշտ պետք է հաշվի առնեն իրենց արտադրանքի դիզայնի անվտանգությունը:

Շատ երկրներում թվային և մեդիա գրագիտությունը, թվային անջրպետը փակելու ջանքերը վերջին տարիներին հանրային ծառայության ՀԼՄ-ների առաքելության մի մասն են եղել: Իտալիայի խորհրդարանը, օրինակ, առաջարկել է, որ ազգային հեռարձակողի առաջնահերթությունները ներառեն թվային անջրպետի փակումը և երեխաների պաշտպանության ապահովումն ինչպես անցանց, այնպես էլ առցանց, որին կարող են հետևել այլ երկրներ:

Լավագույն փորձ. բազմագերատեսչական համագործակցություն

Վերջերս Մայքրոսոֆթը միացավ Power of ZERO գլոբալ արշավին, որը գլխավորում է Նո Բուլի (No Bully) կազմակերպությունը, որի նպատակն է օգնել փոքր երեխաներին և նրանց մասին հոգ տանող մեծահասակներին,որ սովորեն լավագույնս օգտագործել թվային տեխնոլոգիաները և նպաստեն ներառականությանը, որը թվային քաղաքացիության սիրտն է: Նախաձեռնությունը փոքր տարիքի հետ աշխատող մանկավարժներին (արշավը դիտարկում է մինչև 8 տարեկան երեխաներին) և ընտանիքներին առաջարկում է անվճար ուսումնական նյութեր՝ օգնելու փոքր երեխաներին զարգացնել՝ «12 լավ հմտություններ» (12 powers for good) և վաղ տարիքից ամուր հիմքեր ստեղծել պատասխանատու թվային քաղաքացի լինելու համար:

4. Ոլորտի համար ընդհանուր ուղեցույցներ

Աղյուսակ 1-ում *ներկայացված են ոլորտի համար ուղեցույցներ՝ երեխաների և երիտասարդների իրավունքների վրա ապրանքների և ծառայությունների բացասական ազդեցությունը բացահայտելու, կանխելու և մեղմելու, ինչպես նաև երեխաների և երիտասարդների կողմից ՏՀՏ-ների դրական կիրառումը խթանելու համար:*

Նկատի ունեցեք, որ Աղյուսակ 1-ում թվարկված բոլոր քայլերը համապատասխան չեն բոլոր ընկերություններին և ծառայություններին, և ոչ էլ այս աղյուսակում ներկայացված են յուրաքանչյուր ծառայության համար անհրաժեշտ բոլոր քայլերը: Ոլորտի ընդհանուր ուղեցույցները լրացվում են դրանց առանձնահատկություններին հատուկ սփուգաթերթերով (տես բաժին 5) և՝ հակառակը: 2-5 աղյուսակների առանձնահատկությունների վրա հիմնված հատուկ սփուգաթերթերն ընդգծում են լրացուցիչ քայլերը, որոնք առավել համապատասխան են առանձին ծառայությունների համար: Նկատի ունեցեք, որ առանձնահատկություններին հատուկ սփուգաթերթերը կարող են համընկնել, և որ մեկից ավելի սփուգաթերթերը կարող են համապատասխան լինել նույն ծառայության համար:

Աղյուսակ 1. Ընդհանուր ուղեցույցներ ոլորտի համար

Ավելի անվտանգ և տարիքին համապատասխան առցանց միջավայրի ստեղծում (շարունակություն)	Մտածե՛ք այնպիսի մեխանիզմների տրամադրման մասին, ինչպիսիք են ծնողական վերահսկողության ծրագրային ապահովումը և այլ գործիքներ, որոնք հնարավորություն կտան ծնողներին, խնամակալներին կառավարել իրենց երեխաների մուտքն ինտերնետ ռեսուրսներ՝ միաժամանակ նրանց համապատասխան օգտագործման վերաբերյալ ուղեցույցներ տրամադրելով, որպեսզի երեխաների իրավունքները չոտնահարվեն: Դրանք ներառում են արգելափակման, թույլտվության ցուցակներ, բովանդակության զտիչներ, օգտագործման մոնիտորինգ, կոնտակտների կառավարում և ժամանակի ծրագրային սահմանափակումներ:
	Առաջարկե՛ք հեշտ օգտագործվող ծնողական հսկողության տարբերակներ, որոնք թույլ են տալիս ծնողներին և խնամակալներին սահմանափակել որոշ ծառայություններ, բովանդակություն, որտեղ երեխաները կարող են մուտք գործել էլեկտրոնային սարքեր օգտագործելիս: Այս սահմանափակումները կարող են ներառել ցանցի և սարքի ծրագրաշարի և հավելվածի կառավարում: Հաշվի առնելով, որ այն մեծ ազդեցություն է ունենում երեխաների ունակությունների վրա՝ զարգացնելու նրանց թվային հմտությունները և սահմանափակելով նրանց հնարավորությունները համացանցում, այդ վերահսկողության միջոցները պետք է մշակվեն շատ փոքր երեխաների համար՝ տվյալ տարիքային խմբի զարգացման համատեքստում, ծնողների համար համապատասխան ուղեցույցներ ներառելով:
	Հնարավորության դեպքում խթանե՛ք ազգային աջակցության ծառայությունները, որոնք ծնողներն ու խնամակալները կարող են օգտագործել խախտումների մասին հաղորդելու և չարաշահման կամ շահագործման դեպքում աջակցություն փնտրելու համար:

	Ներառե՛ք երեխաների առցանց անվտանգության հարցերի վերաբերյալ պատշաճ ուսումնասիրությունը մարդու իրավունքների կամ ռիսկերի գնահատման գործող շրջանակների մեջ (կորպորատիվ, արտադրանքի, տեխնոլոգիայի կամ երկրի մակարդակով): Որոշե՛ք, թե արդյոք բիզնեսը կամ ոլորտը իր գործունեության միջոցով կարող են առաջացնել կամ նպաստել բացասական ազդեցություններին, կամ արդյոք անբարենպաստ ազդեցությունները կարող են ուղղակիորեն վերագրվել նրա գործունեությանը, ապրանքներին, ծառայություններին կամ գործարար հարաբերություններին:
	Բացահայտե՛ք երեխաների իրավունքների ազդեցությունը տարբեր տարիքային խմբերի վրա՝ ընկերության գործունեության և ապրանքների և ծառայությունների նախագծման, մշակման և ներդրման արդյունքում, ինչպես նաև երեխաների և երիտասարդների իրավունքներին աջակցելու հնարավորությունների արդյունքում:

Երեխաների իրավունքների նկատառումների ինտեգրում կորպորատիվ քաղաքականության և կառավարման բոլոր համապատասխան գործընթացներում (շարունակություն)	Ընդունե՛ք երեխաների պաշտպանության հզորացման և կրթության վրա հիմնված մոտեցում: Հաշվի առեք երեխաների տվյալների պաշտպանության իրավունքները, նրանց գաղտնիության և խոսքի ազատության իրավունքը՝ միաժամանակ առաջարկելով կրթություն և առաջնորդություն ընկերության ծառայությունների միջոցով:
	Օգտագործե՛ք ներքին և արտաքին փորձաքննություն և խորհրդակցեք հիմնական շահագրգիռ կողմերի հետ, այդ թվում՝ երեխաների և երիտասարդների՝ առցանց անվտանգության մեխանիզմների, ընկերության մոտեցումների վերաբերյալ շարունակական կարծիք և ուղեցույց ստանալու համար:
	Այն պետություններում, որտեղ բացակայում են երեխաների և երիտասարդների գաղտնիության և արտահայտվելու ազատության իրավունքների պաշտպանության համապատասխան իրավական շրջանակները, ընկերությունները պետք է ապահովեն, որ քաղաքականությունն ու գործելակերպը համապատասխանեն միջազգային չափանիշներին: Տե՛ս Միավորված ազգերի կազմակերպության Գլխավոր ասամբլեայի 68/167 բանաձևը թվային դարաշրջանում գաղտնիության իրավունքի մասին:
	Ապահովե՛ք իրավական միջոցների հասանելիությունը՝ գործառնական մակարդակի բողոքարկման և զեկուցման մեխանիզմներ ստեղծելով երեխաների իրավունքների ցանկացած խախտման համար (օրինակ՝ ԵՍՇԲՆ, անպատշաճ բովանդակություն կամ շփում կամ գաղտնիության խախտում):

	Նշանակե՛ք երեխաների պաշտպանության քաղաքականության մենեջեր կամ այլ անձ, ում հետ կարելի է կապ հաստատել երեխաների առցանց անվտանգության հետ կապված խնդիրների համար: Եթե երեխային վտանգ է սպառնում, ապա երեխաների պաշտպանության քաղաքականության մենեջերը պետք է անհապաղ զգուշացնի համապատասխան մարմիններին: ԲիԲիՍԻ-ի խմբագրական ուղեցույցները (2019), օրինակ, սահմանում են երեխաների պաշտպանության քաղաքականության մենեջերի նշանակումը, որը պարտադիր է համարվում հանրային ծառայության ԶԼՄ-ներում:
Երեխաներին առցանց պաշտպանելու համար ոլորտի ստանդարտների մշակում	Ստեղծել և ներդնել ընկերություններում ստանդարտներ երեխաների և երիտասարդների պաշտպանության համար՝ կապված կոնկրետ ոլորտի և առանձնահատկությունների հետ:
ԵՍԾՆ-ի համար ստանդարտ գործընթացների մշակում	Համագործակցելով կառավարության, իրավապահ մարմինների, քաղաքացիական հասարակության և թեժ գծի կազմակերպությունների հետ՝ ոլորտը առանցքային դեր ունի ԵՍԾՆ-ի դեմ պայքարում՝ ձեռնարկելով հետևյալ գործողությունները.
	Արգելել վերբեռնումը, տեղադրումը, փոխանցումը, համօգտագործումը կամ հասանելի դարձնելը այնպիսի բովանդակության, որը խախտում է որևէ կողմի իրավունքները կամ խախտում է որևէ տեղական, պետական, ազգային կամ միջազգային իրավունք:

	Հենց պրովայդերները ստանան ԵՍԶՆ-ի մասին հաղորդում/բողոք, անհրաժեշտ է կապ հաստատել ազգային իրավապահ մարմինների կամ ազգային թեժ գծերի հետ՝ ԵՍԶՆ-ի մասին տեղեկատվությունը փոխանցելու համար: Համոզվել, որ առկա են ներքին ընթացակարգեր՝ տեղական և միջազգային օրենքների համաձայն խնդրի լուծմանն ուղղված պարտականություններին համապատասխանելու համար: Այն դեպքում, երբ ընկերությունը գործում է շուկաներում, որտեղ այս հարցում ավելի քիչ զարգացած կարգավորող և իրավապահ վերահսկողություն կա, այն կարող է ուղղորդել բողոքներ ներկայացնել ցանկացողներին Ինտերնետ Թեժ գծերի միջազգային ասոցիացիա (INHOPE), որտեղ բողոքները կարող են ներկայացվել ցանկացած միջազգային թեժ գծի:
ԵՍԶՆ-ի համար ստանդարտ գործընթացների մշակում (*շարունակություն*)	Ստեղծել ներքին ընթացակարգեր՝ ապահովելու ԵՍԶՆ-ի դեմ պայքարի վերաբերյալ տեղական և միջազգային օրենքների համապատասխանությունը: Ստեղծել բարձր պաշտոն կամ թիմ, որը նվիրված է այս ընթացակարգերը կազմակերպության մեջ ինտեգրելուն: Ոլորտի անդամներն այնուհետև պետք է զեկուցեն ձեռնարկված գործողությունների և այս թիմի կողմից ձեռք բերված արդյունքների մասին իրենց տարեկան կորպորատիվ և կայունության զեկույցում: Երբ ազգային կանոնակարգերը բավարար պաշտպանություն չեն ապահովում, ընկերությունները պետք է հարգեն, բայց գերազանցեն ազգային օրենսդրությունը և օգտագործեն իրենց լծակները՝ օրենսդրական փոփոխությունների լոբբինգ անելու համար, որպեսզի ոլորտը կարողանա պայքարել ԵՍԶՆ-ի դեմ:

	Կազմակերպությունում պետք է ստեղծվի նշանակվի պատասխանատու անձ կամ թիմ, որը նվիրված կլինի այս ընթացակարգերի ինտեգրմանը և գործողությունների մոնիտորինգին: Դրանք պետք է թափանցիկ կերպով արտացոլվեն կորպորատիվ և կայունության տարեկան հաշվետվություններում և հասանելի լինեն հանրությանը:
	Նշե՛ք, որ ձեռնարկությունը լիովին կհամագործակցի իրավապահ մարմինների հետաքննության հետ, եթե ապօրինի բովանդակություն հայտնվի կամ հայտնաբերվի, և նշեք այնպիսի տույժերի վերաբերյալ մանրամասներ, ինչպիսիք են տուգանքները կամ վճարման արտոնությունների չեղարկումը:
	Օգտագործե՛ք հաճախորդների համար ընդունելի պայմաններ կամ օգտագործման քաղաքականություն՝ հստակորեն նշելով ընկերության դիրքորոշումը ԵՍՇՆ-ն պահելու կամ համօգտագործելու համար իր ծառայությունների չարաշահման և ցանկացած չարաշահման հետևանքների վերաբերյալ:
	Մշակե՛ք ծանուցման, հեռացման և բողոք ներկայացնելու գործընթացներ, որոնք թույլ են տալիս օգտվողներին հաղորդել ԵՍՇՆ-ի կամ անպատշաճ կոնտակտի և կոնկրետ օգտատիրոջ հայտնաբերման վայրի մասին: Ստեղծե՛ք հաղորդումներ/բողոքներ ներկայացնելու հետագա գործընթացներ, համաձայնեցրեք ընթացակարգերը՝ ապացույցներ հավաքելու և անհապաղ հեռացնելու կամ արգելափակելու մուտքը դեպի ԵՍՇՆ: Համոզվե՛ք, որ, անհրաժեշտության դեպքում, ծառայություններ մատուցողները պահանջում են փորձագետների (օրինակ՝ երեխաների առցանց անվտանգության ազգային մարմինների) կարծիքը՝ նախքան անօրինական բովանդակությունը ոչնչացնելը:

	Համոզվե՛ք, որ համապատասխան երրորդ կողմերը, որոնց հետ ընկերությունը պայմանագրային հարաբերություններ ունի, նմանապես հաստատակամորեն ծանուցում և վերացնում են ԵՍՇՆ-ն:
	Պատրաստ եղե՛ք կարգավորել ԵՍՇՆ –ն և դեպքերի մասին հաղորդում/բողոք ներկայացնել համապատասխան մարմիններին: Եթե հարաբերությունները իրավապահ մարմինների և ազգային թեժ գծի հետ դեռևս հաստատված չեն, համագործակցեք նրանց հետ միասին գործընթացներ զարգացնելու համար:
	Աշխատե՛ք ներքին գործառույթների վրա, ինչպիսիք են հաճախորդների մասին հոգ տանելը, խարդախության կանխումը և անվտանգությունը, որպեսզի համոզվեք, որ ձեռնարկությունը կարող է կասկածելի անօրինական բովանդակության մասին տեղյակ պահել անմիջապես իրավապահ մարմիններին և թեժ գծերին:
ԵՍՇՆ-ի համար ստանդարտ գործընթացների մշակում (*շարունակություն*)	Ներառե՛ք տվյալների պահպանման քաղաքականությունը՝ քրեական հետախուզության դեպքում իրավապահներին աջակցելու համար այնպիսի գործողությունների միջոցով, ինչպիսին է ապացույցների հավաքագրումը: Փաստաթղթավորե՛ք ԵՍՇՆ-ի հետ աշխատող ընկերության փորձը՝ սկսած մոնիտորինգից և վերջացրած բովանդակության վերջնական փոխանցմամբ և ոչնչացմամբ: Ներառե՛ք այն անձնակազմի ցուցակը, որոնք պատասխանատու են փաստաթղթերում նշված բովանդակության հետ աշխատելու համար:

	Խթանե՛ք ԵՍԾՆ-ի մասին տեղեկություններ տալու մեխանիզմները և համոզվե՛ք, որ օգտատերերը գիտեն, թե ինչպես պետք է տեղեկացնել, եթե նրանք հայտնաբերեն նման բովանդակություն: Եթե առկա է ազգային թեժ գիծ, հղում արե՛ք այդ թեժ գծին՝ ձեր կորպորատիվ կայքից և ընկերության կողմից խրախուսվող համապատասխան բովանդակության ծառայություններից:
	Օգտագործե՛ք համապատասխան ծառայությունների տվյալները՝ կանխե՛ք նրանց ծառայություններում կամ հարթակներում՝ երեխաների նկատմամբ սեռական բռնության մասին բովանդակության տարածումը:
	Ակտիվորեն ուսումնասիրե՛ք ամբողջ բովանդակությունը, որը տեղակայված է ընկերության սերվերներում, վերահսկե՛ք նաև՝ առևտրային (բրենդավորված կամ երրորդ կողմ հանդիսացող մատակարարների կողմից կնքված պայմանագրով) կանոնավոր հիմունքներով գործընթացները: Նախատեսե՛ք օգտագործել այնպիսի գործիքներ, ինչպիսիք են երեխաների սեռական բռնության հայտնի նկարների հեշ սկանավորումը, նկարների ճանաչման ծրագրակազմը կամ URL-ի արգելափակումը ԵՍԾՆ-ը կարգավորելու համար:
Ավելի անվտանգ և տարիքին համապատասխան առցանց միջավայրի ստեղծում	Այս ոլորտը կարող է օգնել ստեղծել ավելի ապահով, ավելի հաճելի թվային միջավայր՝ բոլոր տարիքի երեխաների և երիտասարդների համար՝ ձեռնարկելով հետևյալ գործողությունները.
	Ներդրե՛ք անվտանգության և գաղտնիության սկզբունքներ ընկերության տեխնոլոգիաներում և ծառայություններում, առաջնահերթ ուշադրություն դարձրե՛ք այն որոշումներին, որոնք նվազագույնի են հասցնում երեխաներին վերաբերող տվյալների ծավալը:

	Իրականացրե՛ք տարիքին համապատասխան դիզայն, Ձեր կողմից առաջարկվող ծառայություններում: Ներկայացրե՛ք կայքի կանոնների վերաբերյալ երեխաներին հասանելի և տարիքին համապատասխան տեղեկատվություն համապատասխան ծավալի մանրամասներ տրամադրելով: Ի լրումն տարիքին համապատասխան և մատչելի պայմանների, ոլորտը պետք է հստակորեն փոխանցի այնպիսի տեղեկատվություն, ինչպիսիք են կանոնները և հիմնական քաղաքականությունները: Պետք է ընդգծվի ծառայության կողմից ընդունելի և անընդունելի վարքագիծը, որևէ կանոն խախտելու հետևանքները, ծառայության առանձնահատկությունները և այն, ինչին օգտատերը համաձայնում է գրանցվելու միջոցով: Նման տեղեկատվությունը պետք է հատկապես ուղղված լինի երիտասարդ օգտատերերին, նրանց ծնողներին և խնամակալներին:
	Օգտագործե՛ք ծառայությունների մատուցման պայմանները, որպեսզի օգտատերերի ուշադրությունը հրավիրեք ընկերության առցանց ծառայությունների բովանդակության վրա, որը չի կարող հարմար լինել բոլոր տարիքի մարդկանց համար: Կանոնները և պայմանները պետք է ներառեն նաև հստակ մեխանիզմներ ՝ նման կանոնների խախտումների մասին հաղորդելու և դրանց դեմ պայքարելու համար:

Ավելի անվտանգ և տարիքին համապատասխան առցանց միջավայրի ստեղծում (շարունակություն)	Մտածե՛ք այնպիսի մեխանիզմների տրամադրման մասին, ինչպիսիք են ծնողական վերահսկողության ծրագրային ապահովումը և այլ գործիքներ, որոնք հնարավորություն կտան ծնողներին, խնամակալներին կառավարել իրենց երեխաների մուտքն ինտերնետ ռեսուրսներ՝ միաժամանակ նրանց համապատասխան օգտագործման վերաբերյալ ուղեցույցներ տրամադրելով, որպեսզի երեխաների իրավունքները չոտնահարվեն: Դրանք ներառում են արգելափակման, թույլտվության ցուցակներ, բովանդակության զտիչներ, օգտագործման մոնիտորինգ, կոնտակտների կառավարում և ժամանակի ծրագրային սահմանափակումներ:
	Առաջարկե՛ք հեշտ օգտագործվող ծնողական հսկողության տարբերակներ, որոնք թույլ են տալիս ծնողներին և խնամակալներին սահմանափակել որոշ ծառայություններ, բովանդակություն, որտեղ երեխաները կարող են մուտք գործել էլեկտրոնային սարքեր օգտագործելիս: Այս սահմանափակումները կարող են ներառել ցանցի և սարքի ծրագրաշարի և հավելվածի կառավարում: Հաշվի առնելով, որ այն մեծ ազդեցություն է ունենում երեխաների ունակությունների վրա՝ զարգացնելու նրանց թվային հմտությունները և սահմանափակելով նրանց հնարավորությունները համացանցում, այդ վերահսկողության միջոցները պետք է մշակվեն շատ փոքր երեխաների համար՝ տվյալ տարիքային խմբի զարգացման համատեքստում, ծնողների համար համապատասխան ուղեցույցներ ներառելով:
	Հնարավորության դեպքում խթանե՛ք ազգային աջակցության ծառայությունները, որոնք ծնողներն ու խնամակալները կարող են օգտագործել խախտումների մասին հաղորդելու և չարաշահման կամ շահագործման դեպքում աջակցություն փնտրելու համար:

	Խուսափե՛ք առցանց վնասակար կամ անպատշաճ գովազդային բովանդակությունից: Ծառայություններ մատուցող կազմակերպությունների համար սահմանե՛ք օգտատերերի բացահայտման պարտավորություններ՝ այն բովանդակությամբ, որը վերաբերում է չափահաս լսարանին և կարող է վնասակար լինել երեխաների ու երիտասարդների համար: Վնասակար գովազդը կարող է ներառել նաև սննդամթերքի և խմիչքների գովազդ, որոնք հարուստ են ճարպերով, շաքարով կամ աղով: Համապատասխանեցրե՛ք բիզնես պրակտիկան՝ երեխաների և երիտասարդների համար նախատեսված մարքեթինգի և գովազդի կանոնակարգերին և խորհուրդներին: Ուսումնասիրե՛ք, թե որտեղ, երբ և ինչպես երեխաները և երիտասարդները կարող են հանդիպել շուկայի այլ հատվածի համար նախատեսված գովազդային վնասակար հաղորդագրությունների:
	Համոզվե՛ք, որ տվյալների հավաքագրման քաղաքականությունը համապատասխանում է երեխաների և երիտասարդների գաղտնիությանը վերաբերող համապատասխան օրենքներին: Հաշվի առե՛ք այն փաստը, որ պահանջվում է ծնողի համաձայնությունը՝ մինչև առևտրային ձեռնարկությունները կկարողանան երեխայի մասին անձնական տվյալներ հավաքել:

	Հարմարեցրե՛ք և կիրառե՛ք գաղտնիության բարձրացված լռելյայն կարգավորումները՝ 18 տարեկանից ցածր անձանցից հավաքված անձնական տվյալների հավաքագրման, մշակման, պահպանման, վաճառքի և հրապարակման համար՝ ներառյալ գտնվելու վայրի հետ կապված տեղեկություններն ու զննարկման սովորությունները: Գաղտնիության կանխադրված կարգավորումները և գաղտնիության կարևորության մասին տեղեկությունները պետք է համապատասխանեն օգտատերերի տարիքին և ծառայության բնույթին:
	Օգտագործե՛ք տեխնիկական միջոցներ, ինչպիսիք են ծնողական հսկողության համապատասխան գործիքները, դիզայնի անվտանգությունը, տարիքային տարբերվող փորձառությունները, գաղտնաբառով պաշտպանված բովանդակությունը, արգելափակման,թույլատրման ցուցակները, գնումների, ժամանակի վերահսկումը, անջատման գործառույթները, զտումը և մոդերացիան՝ կանխելու անչափահասների հասանելիությունն անպատշաճ բովանդակություն կամ ծառայություններ: Ներդրե՛ք տեխնոլոգիա, որը կարող է որոշել օգտատերերի տարիքը և ներկայացնել նրանց տարիքին համապատասխան հավելվածի տարբերակը: Ինչ վերաբերում է տարիքին համապատասխան բովանդակությանը կամ ծառայություններին, ապա ոլորտի շահագրգիռ կողմերը պետք է քայլեր ձեռնարկեն օգտատերերի տարիքը ստուգելու համար: Հնարավորության դեպքում օգտագործե՛ք տարիքային ստուգումը՝ սահմանափակելու բովանդակության կամ նյութի հասանելիությունը, որը օրենքով կամ քաղաքականության համաձայն նախատեսված է միայն որոշակի տարիքից բարձր անձանց համար: Ընկերությունները պետք է նաև գիտակցեն նման տեխնոլոգիաների չարաշահման հնարավորությունը՝ չսահմանափակեն երեխաների և

	երիտասարդների խոսքի ազատության, տեղեկատվության հասանելիության, գաղտնիությունը պահելու իրավունքը:
Ավելի անվտանգ և տարիքին համապատասխան առցանց միջավայրի ստեղծում (շարունակություն)	Համոզվե՛ք, որ բովանդակությունը և ծառայությունները, որոնք հարմար չեն բոլոր տարիքի օգտատերերի համար, հետևյալն են. • դասակարգված են ազգային չափանիշներին և մշակութային նորմերին համապատասխան • համարժեք լրատվամիջոցներում համապատասխանում են գոյություն ունեցող չափանիշներին • առաջարկվում է տարիքային ստուգում այնտեղ, որտեղ կա դրա անհրաժեշտությունը: Առկա են հստակ պայմաններ, որոնք վերաբերում են ստուգման գործընթացում ձեռք բերված, անձնապես ճանաչելի, տվյալների ոչնչացմանը: Օրինակ, ինչ վերաբերում է մեդիա ստանդարտներին, ապա բոլոր մեդիա կարգավորող մարմինները տարիքային բովանդակության համար մի շարք պահանջներ են ներկայացնում: Ինտերնետ պրովայդերներից պահանջվում է հարմարեցնել սերվերները և կիրառել ուղեցույցներն իրենց բովանդակությունը առաջարկելու համար: Նման փորձառության օրինակ է, Ofcom-ը՝ Միացյալ Թագավորությունում, CSA-ն՝ Ֆրանսիայում և AGCOM-ը՝ Իտալիայում:
	Առաջարկե՛ք տեղեկություններ հաղորդելու հստակ գործիքներ և մշակե՛ք գործունեության հետագա գործընթացը՝ կապված ոչ պատշաճ բովանդակության, կոնտակտների և չարաշահումների մասին հաղորդագրությունների հետ, ինչպես նաև՝ ծառայության օգտատերերին մանրամասն հետադարձ կապ տրամադրեք հաշվետու գործընթացի մասին:

	Ապահովե՛ք երեխաների և երիտասարդների համար նախատեսված ինտերակտիվ տարածքների նախնական մոդերացիան այնպես, որ այն համապատասխանի երեխաների գաղտնիության իրավունքներին, նրանց զարգացող ունակություններին: Ակտիվ մոդերացիան կարող է նպաստել այնպիսի մթնոլորտի ստեղծմանը, որտեղ ահաբեկումներն ու ոտնձգություններն անընդունելի են: Անընդունելի վարքագիծը ներառում է՝ • ինչ-որ մեկի պրոֆիլում տհաճ կամ սպառնալից մեկնաբանությունների տեղադրում, • կեղծ պրոֆիլների կամ ատելության կայքերի ստեղծում՝ զոհին նվաստացնելու նպատակով, • վնաս տալու մտադրությամբ շղթայական հաղորդագրությունների և հավելվածների ուղարկում, • ինչ-որ մեկի սոցիալական հարթակի էջի կոտրում ՝ այլ օգտատերերի վիրավորական հաղորդագրություններ ուղարկելու նպատակով:
	Հատուկ նախազգուշական միջոցներ ձեռնարկե՛ք անձնակազմի անդամների կամ համագործակցողների հետ, ովքեր աշխատում են երեխաների և երիտասարդների հետ: Նրանց համար ոստիկանության մարմիններում կարող է պահանջվել քրեական գործի նախնական ստուգում:
	Գործադիր ղեկավարության առցանց կամ ինտերակտիվ խմբին անհապաղ տեղեկացրե՛ք ցանկացած միջադեպի մասին, որը կապված է կանոնների խախտման կասկածների հետ: Նրանք են պատասխանատու այդ բովանդակության մասին համապատասխան մարմիններին հաղորդելու համար: • Հնարավորության դեպքում հաղորդե՛ք գրումինգի մասին գործադիր ղեկավար

	թիմին և երեխաների պաշտպանության քաղաքականության գծով առաջադրված ղեկավարին: • Հնարավորություն տվե՛ք օգտատերերին հաղորդել գրումինգի կասկածելի միջադեպերի մասին անմիջապես համապատասխան պետական մարմիններին: • Ստեղծե՛ք ուղիղ կապի հնարավորություն էլեկտրոնային փոստի հասցեների միջոցով՝ ահազանգելու և հաղորդելու համար:
	Առաջնահերթություն տվե՛ք երեխայի անվտանգությանն ու բարեկեցությանը: Միշտ գործե՛ք մասնագիտական ոլորտի սահմաններում և համոզվե՛ք, որ երեխաների հետ բոլոր շփումները կարևոր են ծառայության, ծրագրի, միջոցառման, գործունեության կամ նախագծի համար: Երբեք մի ստանձնե՛ք միանձնյա պատասխանատվություն երեխայի համար: Եթե երեխան ուշադրության կարիք ունի, զգուշացրե՛ք ծնողին կամ խնամակալին: Միշտ լսե՛ք և հարգե՛ք երեխաներին: Եթե ինչ-որ մեկն անպատշաճ վարքագիծ է դրսևորում երեխաների հանդեպ, ապա այդ պահվածքի մասին տեղեկացրե՛ք երեխաների պաշտպանության տեղական մարմնին:
Ավելի անվտանգ և տարիքին համապատասխան առցանց միջավայրի ստեղծում (շարունակություն)	Սահմանե՛ք կանոնների հստակ շարք, որոնք հստակ արձանագրված են և կրկնում են ծառայության պայմանները և ուղեցույցների օգտագործման ընդունելի, հիմնական կետերը: Այս կանոնները օգտագործողի համար պետք է սահմանի. • ծառայության բնույթը և այն, ինչ է ակնկալվում այն օգտագործողներից • ինչն է ընդունելի և անընդունելի բովանդակության, վարքի և լեզվի, ինչպես նաև անօրինական օգտագործումն արգելելու առումով • խախտմանը համաչափ հետևանքները, օրինակ՝ իրավապահ մարմիններին

	հաղորդելը կամ օգտատիրոջ կայքի կասեցումը:
	Օգտատերերի համար հեշտացրե՛ք չարաշահումների մասին մտահոգությունների գրանցումը՝ կիրառելով ստանդարտ և մատչելի գործընթացներ, օրինակ՝ անցանկալի հաղորդակցություն ստանալը (օրինակ՝ սփամ):
	Եղե՛ք թափանցիկ և օգտատերերին տրամադրե՛ք հստակ տեղեկատվություն առաջարկվող ծառայությունների բնույթի մասին, օրինակ՝ • բովանդակության, ծառայության տեսակը և ծախսերը • մուտքի համար պահանջվող նվազագույն տարիքը • ծնողական վերահսկողության միջոցների առկայություն, ներառյալ այն, ինչ նրանք ընդգրկում են (օրինակ՝ ցանցը) կամ չեն ընդգրկում (օրինակ՝ Wi-Fi) և դրանց օգտագործման ուսուցում • օգտատիրոջ հավաքագրված տեղեկատվության տեսակը և դրա օգտագործման եղանակը:
	Խթանե՛ք ազգային աջակցության ծառայությունները, որոնք հնարավորություն են տալիս երեխաներին և երիտասարդներին հաղորդել և աջակցություն փնտրել չարաշահման կամ շահագործման դեպքում (տե՛ս՝ օրինակ՝ Child Helpline International):

Երեխաներին, ծնողներին, ուսուցիչներին կրթել երեխաների անվտանգության և նրանց կողմից ՏՀՏ-ների պատասխանատու օգտագործման թեմաներով	Ոլորտը կարող է լրացնել տեխնիկական միջոցառումները կրթական և հզորացման աշխատանքներով՝ կատարելով հետևյալ գործողությունները.
	Հստակ նկարագրել հասանելի բովանդակությունը և համապատասխան ծնողական վերահսկողությունը կամ ընտանեկան անվտանգության կարգավորումները: Լեզուն և տերմինաբանությունը հասանելի, տեսանելի, պարզ և տեղին դարձնել բոլոր օգտատերերի համար, ներառյալ՝ երեխաներին, ծնողներին և խնամակալներին: Նկարագրել հատկապես՝ պայմանների, բովանդակության կամ ծառայությունների օգտագործման հետ կապված ծախսերի, գաղտնիության քաղաքականության, անվտանգության տեղեկատվության և հաշվետվությունների մեխանիզմների հետ:
	Կրթել օգտատերերին, թե ինչպես կառավարել համացանցի օգտագործման հետ կապված մտահոգությունները, ներառյալ սփամը, տվյալների գողությունը և ոչ պատշաճ շփումները, ինչպիսիք են ահաբեկումը և գրումինգը: Նկարագրել, թե ինչ գործողություններ կարող են ձեռնարկել օգտատերերը և ինչպես կարող են մտահոգություններ առաջ քաշել ոչ պատշաճ օգտագործման վերաբերյալ:
	Ստեղծել մեխանիզմներ և ուսուցանել ծնողներին՝ ներգրավվելու իրենց երեխաների, երիտասարդների ՏՀՏ գործունեության մեջ, մասնավորապես՝ փոքր երեխաների գործունեության մեջ, օրինակ՝ հնարավորություն տալով ծնողներին վերանայել երեխաների և երիտասարդների գաղտնիության կարգավորումները:

	Համագործակցել կառավարության և մանկավարժների հետ՝ զարգացնելու ծնողների կարողությունները՝ աջակցելու իրենց երեխաներին և երիտասարդներին, խոսելու նրանց հետ՝ պատասխանատու թվային քաղաքացիներ և ՏՀՏ օգտագործողներ լինելու մասին:
Երեխաներին, ծնողներին և մանկավարժներին կրթել երեխաների անվտանգության և նրանց կողմից ՏՀՏ-ների պատասխանատու օգտագործման մասին	Կրթական նյութեր տրամադրե՛ք՝ դպրոցներում և տանն օգտագործելու համար՝ երեխաների և երիտասարդների կողմից ՏՀՏ-ների օգտագործումը խթանելու և քննադատական մտածողությունը զարգացնելու համար՝ նրանց հնարավորություն տալով ապահով և պատասխանատու վարքագիծ դրսևորել՝ ՏՀՏ-ից օգտվելիս:
	Աջակցե՛ք օգտատերերին՝ տարածելով ընտանեկան առցանց անվտանգության վերաբերյալ ուղեցույցներ, որոնք խրախուսում են ծնողներին և խնամակալներին՝ • ծանոթանալ երեխաների և երիտասարդների կողմից օգտագործվող ապրանքներին և ծառայություններին • ապահովել երեխաների և երիտասարդների կողմից էլեկտրոնային սարքերի չափավոր օգտագործումը՝ որպես առողջ և հավասարակշռված ապրելակերպի մաս • մեծ ուշադրություն դարձնել երեխաների և երիտասարդների վարքագծին, որպեսզի հայտնաբերեք փոփոխություններ, որոնք կարող են վկայել կիբերհալածանքի կամ ոտնձգության մասին:

	Ծնողներին տրամադրե՛ք անհրաժեշտ տեղեկատվություն՝ հասկանալու համար, թե ինչպես են իրենց երեխաները, երիտասարդներն օգտվում ՏՀՏ ծառայություններից, կարգավորե՛ք վնասակար բովանդակության և վարքագծի հետ կապված հարցերը: Պատրաստ եղե՛ք երեխաներին և երիտասարդներին համացանցի պատասխանատու օգտագործման մեջ առաջնորդելու համար: Դա կարելի է հեշտացնել դպրոցների հետ համագործակցելու միջոցով՝ երեխաների համար առցանց անվտանգության ուսումնական ծրագիր և ծնողների համար կրթական նյութեր տրամադրելու միջոցով:
Օգտագործելով տեխնոլոգիաների առաջընթացը երեխաներին պաշտպանելու և կրթելու համար	Գաղտնիությունը պահպանող արհեստական ինտելեկտը, որը հասկանում է տեքստերը, պատկերները, խոսակցությունները և ենթատեքստերը, կարող է հայտնաբերել և անդրադառնալ մի շարք առցանց վնասների, սպառնալիքների: Այդ տեղեկատվությունն օգտագործել երեխաներին հզորացնելու և կրթելու նպատակով, բացատրել, թե ինչպես վարվեն դրա հետ: Խելացի սարքերի միջավայրում, այս գործողությունները կարող են պաշտպանել երիտասարդների տվյալները և գաղտնիությունը՝ միևնույն ժամանակ աջակցելով նրանց:
	Հանրային ծառայությունները և ազգային լրատվամիջոցները կարող են էական դեր խաղալ իրենց ծրագրային առաջարկների միջոցով (անցանց և առցանց)՝ ծնողներին և երեխաներին կրթելու, նրանց առցանց աշխարհի ռիսկերի ու հնարավորությունների մասին իրազեկելու գործում:

Թվային տեխնոլոգիաների խթանում՝ որպես քաղաքացիական ներգրավվածության միջոց	Ոլորտը կարող է խրախուսել և հզորացնել երեխաներին և երիտասարդներին՝ աջակցելով նրանց մասնակցության իրավունքին հետևյալ գործողությունների միջոցով.
	Տրամադրե՛ք տեղեկատվություն ծառայության մասին՝ ընդգծելով այն օգուտները, որոնք երեխաները ստանում են լավ և պատասխանատու վարք դրսևորելով, օրինակ՝ ծառայությունը ստեղծագործական նպատակներով օգտագործելու միջոցով:
	Սահմանե՛ք գրավոր ընթացակարգեր, որոնք ապահովում են քաղաքականության և SS գործընթացների հետևողական իրականացումը, որոնք պաշտպանում են խոսքի ազատությունը բոլոր օգտատերերի՝ ներառյալ երեխաներին և երիտասարդներին, ինչպես նաև մեդիա քաղաքականության հետ կապված համապատասխան փաստաթղթերը:

Թվային տեխնոլոգիաների խթանում՝ որպես քաղաքացիական ներգրավվածության միջոց (շարունակություն)	Խուսափե՛ք օրինական և զարգացման համար համապատասխան բովանդակության գերարգելափակումից: Կարևոր է, որ համոզված լինեք, որ ֆիլտրման հարցումներն ու գործիքները չեն չարաշահվում երեխաների և երիտասարդների տեղեկատվության հասանելիությունը սահմանափակելու համար: Համոզվե՛ք, որ արգելափակված բովանդակության վերաբերյալ թափանցիկությունը ապահովված է և օգտատերերն ունեն անկանխամտածված արգելափակման մասին հաղորդելու հնարավորություն: Այս գործընթացը պետք է հասանելի լինի բոլոր սպառողների, այդ թվում՝ վեբ մասնագետների համար: Հաղորդում/բողոք ներկայացնելու ցանկացած գործընթաց պետք է ապահովի ծառայության հստակ, պատասխանատու և վճռական պայմաններ:
	Մշակե՛ք առցանց հարթակներ, որոնք նպաստում են երեխաների և երիտասարդների ինքնադրսևորման իրավունքին՝ հեշտացնելով նրանց մասնակցությունը հասարակական կյանքում: Խրախուսե՛ք նրանց համագործակցությունը, ձեռներեցությունը և քաղաքացիական մասնակցությունը:
	Մշակե՛ք երեխաների և երիտասարդների համար կրթական բովանդակություն, որը խրախուսում է ուսումնական գործընթացի արդյունավետությունը, ձևավորում ստեղծագործական մտածողություն և հնարավորություն տալիս գտնել խնդիրների լուծումները:
	Խթանե՛ք թվային գրագիտությունը, կարողությունների և ՏՀՏ հմտությունների զարգացումը՝ երեխաների և երիտասարդների շրջանում: Կարևորե՛ք հատկապես գյուղական և անապահով շրջաններում ապրող երեխաների, երիտասարդների՝ ՏՀՏ ռեսուրսներն օգտագործելը, թվային աշխարհում ապահով և լիարժեք գործունեությունը:

	Համագործակցե՛ք տեղական քաղաքացիական հասարակության և կառավարության հետ՝ ազգային և տեղական առաջնահերթությունների շուրջ՝ ՏՀՏ-ների, հարթակների և սարքերի համընդհանուր, հավասար հասանելիության ընդլայնման, դրանց աջակցության հիմքում ընկած ենթակառուցվածքի զարգացման համար:
	Տեղեկացրե՛ք և ներգրավե՛ք հաճախորդներին, նաև՝ ծնողներին, խնամակալներին, երեխաներին և երիտասարդներին, առաջարկվող ծառայությունների մասին, օրինակ. • բովանդակության տեսակի և համապատասխան ծնողական վերահսկողության • չարաշահման, շահագործման և ոչ պատշաճ կամ անօրինական բովանդակության դեպքերի, դրանց հաղորդման մեխանիզմների • հաղորդում/բողոք ներկայացնելու համար հետագա ընթացակարգերի • ծառայությունների այն տեսակների մասին, որոնք տարիքային սահմանափակում ունեն • «սեփական ապրանքանիշի» ինտերակտիվ ծառայությունների անվտանգ և պատասխանատու օգտագործման:
	Զբաղվե՛ք անվտանգ և պատասխանատու թվային քաղաքացիության հետ կապված ավելի լայն խնդիրներով, օրինակ՝ առցանց հեղինակությունը և թվային հետքը, վնասակար բովանդակությունը և գրումինգը: Մտածե՛ք, թե ինչպես համագործակցել տեղական փորձագետների հետ, որոնք են երեխաների հարցերով զբաղվող ՀԿ-ները, բարեգործական կազմակերպությունները և ծնողական խմբերը, որոնք կօգնեն ձևավորել ընկերության ուղերձը՝ այն հասցնել նախատեսված լսարանին:

	Եթե բիզնեսն արդեն աշխատում է երեխաների կամ դպրոցների հետ, օրինակ՝ կորպորատիվ սոցիալական պատասխանատվության ծրագրերի միջոցով: Ուսումնասիրե՛ք այս ներգրավվածությունը ընդլայնելու հնարավորությունը՝ ներառելով երեխաների, երիտասարդների, ինչպես նաև մանկավարժների՝ երեխաների առցանց պաշտպանության հարցերը բարձրաձայնելու և համապատասխան լսարանին հասցնելու համար:
Ներդրումներ ուսումնասիրության մեջ	Ներդրումներ կատարե՛ք փաստերի վրա հիմնված ուսումնասիրության և թվային տեխնոլոգիաների խորը վերլուծության, երեխաների վրա տեխնոլոգիաների ազդեցության, թվային միջավայրի հետ կապված երեխաների պաշտպանության և երեխաների իրավունքների վերաբերյալ նյութերում: Դա կնպաստի, որ առցանց պաշտպանության համակարգերը երեխաների և երիտասարդների կողմից օգտագործվող ծառայությունների մեջ ինտեգրվեն, ավելի տեսանելի դառնա, թե ինչ տեսակի միջամտություններն են առավել արդյունավետ՝ երեխաների առցանց փորձը բարելավելու համար:

ՏՀՏ ընկերությունների տիպաբանություն

Թեև ՀՄՄ-ի այս ուղեցույցներն ուղղված են ՏՀՏ ոլորտին, կարևոր է գիտակցել, որ ՏՀՏ ընկերությունների կողմից առաջարկվող ծառայությունները, դրանց գործունեության եղանակները, կարգավորող համակարգերը, որոնց ներքո գործում են, ներկայացված առաջարկների շրջանակն ու ոլորտի ընդգրկումը տարբեր են:
Ցանկացած տեխնոլոգիական ընկերություն, որի արտադրանքն ու ծառայությունները ուղղակիորեն կամ անուղղակիորեն ուղղված են երեխաներին, կարող են օգտվել նախկինում սահմանված ընդհանուր սկզբունքներից: Կարող են նաև հարմարվել՝ ելնելով իրենց գործունեության կոնկրետ ոլորտից: Հիմնական գաղափարը ՏՀՏ ոլորտին աջակցելն ու ուղղորդելն է, որպեսզի ճիշտ միջոցներ ձեռնարկեն երեխաներին առցանց հարթակներում ավելի լավ
պաշտպանելու առկա վտանգներից: Միաժամանակ կարևոր է նրանց հնարավորություն տալ, որ առցանց աշխարհում կարողանան ավելի լավ նավարկել: Ստորև բերված տիպաբանությունը կօգնի ավելի հստակ պատկերացում կազմել որոշ թիրախային լսարանների մասին. ինչպես են դրանք տեղավորվում հաջորդ բաժնի ստուգաթերթերում:
Հարկ է նշել, որ սրանք ընդամենը մի քանի կոնկրետ բնագավառներ են և ցանկը սպառիչ չէ.

(ա) Ինտերնետ ծառայություններ մատուցողներ, նաև՝ ֆիքսված լայնաշերտ կամ բջջային ցանցի օպերատորների տվյալների ծառայություններ. թեև սա սովորաբար արտացոլում է բաժանորդագրված օգտատերերին ավելի երկարաժամկետ հիմունքներով առաջարկվող ծառայությունները: Կարող է տարածվել նաև այն ձեռնարկությունների վրա, որոնք տրամադրում են անվճար կամ վճարովի հանրային WI-FI թեժ կետեր:

(բ) Սոցիալական ցանցերի, հաղորդագրությունների փոխանակման հարթակներ և առցանց խաղերի հարթակներ:

(գ) Սարքավորումներ և ծրագրաշարեր արտադրողներ, ինչպիսիքեն ձեռքի սարքերի մատակարարները, նաև՝ բջջային հեռախոսներ, խաղային վահանակներ, ձայնային աջակցության վրա հիմնված տնային սարքեր, իրերի ինտերնետ և երեխաների համար խելացի, համացանցին միացված խաղալիքներ արտադրողները:

(դ) Թվային մեդիա տրամադրող ընկերություններ (բովանդակություն ստեղծողներ, բովանդակության հասանելիություն կամ հոսթինգ տրամադրողներ):

(ե) Ընկերություններ, որոնք տրամադրում են հոսքային ծառայություններ, ներառյալ՝ ուղիղ հեռարձակումները:

(զ) Ընկերություններ, որոնք առաջարկում են թվային ֆայլերի պահպանման ծառայություններ, ամպային ծառայություն մատուցողներ:

5. Առանձնահատկություններին վերաբերող ստուգաթերթեր

Այս գլուխը ներառում է նախորդ ընդհանուր ստուգաթերթն ոլորտի համար՝ առաջարկելով տարբերակներ այն ձեռնարկությունների համար, որոնք ծառայություններ են մատուցում հատուկ կարիքներով երեխաների իրավունքների՝ առցանց հարթակներում դրանց հարգման և աջակցության վերաբերյալ:
Հետևյալ առանձնահատկություններին հատուկ ստուգաթերթերն ուրվագծում են Աղյուսակ 1-ում ներկայացված ընդհանուր սկզբունքներն ու մոտեցումները լրացնելու ուղիները, քանի որ դրանք կիրառվում են տարբեր ծառայությունների համար, հետևաբար, պետք է դիտարկվեն ի հավելումն Աղյուսակ 1-ի քայլերի:
Այստեղ ընդգծված առանձնահատկությունները խաչաձև են. մի քանի առանձնահատկություններ պարունակող հատուկ ստուգաթերթեր կարող են համապատասխան լինել նույն ընկերության համար:
Հետևյալ առանձնահատկությունների ստուգաթերթերը կազմակերպված են և վերաբերում են նույն հիմնական ոլորտներին, ինչ ընդհանուր ուղեցույցներն Աղյուսակ 1-ում: Առանձնահատկությունների ստուգաթերթերից յուրաքանչյուրը մշակվել է հիմնական ներդրողների հետ համագործակցությամբ.արդյունքում աղյուսակներում կան աննշան փոփոխություններ:

5.1 Առանձնահատկություն Ա. Տրամադրել կապի, տվյալներիպահպանման և հոսթինգի ծառայություններ

Ինտերնետ հասանելիությունը հիմնարար է երեխաների իրավունքների իրացման համար: Ինտերնետ կապը կարող է նոր աշխարհներ բացել երեխաների համար: Կապի, տվյալների պահպանման և հոսթինգի ծառայություններ մատուցողները հսկայական հնարավորություններ ունեն երեխաների և երիտասարդների համար իրենց առաջարկների մեջ ներառելու անվտանգությունն ու գաղտնիությունը: Այս ծառայության առանձնահատկությունն՝ ի թիվս այլոց, հասցեագրում է բջջային օպերատորներին, ինտերնետ ծառայություններ մատուցողներին, տվյալների պահպանման համակարգերին և հոսթինգ ծառայություններին:

Բջջային օպերատորներն ապահովում են ինտերնետ հասանելիություն և առաջարկում են բջջային սարքերին հատուկ տվյալների փոխանցման ծառայությունների լայն շրջանակ: Շատ օպերատորներ արդենստորագրել են Երեխաների առցանց պաշտպանության պրակտիկայի կանոնները և առաջարկում են մի շարք գործիքներ և տեղեկատվական ռեսուրսներ:

Ինտերնետ ծառայությունների մատակարարների մեծամասնությունը գործում է և՛ որպես ինտերնետ հասանելիություն ապահովող կապուղի, որն ապահովում է մուտք դեպի ինտերնետ և ինտերնետից դուրս, և՛ տվյալների շտեմարան՝ իրենց հոսթինգի, քեշավորման և պահպանման ծառայությունների միջոցով: Արդյունքում նրանք՝ երեխաներին առցանց պաշտպանելու հարցերում առաջնային պատասխանատվություն կրողներն են:

Ինտերնետ հասանելիություն հանրային տարածքներում

Համայնքների, մանրածախ առևտրի, տրանսպորտային ընկերությունների, հյուրանոցային ցանցերի և այլ ձեռնարկությունների և կազմակերպությունների համար գնալով ավելի տարածված է դառնում Wi-Fi թեժ կետերի միջոցով ինտերնետ հասանելիություն ապահովելը: Նման մուտքը սովորաբար անվճար է կամ տրամադրվում է նվազագույն գնով, երբեմն՝ գրանցման նվազագույն պահանջներով՝ որպես հանրային ծառայություն, կամ ընկերության կողմից՝ օգտատերերին իր տարածք ներգրավելու, ավելի շատ մարդկանց համոզելու համար, որ օգտվեն իր ծառայություններից:

Wi-Fi-ի խթանումը տվյալ տարածքում՝ ինտերնետի հասանելիությունն ապահովելու արդյունավետ միջոց է: Այնուամենայնիվ, անհրաժեշտ է զգուշություն ցուցաբերել, երբ նման մուտքն ապահովվում է հանրային վայրերում, որտեղ երեխաները, հավանաբար, կանոնավոր կերպով նույնպես միանում են Համացանցին: Օգտատերերը պետք է նկատի ունենան այն փաստը, որ Wi-Fi ազդանշանները կարող են հասանելի լինել անծանոթներին, այդ դեպքում օգտատիրոջ տվյալները վտանգված կլինեն: Հետևաբար, Wi-Fi մատակարարը միշտ չէ, որ կկարողանա աջակցել կամ վերահսկել իր կողմից տրամադրված ինտերնետ կապի օգտագործումը: Հետևաբար օգտատերերը պետք է նախազգուշական միջոցներ ձեռնարկեն՝ հանրային հասանելի Wi-Fi-ի միջոցով կարևոր տեղեկությունները չկիսելու համար:

Հանրային տարածքներում Wi-Fi մատակարարները կարող են մտածել երեխաների և երիտասարդների պաշտպանության համար լրացուցիչ միջոցների մասին, ինչպիսիք են՝

- Ի լրումն ԵՍՇՆ-ի մուտքն արգելափակելու ջանքերի, ակտիվորեն արգելափակել մուտքը դեպի վեբ հասցեներ, որոնք

պարունակում են անպատշաճ բովանդակություն:
- Ներառել օգտագործման պայմանների և կանոնների դրույթները, որոնք արգելում են Wi-Fi ծառայությունների օգտագործումը՝ ցանկացած այնպիսի նյութ մուտք գործելու կամ ցուցադրելու համար, որը կարող է ոչ պիտանի լինել այնպիսի միջավայրում, որտեղ երեխաներ են: Պայմանները պետք է ներառեն նաև հստակ մեխանիզմներ՝ նման կանոնների խախտման հետևանքների հետ կապված:
- Ձեռնարկել տարաբնույթ միջոցներ՝ պաշտպանվելու չարտոնված մուտքից, որը կարող է հանգեցնել անձնական տվյալների մանիպուլյացիայի կամ կորստի:
- Wi-Fi համակարգում ֆիլտրերի տեղադրում՝ անպատշաճ նյութերի նկատմամբ քաղաքականությունն ամրապնդելու համար:
- Տրամադրել ընթացակարգեր և ծրագրային ապահովում՝ ծնողական հսկողություն առաջարկելու՝ երեխաների և երիտասարդների համացանցի բովանդակության հասանելիության հետ կապված հարցերում:

Լավագույն փորձ. Եվրոպական միության անդամ երկրների մեծ մասի հեռահաղորդակցության կանոնակարգերն, օրինակ, սահմանում են, որ մուտքը համացանց պետք է նույնականացվի անհատական ՍԻՄ քարտերի կամ նույնականացման այլ գործիքների միջոցով:

Աղյուսակ 2-ը ուղեցույց է տրամադրում կապի, տվյալների պահպանման և հոսթինգի ծառայություններ մատուցողներին այն գործողությունների վերաբերյալ, որոնք նրանք կարող են ձեռնարկել երեխաների առցանց պաշտպանությունը և երեխաների մասնակցությունը բարձրացնելու համար:

Աղյուսակ 2. ԵԱՊ ստուգաթերթ Ա առանձնահատկության համար. տրամադրել կապի, տվյալների և հոսթինգի ծառայություններ

Երեխաների իրավունքների նկատառումների ինտեգրում բոլոր համապատասխան կորպորատիվ քաղաքականությունների և կառավարման գործընթացներում	Կապի, տվյալների պահպանման և հոսթինգի ծառայություններ մատուցողները կարող են բացահայտել, կանխել և մեղմել ՏՀՏ-ների բացասական ազդեցությունը երեխաների և երիտասարդների իրավունքների վրա, բացահայտել երեխաների և երիտասարդների իրավունքների առաջխաղացմանն աջակցելու հնարավորությունները:
	Տե՛ս աղյուսակ 1-ի ընդհանուր ուղեցույցները:
Ստանդարտ գործընթացների մշակում՝ ԵՍՇՆ-ի հետ աշխատելու համար	Համագործակցելով կառավարության, իրավապահ մարմինների, քաղաքացիական հասարակության և թեժ գծի կազմակերպությունների հետ, կապի, տվյալների պահպանման և հոսթինգի ծառայություններ մատուցողները կարող են առանցքային դեր խաղալ ԵՍՇՆ-ի դեմ պայքարում՝ ձեռնարկելով հետևյալ գործողությունները.
	Համագործակցել կառավարության, իրավապահ մարմինների, քաղաքացիական հասարակության և թեժ գծի կազմակերպությունների հետ՝ արդյունավետորեն կարգավորելու ԵՍՇՆ-ն և հաղորդում ներկայացնելու համապատասխան մարմիններին: Եթե հարաբերությունները իրավապահ մարմինների և թեժ գծի հետ դեռ հաստատված չեն, հնարավորինս ներգրավել նման գործընթացները զարգացնելու ուղղությամբ: Կապի, տվյալների պահպանման կամ հոսթինգի ծառայություններ մատուցողները կարող են նաև ՏՀՏ ուսուցում ապահովել իրավապահ մարմինների համար: Եթե ընկերությունը գործում է շուկաներում, որտեղ այս հարցում ավելի քիչ զարգացած իրավական և իրավապահ վերահսկողություն կա, այն կարող է ուղղորդել ներկայացված բողոքներն Ինտերնետ Թեժ գծերի միջազգային ասոցիացիա (INHOPE), որտեղ

	հաշվետվությունները կարող են ներկայացվել ցանկացած միջազգային թեժ գծի:
	Ներդնել համապատասխան մարմինների կողմից ստեղծված միջազգայնորեն ճանաչված URL-ների կամ վեբ կայքերի արգելափակման ցուցակները (օրինակ՝ ազգային իրավապահ մարմինների կամ թեժ գծի, Cybertip Canada, Ինտերպոլ, IWF) ՝ օգտատերերի համար նույնականացված ԵՍՇՆ մուտքը դժվարացնելու համար:
	Մշակել ծանուցման, ոչնչացման և հաղորդման գործընթացներ: Չարաշահումների մասին հաղորդումները կապել այդ գործընթացների հետ՝ հանրային ծառայության համաձայնագրի հետ արձագանքման ընթացակարգի և հեռացման ժամանակների հետ զուգահեռ: Տե՛ս, օրինակ, ՅՈՒՆԻՍԵՖ-ի և GSMA ուղեցույցը ծանուցումների և անցանկալի բովանդակության հեռացման քաղաքականության և գործելակերպի վերաբերյալ:
	Ստեղծել հաղորդման մեխանիզմ՝ դրա օգտագործման վերաբերյալ հստակ տեղեկություններով, օրինակ՝ ուղղորդելով հաղորդվող անօրինական բովանդակության և վարքագծի վերաբերյալ, պարզաբանելով, թե որ նյութերը չեն կարող կցվել հաղորդմանը, բողոքին՝ դրանց՝ համացանցում հետագա տարածումից խուսափելու համար:
Ստանդարտ գործընթացների մշակում ԵՍՇՆ-ի հետ աշխատելու համար (շարունակություն)	Քրեական հետախուզության դեպքում աջակցել իրավապահ մարմիններին այնպիսի գործողությունների միջոցով, ինչպիսիք են ապացույցներ հավաքելը: Օգտագործել ծառայության պայմաններն ու դրույթները՝ հատուկ արգելելու ԵՍՇՆ պահելու, համօգտագործելու կամ տարածելու ծառայությունների

	օգտագործումը: Համոզվել, որ այս պայմանները հստակ նշում են, որ ԵՍՇՆ չի թույլատրվի: Համոզվել, որ ծառայության պայմանները և դրույթները նշում են, որ ընկերությունը լիովին կհամագործակցի իրավապահ մարմինների հետ հետաքննության դեպքում, եթե ԵՍՇՆ հայտնաբերվի կամ դրա մասին հաղորդվի:
	Ներկայումս ազգային մակարդակում ԵՍՇՆ-ի՝ առցանց հաշվետվության երկու լուծում կա՝ թեժ գծեր և հաղորդման՝ բողոքի, ներկայացման պորտալներ: Բոլոր առկա թեժ գծերի և պորտալների ամբողջական արդի ցանկը կարելի է գտնել INHOPE-ում: **Թեժ գծեր**. Եթե ազգային թեժ գիծը հասանելի չէ, ուսումնասիրե՛ք հնարավորությունները այն ստեղծելու համար (տե՛ս GSMA INHOPE Թեժ գծերի ուղեցույցը մի շարք տարբերակների համար, ներառյալ՝ INHOPE-ի և INHOPE հիմնադրամի հետ աշխատելը): Հասանելի է GSMA INHOPE ուղեցույցի ինտերակտիվ տարբերակը, որն ուղղորդում է, թե ինչպես մշակել ներքին գործընթացներ հաճախորդների սպասարկման ոլորտի անձնակազմի համար՝ կասկածելի բովանդակության մասին հաղորդումներ ներկայացնելով իրավապահ մարմիններին և INHOPE-ին: *Հաղորդման՝ բողոքների ներկայացման պորտալներ*. IWF-ն առաջարկում է հաղորդման պորտալի այնպիսի տարբերակ, որը թույլ է տալիս համացանցի օգտատերերին՝ առանց թեժ գծերի երկրներում և ազգերում՝ երեխաների նկատմամբ կասկածվող սեռական բռնության մասին լուսանկարների և տեսանյութերի մասին հաղորդել անմիջապես IWF-ին՝ հատուկ պատվիրված առցանց պորտալի էջի միջոցով:

	Կապի, տվյալների պահպանման և հոսթինգի ծառայություններ մատուցողների համար, որոնց ծառայությունները ներառում են բովանդակության տեղադրման որևէ տեսակ (շատերը չեն անում), պետք է տրամադրվեն ծանուցման և հեռացման ընթացակարգեր:
Ստեղծել ավելի անվտանգ և տարիքին համապատասխան թվային միջավայր	Կապի, տվյալների պահպանման և հոսթինգի ծառայություն մատուցողները կարող են օգնել ստեղծել ավելի անվտանգ և հաճելի թվային միջավայր՝ բոլոր տարիքի երեխաների համար՝ կատարելով հետեյալ գործողությունները:
	Տվյալների պահպանման, հոսթինգի ծառայություններ մատուցողները պետք է հաշվի առնեն բոլոր վեբ-էջերի և ծառայությունների հաղորդականության գործառույթի տրամադրման հնարավորությունը, ինչպես նաև՝ մշակեն և փաստաթղթավորեն հստակ գործընթացներ՝ չարաշահումների, կանոնների և պայմանների այլ խախտումների մասին հաղորդումների օպերատիվ կառավարման համար:
	Կապ տրամադրողները պետք է առաջարկեն սեփական ապրանքանիշի վերահսկողության տեխնիկական միջոցներ կամ մատնանշեն մասնագիտացված մատակարարների կողմից ստեղծված մատչելի գործիքներ, որոնք հարմար են վերջնական օգտագործողի համար, առաջարկում են ընկերության ցանցի միջոցով համացանցին հասանելիության արգելափակման կամ ֆիլտրման հնարավորություն: Ապահովել տարիքին համապատասխան ստուգման մեխանիզմներ, եթե ընկերությունն առաջարկում է բովանդակություն կամ ծառայություններ (ներառյալ ընկերության կողմից խթանվող սեփական բրենդը կամ երրորդ անձանց ծառայությունները), որոնք օրինական կամ հարմար են միայն

	չափահաս օգտագործողների համար (օրինակ՝ որոշակի խաղեր, խաղարկություններ):
Երեխաների, ծնողների և մանկավարժների կողմից աջակցությունը՝ երեխաների անվտանգության և ՏՀՏ պատասխանատու օգտագործման հարցերով	Կապի, տվյալների պահպանման և հոսթինգի ծառայություն մատուցողները պետք է արտացոլեն համայնքային ուղեցույցների կանոնների և պայմանների հիմնական դրույթները, որոնք գրված են օգտագործողին հարմար լեզվով՝ աջակցելու երեխաներին, նրանց ծնողներին և խնամք իրականացնող անձանց: Ծառայության ներսում, բովանդակության վերբեռնման պահին, ներառե՛ք հիշեցումներ այնպիսի թեմաների մասին, ինչպիսիք են անպատշաճ համարվող բովանդակության տեսակները:
	Երեխաներին և երիտասարդներին տրամադրել տեղեկատվություն համացանցի անվտանգ օգտագործման վերաբերյալ: Մտածե՛ք հիմնական հաղորդագրությունները խթանելու ստեղծագործական ուղիներ, ինչպիսիք են՝ «Երբեք մի՛ փոխանցեք որևէ կոնտակտային տվյալ (օրինակ՝ ձեր գտնվելու վայրը, հեռախոսահամարը) որևէ մեկին, ում անձամբ չեք ճանաչում»: «Երբեք մի՛ համաձայնեք ինքնուրույն հանդիպել որևէ մեկի հետ, ում հետ ծանոթացել եք առցանց՝ առանց նախապես մեծահասակների հետ խորհրդակցելու: Միշտ վստահելի ընկերոջը պատմե՛ք ձեր գտնվելու վայրի մասին»: «Մի՛ արձագանքեք ահաբեկչական, անպարկեշտ կամ վիրավորական հաղորդագրություններին: Բայց պահպանե՛ք ապացույցները, մի՛ ջնջեք հաղորդագրությունները»:

	«Ասե՛ք վստահելի չափահաս մարդու, ձեր ընկերոջը, եթե անհարմար եք զգում, վրդովված եք ինչ-որ բանից կամ ինչ-որ մեկից»: «Երբեք մի՛ տվեք ձեր հաշվի գաղտնաբառը կամ օգտվողի անունը: Ուշադիր եղե՛ք, որ առցանց այլ մարդիկ կարող են կեղծ տեղեկություններ տալ, որպեսզի համոզեն ձեզ կիսվել ձեր անձնական տեղեկություններով»:
	Ծառայություններ մատուցողները կարող են համագործակցել կազմակերպությունների հետ, որոնք ունեն լավ հնարավորություններ՝ երեխաների համար համացանցի անվտանգ օգտագործման և դրա հետ կապված հարցերի վերաբերյալ: Օրինակների համար տե՛ս Child Helpline International և GSMA գործնական ուղեցույցը երեխաների աջակցության գծերի և բջջային օպերատորների համար
Թվային տեխնոլոգիաների խթանում՝ որպես հետագա քաղաքացիական ներգրավվածության միջոց	*Տե՛ս աղյուսակ 1-ի ընդհանուր ուղեցույցները:*

5.2 Առանձնահատկություն Բ. Առաջարկեք համադրված թվային բովանդակություն

Համացանցը տրամադրում է ամեն տեսակի բովանդակություն և գործունեություն, որոնցից շատերը նախատեսված են երեխաների և երիտասարդների համար: Համադրված խմբագրությամբ բովանդակություն առաջարկող ծառայությունները հսկայական հնարավորություններ ունեն երեխաների և երիտասարդների համար նախատեսված իրենց առաջարկներում անվտանգությունն ու գաղտնիությունը ներառելու համար:

Ծառայության այս առանձնահատկությունը վերաբերում է ինչպես բիզնեսներին, որոնք ստեղծում են իրենց սեփական բովանդակությունը, այնպես էլ նրանց, որոնք հասանելիություն են ապահովում թվային բովանդակությանը: Այն, ի թիվս այլոց, վերաբերում է նորություններին և մուլտիմեդիա ծառայություններին, ազգային և հանրային հեռարձակման ծառայություններին և խաղերի ոլորտին:

Աղյուսակ 3-ը ուղեցույց է տրամադրում ծառայություններ մատուցողներին, որոնք առաջարկում են համադրված խմբագրությամբ բովանդակություն այն քաղաքականության և գործողությունների վերաբերյալ, որոնք նրանք կարող են ձեռնարկել երեխաների առցանց պաշտպանությունն ու մասնակցությունը բարձրացնելու համար:

Աղյուսակ 3. ԵԱՊ վերաբերյալ ստուգաթերթ Բ հատկանիշի համար. Առաջարկել ընտրված թվային բովանդակություն

Երեխաների իրավունքների նկատառումների ինտեգրում բոլոր համապատասխան կորպորատիվ քաղաքականության և կառավարման գործընթացներում	Համադրված թվային բովանդակություն տրամադրող ծառայությունները կարող են օգնել բացահայտել, կանխել և մեղմել ՏՀՏ-ների բացասական ազդեցությունները երեխաների և երիտասարդների իրավունքների վրա, ինչպես նաև բացահայտել երեխաների և երիտասարդների իրավունքների պաշտպանման աջակցելու հնարավորությունները՝ ձեռնարկելով հետևյալ գործողությունները.
	Մշակել քաղաքականություն, որը կպաշտպանի երեխաների և երիտասարդների բարեկեցությունը, ովքեր առցանց բովանդակություն են ներկայացնում՝ հաշվի առնելով 18 տարեկանից ցածր մարդկանց ֆիզիկական և էմոցիոնալ բարեկեցությունը և արժանապատվությունը, ովքեր ներգրավված են ծրագրերում, ֆիլմերում, խաղերում, նորություններում և այլն՝ անկախ համաձայնությունից, որը կարող էր տրված լինել ծնողի կամ այլ չափահասի կողմից:

Ստանդարտ գործընթացների մշակում ԵՍՇՆ-ի հետ աշխատելու համար	Համագործակցելով կառավարության, իրավապահ մարմինների, քաղաքացիական հասարակության և թեժ գծի կազմակերպությունների հետ՝ համադրված թվային բովանդակություն առաջարկող ընկերությունները կարող են առանցքային դեր խաղալ ԵՍՇՆ-ի դեմ պայքարում հետևյալ գործողությունների միջոցով. ԵՍՇՆ-ի դեպքերում, օրինակ՝ «մեկնաբանության» գործառույթների միջոցով, որտեղ օգտվողները կարող են բովանդակություն վերբեռնել, անձնակազմը պետք է կապ հաստատի գործադիր կառավարման թիմի հետ, որը պատասխանատու է նման նյութը մասին համապատասխան մարմիններին հաղորդելու համար: Բացի այդ, նրանց պետք է. • անհապաղ զգուշացնել ազգային իրավապահ մարմիններին • զգուշացնել իրենց ղեկավարին և նյութի մասին զեկուցել երեխաների պաշտպանության քաղաքականության ղեկավարին • միջադեպի մանրամասներով կապվել ներքին հետաքննության ծառայության հետ հեռախոսով կամ էլեկտրոնային փոստով՝ խորհրդատվություն ստանալու համար • սպասել համապատասխան գործակալության խորհրդին՝ նյութը ջնջելուց, այն ընդհանուր տարածությունում պահելուց կամ փոխանցելուց առաջ:

Ստանդարտ գործընթացների մշակում ԵՄՇՆ-ի հետ աշխատելու համար	Եթե նյութը բացահայտված է, այն պետք է ուղղակիորեն հաղորդվի ինտերնետի անվտանգության ոլորտում մասնագիտացած կազմակերպությանը, որը գործարկում է թեժ գծի հաղորդման/բողոքի ներկայացման համակարգը հանրության անդամների և տեղեկատվական տեխնոլոգիաների մասնագետների համար՝ պոտենցիալ անօրինական առցանց բովանդակության որոշակի ձևերի մասին հաղորդելու համար: Օրինակ՝ հիմնվելով Երեխաների պաշտպանության քաղաքականության վրա՝ ԲիԲիՍի-ն հրապարակել է խմբագրական ուղեցույց՝ երեխաների և երիտասարդների հետ շփվելու վերաբերյալ: Այն մշակել է լրացուցիչ ստուգաթերթեր և վարքագծի կանոններ երեխաների և երիտասարդների հետ առցանց աշխատելու համար, որոնք տարածվում են նաև ենթակապալառուների և արտաքին մատակարարների վրա: Երեխաների պաշտպանության վերաբերյալ Ofcom-ի քաղաքականությունը Միացյալ Թագավորությունում վերաբերում է առցանց բովանդակությանը, շարժական սարքերին և խաղային վահանակներին առանձին: Ներդրեք արագ և հուսալի էսկալացիայի ռազմավարություն, եթե հրապարակվի CSAM կամ կասկածներ առաջանան անօրինական վարքագծի վերաբերյալ: Այս նպատակով՝ • օգտատերերին առաջարկել պարզ և հեշտ հասանելի միջոց բովանդակություն արտադրողին հաղորդելու առցանց համայնքի ցանկացած կանոնի խախտման մասին • հեռացնել բովանդակությունը, որը խախտում է կանոնները Նախքան՝ տարիքը հաշվի առնելով, խմբագրական բովանդակություն սոցիալական ցանց ներբեռնելը, տեղյակ

	եղեք կայքի դրույթներին և պայմաններին: Զգույշ եղեք տարբեր սոցիալական ցանցերում նվազագույն տարիքային պահանջների նկատմամբ: Յուրաքանչյուր առցանց տարածքի պայմաններն ու դրույթները պետք է ներառեն նաև նման կանոնների խախտման վերաբերյալ հաղորդումների հստակ մեխանիզմներ:
Ավելի անվտանգ և տարիքին համապատասխան առցանց միջավայրի ստեղծում	Համադրված թվային բովանդակություն առաջարկող ընկերությունները կարող են օգնել ստեղծել ավելի ապահով և հաճելի թվային միջավայր բոլոր տարիքի երեխաների և երիտասարդների համար՝ կատարելով հետևյալ գործողությունները.
	Աշխատեք ոլորտի մասնագետների հետ՝ մշակելու բովանդակության դասակարգման/տարիքային գնահատման համակարգեր, որոնք հիմնված են ընդունված ազգային կամ միջազգային ստանդարտների վրա և համահունչ են համարժեք լրատվամիջոցներում ընդունված մոտեցումներին: Հնարավորության դեպքում բովանդակության դասակարգումները պետք է համապատասխանեն տարբեր մեդիա հարթակներում, օրինակ՝ կինոթատրոնում և սմարթֆոնի վրա ֆիլմի թրեյլերը օգտատերերին ցույց կտա նույն դասակարգումները:
	Մշակեք երեխաներին հարմար և տարիքին համապատասխան նյութեր երեխաների և երիտասարդների համար, որոնք ապահով են դիզայնով և լրացվում են տարիքի ստուգման ապահով համակարգով:
	Որպեսզի օգնեք ծնողներին և մյուսներին որոշել, թե արդյոք բովանդակությունը համապատասխան է երեխաների և երիտասարդների տարիքին, ստեղծեք բովանդակության գնահատման համակարգերին համապատասխան հավելվածներ և ծառայություններ բոլոր

	մեդիաներում: Ընդունեք տարիքի ստուգման համապատասխան մեթոդներ՝ երեխաներին և երիտասարդներին թույլ չտալու համար մուտք գործել տարիքին անհամապատասխան բովանդակություն, կայքեր, ապրանքներ կամ ինտերակտիվ ծառայություններ: Տրամադրել խորհուրդներ և հիշեցումներ իրենց կողմից օգտագործվող բովանդակության բնույթի և տարիքին անհամապատասխանության վերաբերյալ:
	Ընկերությունը, որն առաջարկում է տեսալսողական և մուլտիմեդիա ծառայություններ, կարող է տրամադրել անձնական նույնականացման կոդ այն օգտատերերին, ովքեր ցանկանում են մուտք գործել բովանդակություն, որը կարող է վնասակար լինել երեխաների և երիտասարդների համար:
	Ապահովել ապրանքների և ծառայությունների գնագոյացման և օգտագործողների մասին հավաքագրված տեղեկատվության թափանցիկությունը: Համոզվեք, որ տվյալների հավաքագրման քաղաքականությունը համապատասխանում է երեխաների և երիտասարդների գաղտնիությանը վերաբերող համապատասխան օրենքներին, ներառյալ՝ արդյոք ծնողների համաձայնությունը պահանջվում է, նախքան առևտրային ձեռնարկությունները կարող են անձնական տվյալներ հավաքել երեխայից կամ երեխայի մասին:
	Համոզվել, որ գովազդը կամ առևտրային հաղորդակցությունը հստակորեն ճանաչելի են որպես այդպիսին: Վերահսկել առցանց հասանելի բովանդակությունը և հարմարեցնել այն օգտատերերի խմբերին, ովքեր, հավանաբար, հասանելիություն կունենան դրան՝ օրինակ՝ երեխաների և երիտասարդների համար առցանց գովազդի

	համար համապատասխան քաղաքականություն սահմանելով: Եթե առաջարկվող բովանդակությունն աջակցում է ինտերակտիվ տարրին, ինչպիսիք են մեկնաբանությունները, առցանց ֆորումները, սոցիալական ցանցերը, խաղային հարթակները, զրուցարանները կամ վեբ-ֆորումները, ներկայացրեք «տնային կանոնների» հստակ փաթեթը հաճախորդների համար հարմար լեզվով՝ ծառայության պայմանների և օգտատերերի ուղեցույցների շրջանակներում:
	Որոշեք, թե ինչ մակարդակի ներգրավվածություն է անհրաժեշտ առցանց ծառայություն սկսելուց առաջ: Երեխաներին գրավելուն ուղղված ծառայությունները պետք է ներկայացնեն միայն երիտասարդ լսարանի համար հարմար բովանդակություն: Եթե կասկածներ կան, կարող եք խորհրդակցել երեխաների պաշտպանության համար պատասխանատու ազգային մարմինների հետ:
	Տրամադրել հստակ և փաստացի բովանդակության պիտակավորում: Ուշադիր եղեք, որ օգտատերերը կարող են ստանալ ոչ պատշաճ բովանդակություն՝ հետևելով երրորդ կողմի կայքերի հղումներին, որոնք շրջանցում են համատեքստային էջերը:
Երեխաներին, ծնողներին և մանկավարժներին կրթել երեխաների անվտանգության և նրանց կողմից ՏՀՏ-ների պատասխանատու օգտագործման մասին	Համադրված թվային բովանդակություն առաջարկող ընկերությունները կարող են տեխնիկական միջոցները լրացնել երեխաների հնարավորությունները ընդլայնող կրթական միջոցառումներով՝ ձեռնարկելով հետևյալ գործողությունները:
	Հաճախորդներին տրամադրել բովանդակության մասին կոնկրետ և հստակ տեղեկատվություն, ինչպիսիք են՝ բովանդակության տեսակը, տարիքային վարկանիշները / սահմանափակումները, անպարկեշտ արտահայտությունները կամ

	բռնությունը և համապատասխան հասանելի ծնողական վերահսկողությունը, ինչպես նաև, թե ինչպես պետք է հաղորդել սխալ օգտագործման և անպատշաճ կամ անօրինական բովանդակության մասին և ինչպես պետք է վարվել այդ հաղորդումների հետ: Ինտերակտիվ աշխարհում այս տեղեկատվությունը պետք է տրամադրվի յուրաքանչյուր ծրագրի համար բովանդակային պիտակների տեսքով:
	Խրախուսեք մեծահասակներին, հատկապես ծնողներին, խնամակալներին և մանկավարժներին, մասնակցել երեխաների և երիտասարդների առցանց բովանդակության սպառմանը, որպեսզի նրանք կարողանան օգնել երեխաներին և երիտասարդներին բովանդակություն գտնելու ժամանակ ընտրության հարցում և առաջնորդել նրանց, ինչպես նաև օգնել սահմանել վարքագծի կանոններ: Օգնե՛ք երեխաներին (ինչպես նաև ծնողներին և խնամակալներին) սովորել կառավարել իրենց էկրանային ժամանակը և հասկանալ, թե ինչպես օգտագործել տեխնոլոգիան այնպես, որ նրանց հաճելի լինի, այդ թվում՝ երբ կանգ առնել և ինչ-որ այլ բանով զբաղվել:
	Ներկայացրե՛ք օգտագործման կանոնները հասկանալի և մատչելի լեզվով, որոնք խրախուսում են երեխաներին և երիտասարդներին լինել զգոն և պատասխանատու համացանցում «նավարկելիս» :
	Ստեղծե՛ք տարիքին համապատասխան գործիքներ, ինչպիսիք են ձեռնարկները և օգնության կենտրոնները: Աշխատեք առցանց կամ անձամբ կանխարգելման ծրագրերի և խորհրդատվական կենտրոնների հետ, երբ անհրաժեշտ է: Օրինակ, եթե վտանգ կա, որ երեխաները և երիտասարդները չափազանց ներգրավված

	են տեխնոլոգիայի մեջ, ինչը նրանց համար դժվարացնում է անձնական հարաբերություններ զարգացնելը կամ առողջ ֆիզիկական գործունեություն ծավալելը, կայքը կարող է տրամադրել հղում օգնության գծի կամ խորհրդատվական ծառայության համար: Անվտանգության մասին տեղեկությունները, ինչպիսիք են խորհուրդների հղումները, դարձրեք ակնառու, հեշտությամբ հասանելի և պարզ, երբ առցանց բովանդակությունը հավանաբար գրավում է երեխաների և երիտասարդների մեծ մասին:
	Առաջարկե՛ք ծնողական վերահսկողության գործիք, ինչպիսին է " կողպեքը", վերահսկելու բովանդակությունը, որը հասանելի է որոշակի բրաուզերի միջոցով:
	Համագործակցե՛ք ծնողների հետ՝ երաշխավորելու համար, որ երեխաների մասին համացանցում հայտնված տեղեկատվությունը նրանց վտանգի տակ չդնի: Այն, թե ինչպես են երեխաները նույնականացվում խմբագրությամբ մշակված բովանդակության մեջ, մանրակրկիտ քննարկում է պահանջում և կախված է համատեքստից: Ստացե՛ք երեխաների համաձայնությունը ծրագրերում, ֆիլմերում, տեսանյութերում ցուցադրելիս, որտեղ հնարավոր է, և հարգեք մասնակցություն չունենալու ցանկացած մերժում:
Թվային տեխնոլոգիաների խթանում՝ որպես հետագա քաղաքացիական ներգրավվածության միջոց	Համադրված թվային բովանդակություն առաջարկող ընկերությունները կարող են խրախուսել և հզորացնել երեխաներին և երիտասարդներին՝ աջակցելով նրանց մասնակցության իրավունքին հետևյալ գործողությունների միջոցով.
	Մշակե՛ք և/կամ առաջարկեք մի շարք բարձրորակ, դժվարին, կրթական, հաճելի և հետաքրքիր բովանդակություն, որը համապատասխանում է տարիքին և օգնում է երեխաներին և երիտասարդներին

	հասկանալ աշխարհը, որտեղ նրանք ապրում են: Բացի գրավիչ և օգտագործելի, հուսալի և անվտանգ լինելուց, նման բովանդակությունը կարող է նպաստել երեխաների և երիտասարդների ֆիզիկական, մտավոր և սոցիալական զարգացմանը՝ տրամադրելով զվարճանալու և կրթվելու նոր հնարավորություններ: Պետք է խրախուսվի այն բովանդակությունը, որը երեխաներին հնարավորություն է տալիս ընդունելու բազմազանությունը և լինել դրական օրինակ:

5.3 Առանձնահատկություն Գ. օգտվողների կողմից ստեղծված բովանդակության ցուցադրում և օգտատերերի միջև կապի հաստատում

Կար ժամանակ, երբ առցանց աշխարհում շատ էին մեծահասակները, բայց այժմ պարզ է, որ երեխաներն ու երիտասարդները բազմաթիվ հարթակներում հիմնական մասնակիցներն են՝ օգտատերերի կողմից ստեղծված բովանդակության ստեղծման և տարածման գործում: Այս ծառայության առանձնահատկությունն, ի թիվս այլոց, վերաբերում է սոցիալական մեդիայի ծառայություններին, հավելվածներին և կայքերին, որոնք առնչվում են ստեղծագործական գործունեությանը:

Ծառայությունները, որոնք կապում են օգտվողներին միմյանց հետ, կարելի է բաժանել երեք կատեգորիայի.

Հաղորդագրությունների փոխանակման հավելվածներ (Facebook Messenger, Groupme, Line, Tinder, Telegram, Viber, WhatsApp):

Սոցիալական ցանցերի ծառայություններ, որոնք թույլ են տալիս օգտատերերին կիսվել բովանդակությամբ և շփվել այլ օգտատերերի հետ իրենց ցանցերի ներսում և դրսում (Instagram, Facebook, SnapChat, TikTok):

Ուղիղ հեռարձակման հավելվածներ (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive):

Ծառայությունների մատակարարները պահանջում են նվազագույն տարիք՝ հարթակներում գրանցվելու համար, սակայն դա դժվար է ստուգել, քանի որ տարիքի ստուգումը կատարվում է օգտատիրոջ կողմից ներկայացված տվյալների հիման վրա: Ծառայությունների մեծ մասը, որոնք նոր օգտատերերին միմյանց հետ են կապում, նաև տեղորոշման փոխանակման գործառույթներ են թույլ տալիս: Այս ծառայություններից օգտվող երեխաները և երիտասարդները ավելի հաճախ են ենթարկվում անցանց վտանգներին:

Աղյուսակ 4-ը, *որը հարմարեցված է խոշորագույն սոցիալական ցանցերից մեկի կողմից կիրառվող կանոններին, ծառայություններ մատուցող ընկերություններին, որոնք տրամադրում են բովանդակությամբ կիսվելու, նոր միացող օգտատերերին ներառելու հնարավորություն, տրամադրում են ուղեցույց և առաջարկություններ այն քաղաքականության և գործողությունների վերաբերյալ, որոնք օգտատերերը կարող են ձեռնարկել՝ Համացանցում երեխաների պաշտպանության և երեխաների մասնակցության ակտիվացման համար:*

Աղյուսակ 4: ԵԱՊ ստուգաթերթ Գ առանձնահատկության համար: Օգտվողների կողմից ստեղծված բովանդակության ցուցադրում և օգտատերերի միջև կապի հաստատում

Երեխաների իրավունքների նկատառումների ինտեգրում բոլոր համապատասխան կորպորատիվ քաղաքականության և կառավարման գործընթացներում	Օգտատերերի կողմից ստեղծված բովանդակությամբ կիսվելու և օգտատերերի միջև կապ հաստատելու հնարավորություն ընձեռող ծառայությունները կարող են բացահայտել, կանխել և մեղմացնել ՏՀՏ-ների բացասական ազդեցությունը երեխաների և երիտասարդների իրավունքների վրա: Տրամադրել երեխաների և երիտասարդների իրավունքների առաջխաղացմանն աջակցելու հնարավորությունները:
	Տե՛ս աղյուսակ 1-ի ընդհանուր ուղեցույցները:
Ստանդարտ գործընթացների մշակում՝ ԵՍՇՆ-ի հետ աշխատելու համար	Համագործակցելով կառավարության, իրավապահ մարմինների, քաղաքացիական հասարակության և թեժ գծի կազմակերպությունների հետ, օգտատերերի կողմից ստեղծված բովանդակությամբ կիսվելու և օգտվողների միջև կապ հաստատելու հնարավորություն ընձեռող ընկերությունները կարող են առանցքային դեր խաղալ ԵՍՇՆ-ի դեմ պայքարում՝ կատարելով հետևյալ գործողությունները.
	Սահմանե՛լ ընթացակարգեր բոլոր կողմերի համար՝ արտակարգ իրավիճակների և սովորական հարցումների ժամանակ իրավապահներին անհապաղ օգնություն ցուցաբերելու համար:
	Նշե՛լ, որ ձեռնարկությունը լիովին կաջակցի իրավապահ մարմինների հետաքննությանը, եթե ապօրինի բովանդակություն հայտնվի կամ հայտնաբերվի: Տեղեկացնե՛լ այնպիսի տույժերի վերաբերյալ, ինչպիսիք են տուգանքները կամ վճարման արտոնությունների չեղարկումը:

	Աշխատե՛լ ներքին գործառույթների բարելավման վրա, ինչպիսիք են՝ հաճախորդների սպասարկումը, խարդախության կանխումը և անվտանգությունը, համոզվելու համար, որ ձեռնարկությունը կարող է կասկածելի անօրինական բովանդակության մասին հաղորդումներ ներկայացնել անմիջապես իրավապահ մարմիններին և թեժ գծերին:
	Օգտագործե՛լ ծառայության մատուցման պայմաններն ու դրույթները՝ արգելելու անօրինական բովանդակությունը և վարքագիծը՝ ընդգծելով, որ. • Չի՛ հանդուրժվի վնասակար բովանդակությունը՝ ներառյալ կոնտակտային կամ ոչ կոնտակտային չարաշահման մտադրությամբ երեխաների գրումինգի կասկածանքները • Չի՛ հանդուրժվի անօրինական բովանդակությունը՝ ներառյալ ԵՍՇՆ-ի վերբեռնումը կամ հետագա տարածումը • Ընկերությունը կանդրադառնա և լիովին կհամագործակցի իրավապահ մարմինների հետաքննության հետ, եթե հայտնվի կամ հայտնաբերվի անօրինական բովանդակություն, կամ՝ երեխաների պաշտպանության քաղաքականության որևէ խախտում:
	Փաստաթղթավորե՛լ ԵՍՇՆ-ի հետ աշխատելու ընկերության փորձը՝ սկսած մոնիտորինգից՝ ընդլայնելով մինչև բովանդակության վերջնական փոխանցումը և ոչնչացումը: Փաստաթղթում ներառե՛լ այն անձնակազմի ցուցակը, որը պատասխանատու է նյութի հետ աշխատելու համար:

	Ընդունել օգտատերերի կողմից ստեղծված բովանդակության սեփականության իրավունքի վերաբերյալ քաղաքականություն՝ ներառյալ օգտատիրոջ խնդրանքով օգտատիրոջ ստեղծած բովանդակությունը հեռացնելու տարբերակը: Հեռացրեք բովանդակությունը, որը խախտում է ծառայություն մատուցողի քաղաքականությունը և զգուշացրե՛ք նյութը հրապարակած օգտատիրոջը խախտման մասին:
Ստանդարտ գործընթացների մշակում ԵՍՇՆ-ի հետ աշխատելու համար (շարունակություն)	Նշել, որ օգտատիրոջ կողմից ընդունելի օգտագործման կանոններին չհամապատասխանելը կունենա հետևանքներ, այդ թվում՝ • բովանդակության հեռացում, նրանց էջերի, կայքի կասեցում կամ փակում, • որոշակի տեսակի բովանդակություն կիսելու կամ որոշակի հատկանիշներ օգտագործելու հնարավորության չեղարկում, • երեխաների հետ շփվելու կանխարգելում, • խնդիրների դեպքում տվյալների՝ իրավապահներին փոխանցում
Երեխաների նկատմամբ սեռական բռնության նյութերի հետ աշխատելու ստանդարտ գործընթացների մշակում	Խթանել ԵՍՇՆ-ի կամ որևէ այլ անօրինական բովանդակության վերաբերյալ հաղորդում/բողոք ներկայացնելու մեխանիզմները և համոզված լինել, որ օգտատերերը գիտեն, թե ինչպես պետք է հաղորդում/բողոք ներկայացնեն ոչ պատշաճ բովանդակության հայտնաբերման դեպքում: Կառուցե՛ք համակարգեր,տրամադրեք վերապատրաստված անձնակազմ՝ խնդիրները յուրաքանչյուր դեպքի հիման վրա գնահատելու և համապատասխան գործողություններ ձեռնարկելու համար: Ստեղծե՛ք համապարփակ և լավ ռեսուրսներով օպերատիվ թիմեր՝ օգտատերերի աջակցության համար: Անհրաժեշտ է, որ այս թիմերը վերապատրաստվեն տարբեր միջադեպերի հանդիպելու դեպքում արագ, համարժեք արձագանք և համապատասխան գործողություններ ձեռնարկելու համար: Երբ օգտատերը բողոք է ներկայացնում, միջադեպի

	տեսակից կախված, այն պետք է փոխանցվի համապատասխան փորձառությունն ունեցող անձնակազմին: Ընկերությունը կարող է նաև ստեղծել հատուկ թիմեր՝ օգտատերերի բողոքարկումները լուծելու համար, այն դեպքերում, երբ հաղորդումը/բողքը կարող է սխալմամբ ներկայացվել:
	Գործընթացներ կիրառե՛ք՝ անհապաղ հեռացնելու կամ արգելափակելու մուտքը դեպի ԵՍՇՆ՝ ներառյալ ծանուցման և հեռացման գործընթացները՝ ապօրինի բովանդակությունը բացահայտվելուն պես հեռացնելու համար: Համոզվե՛ք, որ երրորդ կողմերի մոտ էլ, որոնց հետ ընկերությունը պայմանագրային հարաբերություններ ունի, նմանապես հաստատուն ծանուցման և հեռացման գործընթացներ են գործում: Եթե օրենսդրությունը թույլ է տալիս, ապա հետաքննության դեպքում նյութը կարող է պահվել որպես հանցագործության ապացույց:
	Մշակե՛ք տեխնիկական համակարգեր, որոնք կարող են հայտնաբերել անօրինական բովանդակություն, կանխել դրա վերբեռնումը կամ մշակել այն՝ ընկերության անվտանգության թիմի կողմից անհապաղ վերանայման համար: Ձեռնարկե՛ք համապատասխան բոլոր միջոցները՝ ծառայությունները չարաշահումից պաշտպանելու՝ վերբեռնելու, տարածելու կամ ԵՍՇՆ ստեղծելու համար: Հնարավորության դեպքում ստեղծե՛ք պրոակտիվ տեխնիկական միջոցներ՝ վերլուծելու պրոֆիլի հետ կապված օբյեկտները և մետատվյալները՝ հանցավոր վարքագիծը կամ օրինաչափությունները հայտնաբերելու և համապատասխան գործողություններ ձեռնարկելու համար:

	Եթե հավելվածը կամ ծառայությունը հաճախորդներին թույլ է տալիս վերբեռնել և պահել լուսանկարներ՝ ընկերությանը պատկանող կամ շահագործվող սերվերների վրա, ապա իրականացվեն գործընթացներ և գործիքներ՝ բացահայտելու լուսանկարները, որոնք, ամենայն հավանականությամբ, պարունակում են ԵՍՇՆ: Մտածե՛ք նույնականացման պրոակտիվ մեթոդներ, ինչպիսիք են սկանավորման տեխնոլոգիան կամ մարդու կողմից ստուգումը:
Ավելի անվտանգ և տարիքին համապատասխան առցանց միջավայրի ստեղծում	Ծառայությունների մատակարարները, որոնք առաջարկում են օգտատերերի կողմից ստեղծված բովանդակություն և կապում են օգտատերերին, կարող են օգնել ստեղծել ավելի ապահով, ավելի հաճելի թվային միջավայր բոլոր տարիքի երեխաների համար՝ կատարելով հետևյալ գործողությունները:
	Ծառայության պայմանների և օգտատերերի ուղեցույցների շրջանակներում հաղորդակցվե՛լ հաճախորդներին հարմար լեզվով՝ «տնային կանոնների» հստակ փաթեթով, որը սահմանում է • ծառայության բնույթը և այն, ինչ ակնկալվում է դրա օգտագործողներից. • ինչն է ընդունելի և անընդունելի բովանդակության, վարքի և լեզվի, ինչպես նաև անօրինական օգտագործման արգելման առումով • ցանկացած խախտման հետևանքները, օրինակ՝ իրավապահ մարմիններին հայտնելը և օգտատիրոջ կայքի կասեցումը:
	Հիմնական անվտանգության և իրավական հաղորդագրությունները պետք է ներկայացվեն տարիքին համապատասխան ձևաչափով (այսինքն՝ օգտագործելով ինտուիտիվ պատկերներ և խորհրդանիշներ) ինչպես գրանցման ժամանակ, այնպես էլ հետագայում, քանի որ կայքում տարբեր գործողություններ են կատարվում:

	Հեշտացրե՛ք օգտատերերի նկատմամբ չարաշահումների մասին մտահոգությունների մասին հայտնելը՝ կիրառելով ստանդարտ և մատչելի գործընթացներ տարբեր մտահոգությունների դեմ պայքարելու համար, ինչպիսիք են անցանկալի հաղորդակցությունները (սփամ, ահաբեկում) կամ անպատշաճ բովանդակություն տեսնելը:
	Տրամադրե՛ք տարիքին համապատասխան բովանդակության համօգտագործման և տեսանելիության կարգավորումներ: Օրինակ՝ երեխաների և երիտասարդների համար գաղտնիության և տեսանելիության կարգավորումները դարձրե՛ք ավելի սահմանափակող, քան մեծահասակների համար:
	Կիրառե՛լ նվազագույն տարիքային պահանջներ, աջակցել տարիքի ստուգման նոր համակարգերի հետազոտմանը և զարգացմանը: Օրինակ՝ կենսաչափությունը՝ օգտագործելով նման գործիքների մշակման համար հայտնի միջազգային ստանդարտները: Քայլեր ձեռնարկե՛ք՝ հայտնաբերելու և հեռացնելու անչափահաս օգտատերերին, ովքեր սխալ են ներկայացրել իրենց տարիքը՝ հասանելիություն ստանալու համար: Եթե արդեն գոյություն չունի, ստեղծե՛ք մուտքի համապատասխան գործընթացներ՝ որոշելու համար, թե արդյոք օգտվողները բավականաչափ մեծ են բովանդակություն կամ ծառայություն մուտք գործելու համար՝ առանց վտանգելու նրանց ինքնությունը, գտնվելու վայրը և անձնական տվյալները: Օգտագործե՛ք ազգային հաստատված տարիքի ստուգման ֆունկցիոնալ համակարգերը՝ երեխաների տվյալների գաղտնիությունն ապահովելու նպատակով:
Ավելի անվտանգ և տարիքին համապատաս-	Պաշտպանե՛ք երիտասարդ օգտատերերին անցանկալի հաղորդակցությունից և համոզվե՛ք, որ գաղտնիության և տեղեկատվության հավաքագրման ուղեցույցները գործում են:

խան առցանց միջավայրի ստեղծում (շարունակություն)	Գտե՛ք լուսանկարները ու տեսանյութերը ստուգելու, ոչ պատշաճները հայտնաբերելու դեպքում՝ ջնջելու եղանակներ: Հայտնի պատկերների հեշ սկանավորումը և լուսանկարների ճանաչման ծրագրակազմը գործիքներ են, որոնք կարող են օգնել այդ հարցում: Երեխաներին ուղղված ծառայություններում լուսանկարներն ու տեսանյութերը կարող են նախապես ստուգվել՝ համոզվելու համար, որ երեխաները չեն հրապարակում իրենց կամ ուրիշների մասին անձնական գաղտնի տեղեկություններ:
	Մի շարք միջոցներ կարող են օգտագործվել օգտատերերի կողմից ստեղծված բովանդակության հասանելիությունը վերահսկելու, երեխաներին և երիտասարդներին առցանց ոչ պատշաճ կամ անօրինական բովանդակությունից պաշտպանելու համար: Համոզվե՛ք, որ խաղերում և սոցիալական մեդիայի այլ կարգավորումներում օգտագործվում են անվտանգ գաղտնաբառեր՝ երեխաներին և երիտասարդներին պաշտպանելու համար: Այլ տեխնիկաները ներառում են՝ • Ստուգե՛լ քննարկման խմբերը՝ բացահայտելու ոչ պատշաճ թեման, ատելության խոսքն ու անօրինական վարքագիծը: Ջնջե՛լ այդպիսի բովանդակությունը, եթե պարզվում է, որ այն խախտում է օգտագործման պայմանները. • Գործիքների մշակում՝ ակտիվորեն փնտրելու և հեռացնելու բովանդակություն, որն անօրինական է կամ խախտում է ընկերության պայմաններն ու սպասարկման դրույթները, ինչպես նաև՝ կանխելու ոչ պատշաճ, անօրինական բովանդակության վերբեռնումը կայք: • Հաղորդագրությունների տախտակների նախնական մոդերավորում՝ երեխաների և երիտասարդների հետ աշխատանքում

	մասնագիտացած մոդերատորների թիմի հետ, որոնք ստուգում են այն բովանդակությունը, որը հակասում է հրապարակված «տան կանոններին»: Յուրաքանչյուր հաղորդագրություն կարող է ստուգվել նախքան այն հրապարակելը, և մոդերատորները կարող են նաև նկատել, նշել կասկածելի օգտատերերին: • Ստեղծե՛լ խմբերի պատասխանատու թիմեր, որոնք ծառայում են որպես մոդերատորների շփման առաջին կետ, երբ նրանք օգտատիրոջ հետ կապված մտահոգություններ են հայտնում:
	Պատասխանատու եղե՛ք կոմերցիոն բովանդակության ստուգման համար՝ ներառյալ ֆորումներում, սոցիալական ցանցերում և խաղային կայքերում: Իրականացրե՛ք համապատասխան չափորոշիչներ և կանոններ՝ երեխաներին տարիքին անհամապատասխան գովազդից պաշտպանելու, երեխաների և երիտասարդների համար առցանց գովազդի հստակ սահմաններ սահմանելու համար:

Երեխաների, ծնողների և մանկավարժների ուսուցում՝ երեխաների անվտանգության և նրանց կողմից ՏՀՏ-ների պատասխանատու օգտագործման մասին	Ծառայությունների մատակարարները, որոնք առաջարկում են օգտատերերի կողմից ստեղծված բովանդակություն, կարող են իրականացնել տեխնիկական միջոցառումներ կրթական հզորացման գործողություններով՝ կատարելով հետևյալ գործողությունները.
	Ստեղծե՛ք բաժին՝ նվիրված անվտանգության խորհուրդներին, հոդվածներին, առանձնահատկություններին և թվային քաղաքացիության մասին երկխոսությանը, ինչպես նաև՝ երրորդ կողմի փորձագետների օգտակար բովանդակության հղումներին: Անվտանգության խորհուրդները պետք է տեղադրված լինեն հեշտ հասանելի տեղում և տրվեն հեշտ հասկանալի լեզվով: Պլատֆորմ մատակարարողներին նաև խրախուսվում է ունենալ միատեսակ նավիգացիոն ինտերֆեյս տարբեր սարքերում, ինչպիսիք են համակարգիչները, պլանշետները կամ բջջային հեռախոսները:
	Ծնողներին տրամադրե՛ք առկա բովանդակության և ծառայությունների տեսակների մասին հստակ տեղեկատվություն: Օրինակ՝ տեղեկատվություն սոցիալական ցանցերի, օգտատիրոջ գտնվելու վայրի մասին, ինչպես է համացանցին հասանելիությունը ապահովում շարժական սարքերի միջոցով, ծնողների համար հասանելի տարբերակները՝ վերահսկման միջոցներ կիրառելու համար:

	Տեղեկացրե՛ք ծնողներին, թե ինչպես պետք է հաղորդել չարաշահումների, շահագործումների, անպատշաճ կամ անօրինական բովանդակության մասին և այն մասին, թե ինչ է տեղի ունենալու հաղորդում ներկայացնելու դեպքում: Տեղեկացրե՛ք նրանց, թե որ ծառայություններն են տարիքային սահմանափակում ունեցող, ինտերակտիվ ծառայություններից օգտվելիս անվտանգ և պատասխանատու վարք դրսևորելու այլ եղանակների մասին:
	Ստեղծե՛ք «վստահության և հեղինակության» վրա հիմնված համակարգ՝ լավ վարքագիծը խրախուսելու և հասակակիցներին հնարավորություն տալու սեփական օրինակով միմյանց փոխանցելու լավագույն փորձը: Խթանե՛լ սոցիալական շփումների կարևորությունը, որոնք մարդկանց թույլ են տալիս կապ հաստատել այլ օգտատերերի, վստահելի ընկերների հետ՝ օգնելու լուծել կոնֆլիկտը կամ զրույց սկսել անհանգստացնող բովանդակության մասին:
	Տրամադրե՛լ խորհուրդներ և հիշեցումներ տվյալ ծառայության կամ բովանդակության բնույթի և այն անվտանգ օգտագործելու մասին: Ներառե՛ք համայնքի համար նախատեսված ուղեցույցներն ինտերակտիվ ծառայությունների մեջ: Օրինակ՝ էկրանին հայտնվող հաղորդագրություններով, որոնք հիշեցնում են օգտատերերին համապատասխան և անվտանգ վարքագծի մասին, խորհուրդ տալով չհրապարակե՛լ իրանց կոնտակտային տվյալները:
	Համագործակցե՛ք ծնողների հետ և ուղղորդե՛ք նրանց՝ համոզվելու, որ երեխաների մասին համացանցում հայտնված տեղեկատվությունը նրանց վտանգի տակ չի դնում: Ստացե՛ք երեխաների հստակ համաձայնությունը, երբ ցուցադրում եք իրենց կողմից ստեղծված բովանդակությունը, որտեղ պետք է հարգեք ցանկացած մերժում:

Խթանե՛լ թվային տեխնոլոգիաները՝ որպես քաղաքացիական ներգրավվածության միջոց	Օգտատերերի կողմից ստեղծված բովանդակություն առաջարկող ծառայությունները կարող են խրախուսել և հզորացնել երեխաներին և երիտասարդներին՝ խրախուսելով նրանց մասնակցային իրավունքը:
	Տե՛ս աղյուսակ 1-ի ընդհանուր ուղեցույցները:

5.4 Առանձնահատկություն Դ. Արհեստական բանականության վրա հիմնված համակարգեր

Խորը ուսուցման տեխնոլոգիաներին տրվող մեծ ուշադրությունից հետո «արհեստական բանականություն», «մեքենայական ուսուցում» և «խորը ուսուցում» տերմինները փոխադարձաբար օգտագործվում են հանրության կողմից՝ արտացոլելու մեքենաներում՝ «խելացի» վարքագծի վերարտադրման հայեցակարգը: Այս բաժնում մենք կենտրոնանում ենք այն ուղիների վրա, որոնցով մեքենայական ուսուցումը և խորը ուսուցման գործընթացներն ազդում են երեխաների կյանքի, նրանց իրավունքների վրա:

«Վերջին մի քանի տարիների ընթացքում արհեստական բանականության վրա հիմնված տեխնոլոգիաների էքսպոնենցիալ առաջընթացի պատճառով՝ երեխաների իրավունքները պաշտպանող ներկայիս միջազգային շրջանակը բացահայտորեն չի անդրադառնում արհեստական բանականության մշակման և կիրառման արդյունքում առաջացած բազմաթիվ խնդիրների: Այնուամենայնիվ, այն բացահայտում է մի քանի իրավունքներ, որոնք կարող են ազդել այս տեխնոլոգիաների վրա: Հետևաբար՝ կարևոր մեկնարկային կետ է ցանկացած վերլուծության համար. ինչպես կարող են երեխաների իրավունքների վրա դրական կամ բացասաբար ազդել նոր տեխնոլոգիաները, ինչպիսիք են գաղտնիության, կրթության, խաղալու իրավունքները և անխտրական վարքագիծը»:[26]

ԱԲ-ի կիրառումը կարող է ազդեցություն ունենալ երեխաների վրա, տարբեր ծառայությունների տեսքով, որոնք օգտագործվում են սոցիալական ցանցերում, ինչպիսիք են տեսանյութերի ցուցադրման հարթակները: Մեքենայական ուսուցման ալգորիթմները՝ օրինակ՝ առաջարկությունների շարժիչը, որը հիմնականում օգտագործվում է տեսանյութերի փոխանակման հանրաճանաչ հարթակներում, օպտիմիզացված են՝ որոշակի ժամանակահատվածում որոշակի տեսանյութերի առավելագույն դիտում ապահովելու համար:[27]

Սենսորային էկրանի տեխնոլոգիան և այս հարթակների դիզայնը թույլ են տալիս շատ փոքր երեխաներին թերթել և ծանոթանալայս բովանդակությունը: Հատկապես մտահոգություն կա, որ ալգորիթմները, որոնք օգտագործում են առաջարկվող տեսանյութերը, կարող են երեխաներին գցել թակարդը՝ վատ կամ ոչ պատշաճ բովանդակության «ֆիլտրի փուչիկների» մեջ: Քանի որ երեխաները հատկապես հետևում են բովանդակությանը, «ցնցող տեսանյութերը» կարող են գրավել նրանց ուշադրությունը և հեռացնել երեխաներին հարմար միջավայրից:[28]

---

26 ՅՈՒՆԻՍԵՖ և Բերքլիի համալսարան, «Executive Summary: Artificial Intelligence and Children's Rights», 2018.
27 Ibid.
28 Ibid.

ԱԲ-ն նաև ազդում է երեխաների առցանց պաշտպանության վրա՝ կապված խելացի խաղալիքների հետ: Խելացի խաղալիքների շահագործման հետ կապված հստակ գործընթացներն ունեն իրենց մարտահրավերները, օրինակ՝ խաղալիքը (որը կապվում է երեխայի հետ), բջջային հավելվածը, որը գործում է որպես մուտքի կետ Wi-Fi կապի համար, և սպառողի անհատականացված առցանց հաշիվը, որտեղ պահվում են տվյալները: Նման խաղալիքները կապված են ամպային համակարգի սերվերների հետ, որոնք պահում և մշակում են խաղալիքի հետ շփվող երեխաների տրամադրած տվյալները: Այս մոդելի դեպքում առկա են գաղտնիության հետ կապված մտահոգություններ: Եթե անվտանգությունը չի կիրառվում յուրաքանչյուր շերտում, ինչը ցույց են տվել հակերության բազմաթիվ դեպքերը, որոնցում անձնական տվյալները արտահոսել են: Ավելին՝ կոտրված սարքերից մի քանիսը (ներառյալ խելացի վեբ սարքերը, ինչպիսիք են մանկական մոնիտորները, ձայնային օգնականները և այլն) կարող են օգտագործվել՝ օգտատերերին հսկողության տակ պահելու համար՝ առանց նրանց իմացությունը կամ համաձայնությունը ստանալու:

Այս սարքերն օգտագործող երեխաների դեմ հայտնաբերված սպառնալիքներին արձագանքման մեխանիզմներ ինտեգրելիս, օրինակ՝ հայտնաբերված վարքագծի վրա հիմնված խորհուրդներ և առաջարկություններ տրամադրելով (ինչպես ավելի վաղ նշվել է BBC Own It հավելվածի հետ), շատ կարևոր է, որ խելացի սարքերը նախագծող ընկերությունները մշակեն այս առաջարկությունները՝ խորհրդակցելով երեխաների իրավունքների պաշտպանության հարցերով զբաղվող փորձագետների հետ:

Թեև որոշ ընկերություններ առաջ են քաշում արհեստական բանականության էթիկական օգտագործման սկզբունքները, պարզ չէ, թե արդյոք գոյություն ունեն ԱԲ-ի[29] և երեխաների դեմ ուղղված հանրային քաղաքականության մեխանիզմներ:[30] Մի քանի տեխնոլոգիական և առևտրային ասոցիացիաներ և համակարգչային գիտության խմբեր մշակել են էթիկական սկզբունքներ ԱԲ-ի հետ կապված:[31] Այնուամենայնիվ, դրանք բացահայտորեն չեն վերաբերում երեխաների իրավունքներին, այն եղանակներին, որոնցով այս ԱԲ տեխնոլոգիաները կարող են ռիսկեր ստեղծել երեխաների համար, կամ՝ դրանք մեղմելու նախաձեռնողական ծրագրերին:
«Կորպորացիաների նման՝ ամբողջ աշխարհի կառավարությունները ևս որդեգրել են ռազմավարություններ՝ ԱԲ-ի զարգացման և կիրառմանառաջատարներ դառնալու համար»:[31]

29 Տե՛ս Մայքրոսոֆթի, "Salient Human Rights Issues", Report - FY17; և Գուգլի, "Responsible Development of AI" (2018).
30 Մայքրոսոֆթի պաշտոնական բլոգ, "The Future Computed: Artificial Intelligence and its role in society", 2018.
31 Ibid

Այնուամենայնիվ, պարզ չէ, թե ինչպես են նման ազգային ռազմավարություններն ուղղակիորեն վերաբերում երեխաների իրավունքներին:

Բարելավե՛լ Ֆեյսբուքի կողմից ինքնասպանությունների և ինքնավնասումների հետ կապված բովանդակության կառավարումը 2019-ին Ֆեյսբուքը սկսեց կանոնավոր խորհրդակցություններ անցկացնել աշխարհի տարբեր երկրների փորձագետների հետ՝ քննարկելու ինքնասպանության և ինքնավնասման հետ կապված ավելի բարդ թեմաներ: Դրանք ներառում են, թե ինչպես վարվել ինքնասպանության վերաբերյալ գրառումների, դեպրեսիվ բովանդակության ռիսկերի և ինքնասպանության դրդող նյութերի հետ: Այս հանդիպումների լրացուցիչ մանրամասները հասանելի են Ֆեյսբուքի՝ Անվտանգության կենտրոնի ինքնասպանությունների կանխարգելման նոր էջում: Այս խորհրդատվությունները հանգեցրին մի քանի բարելավումների, թե ինչպես է Ֆեյսբուքը կառավարում այս տեսակի բովանդակության տարածումը: Օրինակ՝ ինքնավնասման ինքնավնասմանհետ կապված քաղաքականությունը ամրապնդվել է՝ արգելելու գրաֆիկական կտրող պատկերները՝ ակամա ինքնավնասումը խթանելուց կամ հրահրելուց խուսափելու համար: Նույնիսկ այն դեպքում, երբ ինչ-որ մեկը փնտրում է աջակցություն կամ պատմում է վնասվածք ստանալուց հետո վերականգնման փուլի մասին, Ֆեյսբուքըցուցադրում է զգայունության էկրան՝ ինքնավնասումից ապաքինված կտրվածքների լուսանկարների վրա: Բովանդակության այս տեսակն այժմ հայտնաբերվում է արհեստական բանականության կիրառման միջոցով, որի շնորհիվ հնարավոր վնասակար նյութերի հետ կապված գործողությունները՝ ներառյալ դրանք հեռացնելը կամ զգայուն էկրաններ ավելացնելը, կարող են մեխանիկորեն իրականացվել: 2019 թվականի ապրիլից հունիս ամիսները Ֆեյսբուքն իր կայքում ու սումնասիրել է ավելի քան 1,5 միլիոն ինքնասպանության և ինքնավնասման բովանդակություն: Նախքան օգտատերերի կողմից հաղորդում ստանալը բացահայտել է դրանց ավելի քան 95 տոկոսը: Այդ նույն ժամանակահատվածում Instagram-ն ուսումնասիրել է ավելի քան 800 հազար նմանատիպ բովանդակություն, որոնցից ավելի քան 77 տոկոսը հայտնաբերվել է նախքան օգտատերերի կողմից հաղորդվելը:

Իրական ժամանակում պոտենցիալ բուլինգի կամ հասակակիցների կողմից բռնության բացահայտման, օգտատերերին հաղորդագրություններ ուղարկելու մասին Instagram-ը տեղադրում է արհեստական բանականություն՝ արմատախիլ անելու այնպիսի վարքագծի դեպքեր, ինչպիսիք են վիրավորանքները, ամոթանքը և անհարգալից վերաբերմունքը: Օգտագործելով հաղորդման բարդ գործիքներ՝ մոդերատորները կարող են արագ փակել առցանց ահաբեկչության հեղինակին պատկանող էջը:

Լավ փորձ: Արհեստական բանականության օգտագործումը երեխաների սեռական բռնության նյութերի նույնականացման գործում

Երեխաների շահագործման դեմ պայքարում հիմնվելով Microsoft-ի՝ PhotoDNA-ի մեծ ներդրման վրա և Google Content Safety API-ի՝ վերջերս գործարկելու վրա, ֆեյսբուքը մշակել է նաև տեխնոլոգիաներ՝ երեխաների նկատմամբ սեռական բռնության բովանդակությունը հայտնաբերելու համար:

Այս տեխնոլոգիաները, որոնք հայտնի են որպես PDQ և TMK+PDQF, գործիքների փաթեթի մի մասն են, որոնք Ֆեյսբուքն օգտագործում է վնասակար բովանդակությունը հայտնաբերելու համար: Ոլորտին հասանելի այլ ալգորիթմներ և գործիքներ ներառում են pHash, aHash և dHash: Ֆեյսբուքի լուսանկարների համընկնման ալգորիթմը՝ PDQ, ոգեշնչված է pHash-ի կողմից, չնայած այն ի սկզբանե ստեղծվել է որպես առանձին ալգորիթմ՝ անկախ ծրագրային ապահովման ներդրմամբ:

Տեսանյութի համադրման տեխնոլոգիան՝ TMK + PDQF - ը, համատեղ մշակվել է Ֆեյսբուքի Արհեստական Բանականության հետազոտական խմբի, Մոդենայի ու Ռեջո Էմիլիայի համալսարանների գիտնականների կողմից՝ Իտալիայում:

Այս տեխնոլոգիաները ստեղծում են ֆայլերի պահպանման արդյունավետ միջոց՝ կարճ թվային հեշերի տեսքով, որոնք կարող են որոշել, թե արդյոք երկու ֆայլերը նույնն են կամ նման, նույնիսկ եթե նախնական լուսանկարը կամ տեսանյութն առկա չէ: Հեշերը նաեւ ավելի հեշտ է կիսել այլ ընկերությունների եւ ոչ առեւտրային կազմակերպությունների հետ:

PDQ-ն և TMK+PDQF-ը նախագծվել են բարձր մասշտաբով աշխատելու համար՝ աջակցելով վիդեո շրջանակների հաշինգին և իրական ժամանակի հավելվածներին:

Արհեստական բնականության վրա հիմնված որոշումների մշակման, իրականացման խնդիրներում՝ սկզբունքների համաձայնեցման վերաբերյալ, ձեռնարկություններին որոշ առաջարկություններ են ներկայացված *Աղյուսակ 5*-ում:

Առաջարկությունները հիմնված են ՅՈՒՆԻՍԵՖ-ի՝ արհեստական բանականության և երեխաների վերաբերյալ գլոբալ քաղաքականության ուղեցույցի մշակման վրա, որն ուղղված կլինի կառավարություններին և արդյունաբերությանը: Խնդրում ենք այցելել https://www.unicef.org/globalinsight/featured-projects/ai-children կայք՝ ծրագրի մասին լրացուցիչ տեղեկությունների համար: Առաջարկությունները նաև ներառում են ՅՈՒՆԻՍԵՖ-ի և Բերքլիի համալսարանի՝ ԱԲ-ի և երեխաների իրավունքների մասին փաստաթղթի հիմնադրույթները:[32]

32 UNICEF and UC Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.

Աղյուսակ 5. ԵԱՊ ստուգաթերթ՝ Դ առանձնահատկության համար. ԱԲ-ի վրա հիմնված համակարգեր

Երեխաների իրավունքների ինտեգրում՝ համապատասխան կորպորատիվ քաղաքականության և կառավարման գործընթացներում	ԱԲ-ի վրա հիմնված համակարգերի մատակարարները կարող են բացահայտել, կանխել և մեղմացնել ՏՀՏ-ների բացասական ազդեցությունը երեխաների և երիտասարդների իրավունքների վրա: Բացահայտե՛լ երեխաների և երիտասարդների իրավունքների առաջխաղացմանն աջակցելու հնարավորությունները:
	ԱԲ համակարգերը պետք է նախագծվեն, մշակվեն, ներդրվեն և հետազոտվեն՝ հարգելու, խթանելու և իրականացնելու երեխաների իրավունքներն, ինչպես ամրագրված է Երեխայի իրավունքների մասին կոնվենցիայում: ԱԲ համակարգերը պետք է օգտագործվեն այս հարցում առավելագույնս աջակցելու համար:
	Օգտագործե՛ք ներառական դիզայնի մոտեցում՝ երեխաներին առնչվող ապրանքներ մշակելիս, որոնք առավելագույնի են հասցնում գենդերային, աշխարհագրական և մշակութային բազմազանությունը: Ներառում են շահագրգիռ կողմերի լայն շրջանակ, ինչպիսիք են ծնողները, ուսուցիչները, մանկական հոգեբանները և, անհրաժեշտության դեպքում, հենց երեխաները:
	Կառավարման շրջանակները՝ ներառյալ էթիկական ուղեցույցները, օրենքները, չափորոշիչները և կարգավորող մարմինները, պետք է ստեղծվեն՝ վերահսկելու գործընթացները, որոնք երաշխավորում են, որ ԱԲ համակարգերի կիրառումը չի խախտում երեխաների իրավունքները:

Ստանդարտ գործընթաց-ների մշակում ԵՍԾՆ-ի հետ աշխատելու համար	Համագործակցելով կառավարության, իրավապահ մարմինների, քաղաքացիական հասարակության և թեժ գծի կազմակերպությունների հետ, ԱԲ-ի վրա հիմնված համակարգերի մատակարարները առանցքային դեր են խաղում ԵՍԾՆ-ի դեմ պայքարում՝ ձեռնարկելով հետևյալ գործողությունները.
	Տե՛ս աղյուսակ 1-ի ընդհանուր ուղեցույցները.
Ավելի անվտանգ և տարիքին համապատաս-խան առցանց միջավայրի ստեղծում	ԱԲ-ի վրա հիմնված համակարգերի մատակարարները կարող են օգնել ստեղծել ավելի ապահով և հաճելի թվային միջավայր բոլոր տարիքի երեխաների համար՝ կատարելով հետևյալ գործողությունները.
	Երեխաների վրա ազդող տեխնոլոգիաներ մշակելիս՝ որդեգրե՛լ բազմակողմանի մոտեցում և խորհրդակցել քաղաքացիական հասարակության՝ ներառյալ ակադեմիական շրջանակների հետ: Բացահայտե՛լ այս տեխնոլոգիաների հնարավոր ազդեցությունները պոտենցիալ վերջնական օգտագործողների բազմազան շրջանակի իրավունքների վրա:
	Իրականացնե՛լ դիզայնի անվտանգություն և դիզայնի գաղտնիություն՝ երեխաների համար նախատեսված այն ապրանքների և ծառայությունների համար, որոնք սովորաբար օգտագործվում են նրանց կողմից:
	Քանի որ ԱԲ համակարգերը տվյալների կարիք ունեն, իրենց ծառայությունների համար ԱԲ օգտագործող ընկերությունները պետք է հատուկ զգոնություն ցուցաբերեն երեխաների անձնական տվյալների հավաքագրման, մշակման, պահպանման, վաճառքի և հրապարակման խնդիրներին: ԱԲ համակարգերը պետք է թափանցիկ լինեն այն իմաստով, որ պետք է հայտնաբերվի, թե ինչպես և ինչու է համակարգը այս կամ այն

	որոշումը կայացրել, ռոբոտի դեպքում՝ ինչու է այդպես վարվել: Նման թափանցիկությունը կարևոր է վստահության ամրապնդման և աուդիտի, հետաքննության և օգնության դիմելու համար՝ երեխաներին վնաս պատճառելու կասկածանքով: Համոզվե՛լ, որ գոյություն ունեն ֆունկցիոնալ և իրավաբանական մեխանիզմներ՝ դատարան դիմելու համար, եթե երեխաներին վնաս է հասցվել կամ նրանք պնդում են, որ իրենց վնաս է հասցվել ԱԲ համակարգերի միջոցով : Անհրաժեշտ է մշակել ընթացակարգեր՝ ցանկացած խտրական հետևանքների՝ ժամանակին վերացման համար, ինչպես նաև ստեղծել վերահսկող մարմիններ՝ բողոքարկումների քննության և երեխաների անվտանգության, պաշտպանության մշտական մոնիթորինգի համար: Վնասի հատուցման հաշվետվողականությունն ու մեխանիզմները գործում են ձեռք ձեռքի տված:
	Հատկապես գաղտնի տվյալների հետ աշխատելու պլաններ մշակե՛ք՝ ներառյալ չարաշահումների կամ այլ վնասների բացահայտումները, որոնք կարող են կիսվել ընկերության հետ իր արտադրանքի միջոցով: Թվային հարթակները և ԱԲ համակարգերը պետք է նվազագույնի հասցնեն երեխաների վերաբերյալ տվյալների հավաքագրումը և առավելագույնի հասցնեն երեխաների վերահսկողությունը՝ նրանց ստեղծած տվյալների նկատմամբ: Օգտագործման պայմանները պետք է հասկանալի լինեն երեխաների համար՝ նրանց իրազեկությունը և լիազորությունները զարգացնելու համար:

Երեխաների, ծնողների և մանկավարժների կրթումը՝ երեխաների անվտանգության և նրանց կողմից ՏՀՏ-ների պատասխանատու օգտագործման մասին	Արհեստական բանականության կողմից կառավարվող համակարգերի մատակարարները կարող են տեխնիկական միջոցները լրացնել կրթության և հնարավորությունների ընդլայնման միջոցառումներով:
	Պետք է բացատրել արհեստական բանականության համակարգերի նպատակը երեխա օգտատերերին և նրանց ծնողներին կամ խնամակալներին, որպեսզի նրանք կարողանան որոշել օգտագործել կամ հրաժարվել նման հարթակներից:
Խթանել թվային տեխնոլոգիաները՝ որպես հետագա քաղաքացիական ներգրավվածության միջոց	ԱԲ-ի վրա հիմնված համակարգերի մատակարարները կարող են խրախուսել և հզորացնել երեխաներին և երիտասարդներին՝ աջակցելով նրանց մասնակցության իրավունքի պահպանմանը:
	Տե՛ս աղյուսակ 1-ի ընդհանուր ուղեցույցները:
Օգտագործելով տեխնոլոգիաների առաջընթացը՝ երեխաներին պաշտպանելու և կրթելու համար	ԱԲ-ի վրա հիմնված համակարգերը պետք է մշակվեն՝ աջակցելու երեխաների զարգացմանը և բարեկեցությանը՝ որպես արդյունք բոլոր համակարգերի նախագծման, զարգացման և ներդրման մեջ: Լավագույն հասանելի, լայնորեն ընդունված զարգացման և բարեկեցության չափանիշները պետք է լինեն դրանց հղման կետը: Ընկերությունները պետք է ներդրումներ կատարեն արհեստական ինտելեկտի վրա հիմնված էթիկական գործիքների հետազոտման և մշակման մեջ՝ առցանց ԵՍԶԲ-ի, առցանց ոտնձգություններն ու ահաբեկման գործողությունները հայտնաբերելու համար՝ համագործակցելով երեխաների իրավունքների և հենց երեխաների պաշտպանության ոլորտում մասնագիտացած հիմնական փորձագետների հետ:

ԱԲ տեխնոլոգիայի առաջընթացը պետք է կիրառվի երեխաների համար՝ տարիքին համապատասխան հաղորդագրություններ ուղարկելու նպատակով՝ առանց վտանգելու նրանց ինքնությունը, գտնվելու վայրը և անձնական տվյալները:

Հղումներ

ԲիԲիՍի քաղաքականություն.

Երեխաների պահպանության և պաշտպանության քաղաքականության տարբերակ 2017, վերանայված 2018 և թարմացված տարբերակ 2019 թ.

- ԲիԲիՍի-ում երիտասարդների և երեխաների հետ աշխատելը
- Արտաքին մատակարարների՝ Երեխաների պաշտպանության վերաբերյալ կանոնների շրջանակ Անկախ Արտադրող ընկերությունների համար, որոնք աշխատում են ԲիԲիՍի-ի արտադրությունում:
- Ուղեցույց. առցանց շփում երեխաների և երիտասարդների հետ՝ նրանց առցանց գործունեության համար խմբագրական ուղեցույցների վերաբերյալ:
- Միացյալ Թագավորությունում սոցիալական մեդիայի համար տարիքային ստուգումը չպահպանող հետաքննություն 2016, 2017, 2020թ.

Բառարան

Ստորև բերված սահմանումները հիմնականում վերցված են գոյություն ունեցող տերմինաբանությունից, որն ամրագրված է 1989 թ. Երեխայի իրավունքների կոնվենցիայում, ինչպես նաև Երեխաների սեռական շահագործման միջգերատեսչական աշխատանքային խմբի կողմից՝ Սեռական շահագործումից և սեռական հարաբերությունից երեխաների պաշտպանության տերմինաբանական ուղեցույցներում: Սեռական շահագործում (2016թ. Լյուքսեմբուրգի ուղեցույցներ), Սեռական շահագործումից և սեռական բռնությունից երեխաների պաշտպանության մասին Եվրոպայի խորհրդի կոնվենցիայի կողմից (2007թ.), ինչպես նաև՝ ՅՈՒՆԻՍԵՖ-ի Գլոբալ երեխաների առցանց զեկույցով (2019թ.):

Դեռահաս

Դեռահասները 10-19 տարեկան մարդիկ են: Կարևոր է նշել, որ «դեռահասները» միջազգային իրավունքի համաձայն պարտադիր տերմին չէ, և 18 տարեկանից ցածր անձինք համարվում են երեխաներ, մինչդեռ 18–19 տարեկան անձինք համարվում են չափահաս, եթե նրանք չափահաս չեն համարվում ավելի վաղ՝ ազգային օրենսդրությանը համապատասխան:[33]

Արհեստական բանականություն

Արհեստական բանականությունն ամենալայն իմաստով (AI). անորոշ կերպով վերաբերում է համակարգերին, որոնք մաքուր գիտական ֆանտաստիկա են (այսպես կոչված «ուժեղ» ԱԲ-ներ և համակարգեր, որոնք արդեն գործում են, ունակ են կատարել շատ բարդ առաջադրանքներ (նկարագրված համակարգեր՝ որպես «թույլ» կամ «չափավոր» ԱԲ-ներ, ինչպիսիք են՝ դեմքի կամ ձայնի ճանաչումը, տրանսպորտային միջոցներ վարելը):[34]

Արհեստական բանականության համակարգեր

ԱԲ համակարգը մեքենայական համակարգ է, որը կարող է մարդու կողմից սահմանված նպատակների որոշակի փաթեթի համար կանխատեսումներ կատարել, առաջարկություններ կամ իրական, վիրտուալ միջավայրերի վրա ազդող որոշումներ: ԱԲ համակարգերը նախագծված են՝ աշխատելու տարբեր մակարդակների ինքնավարությամբ:[35]

Ալեքսա (Alexa)

Amazon Alexa-ն, որը հայտնի է պարզապես Ալեքսա անունով, վիրտուալ ԱԲ օգնական է, որը մշակվել է Amazon-ի կողմից: Այն ի վիճակի է ձայնային փոխազդեցության, երաժշտության նվագարկման, անելիքների ցուցակներ կազմելու, զարթուցիչների տեղադրման, փոդքաստների հոսքի, աուդիոգրքեր նվագելու և եղանակի, երթևեկության, սպորտի և իրական ժամանակում այլ տեղեկություններ տրամադրելու, ինչպիսիք են՝ նորությունները: Ալեքսանն կարող է նաև կառավարել մի քանի խելացի սարքեր՝ օգտագործելով իրեն որպես տան ավտոմատացման համակարգ: Օգտատերերը կարող են ընդլայնել Ալեքսայի հնարավորությունները՝ տեղադրելով «հմտություններ» (լրացուցիչ գործառույթներ, որոնք մշակվել են երրորդ կողմի վաճառողների

33 *Յունիսեֆ և ՀՄՄ, «Երեխաների առցանց պաշտպանության ուղեցույցներ՝ նախատեսված ոլորտի համար», 2014.*
34 *Եվրոպայի խորհուրդ, «Ինչ է ԱԲ-ն».*
35 *ՏՀՀԿ, «Արհեստական ինտելեկտի վերաբերյալ խորհրդի հանձնարարականը», 2019.*

կողմից, այլ կարգավորումներում, որոնք ավելի հաճախ կոչվում են հավելվածներ, ինչպիսիք են՝ եղանակային ծրագրերը և աուդիո գործառույթները:[36]

Երեխայի լավագույն շահը

Վերաբերում է բոլոր այն տարրերին, որոնք անհրաժեշտ են կոնկրետ իրավիճակում որոշակի երեխայի կամ երեխաների խմբի համար որոշում կայացնելու համար.[37]

Երեխա

Երեխայի իրավունքների մասին կոնվենցիայի 1-ին հոդվածի համաձայն՝ երեխա է համարվում 18 տարեկանից ցածր յուրաքանչյուր ոք, բացառությամբ այն դեպքերի, երբ ազգային օրենսդրությամբ ավելի վաղ հասունություն է ձեռք բերվել:[38]

Երեխաների սեռական շահագործում և բռնություն

Նկարագրում է սեռական շահագործման և սեռական բռնության բոլոր ձևերը, օրինակ՝ ա) երեխային դրդելը կամ հարկադրելը որևէ անօրինական սեռական գործունեության մեջ, բ) երեխաների շահագործումը մարմնավաճառության կամ այլ ապօրինի սեռական պրակտիկայի մեջ, գ) երեխաների շահագործնական օգտագործումը պոռնոգրաֆիկ ներկայացումներում և նյութերում»,[39] ինչպես նաև՝ «սեռական շփում, որը սովորաբար ենթադրում է անձի վրա գործադրվող բռնություն՝ առանց համաձայնության:[40] Երեխաների սեռական շահագործումը և չարաշահումը (ԵՍՇՆ) ավելի ու ավելի է տարածվում համացանցի կամ առցանց միջավայրի հետ որոշակի կապի միջոցով:

Երեխաների սեռական շահագործման և չարաշահման նյութեր

ՏՀՏ-ների արագ զարգացումը ստեղծեցին առցանց ԵՍՇԲ-ի նոր ձևեր, որոնք կարող են իրականացվել առցանց միջավայրում և պարտադիր չէ, որ ներառեն ֆիզիկական՝ դեմառդեմ, հանդիպում երեխայի հետ:[41]

---

36 Յունիսեֆ և ՀՄՄ, «Երեխաների առցանց պաշտպանության ուղեցույցներ՝ նախատեսված ոլորտի համար», 2014.
37 Տես ՄԱԿ-ի Երեխաների իրավունքների կոնվենցիան:
38 Յունիսեֆ և ՀՄՄ, «Երեխաների առցանց պաշտպանության ուղեցույցներ՝ նախատեսված ոլորտի համար», 2014:
39 Միավորված ազգերի կազմակերպության Երեխայի իրավունքների մասին կոնվենցիայի 34-րդ հոդվածը:
40 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Լյուքսեմբուրգի ուղեցույցներ), 2016.
41 Լյուքսեմբուրգի ուղեցույցները (ինչպես վերևում), 2016թ. և ՅՈՒՆԻՍԵՖ, Global Kids Online report, 2019

Չնայած բազմաթիվ նյութերում երեխաների նկատմամբ սեռական բռնության լուսանկարները և տեսագրությունները դեռևս նշվում են որպես «մանկական պոռնոգրաֆիա» կամ «երեխաների անպարկեշտ պատկերներ», այս ուղեցույցներում այդ խնդիրները միասին կոչվում են «երեխաների նկատմամբ սեռական բռնության նյութեր» (ԵՍԲՆ): Այս տերմինը համապատասխանում է Լայնաշերտ Հանձնաժողովի Ուղեցույցներին և WePROTECT Global Alliances' Model National Response-ին [42] ՝ ավելի ճշգրիտ է նկարագրում բովանդակությունը: Պոռնոգրաֆիան վերաբերում է օրինական, առևտրային արդյունաբերությանը և, ինչպես նշվում է Լյուքսեմբուրգի ուղեցույցում.

«Տերմինի օգտագործումը կարող է (ակամա թե ակամա) նպաստել հանցանքի ծանրության նվազեցմանը, նույնիսկ՝ օրինականացնելու այն, ինչ իրականում համարվում է երեխաների սեռական բռնություն կամ սեռական շահագործում: «Մանկական պոռնոգրաֆիա» տերմինը կարող է ենթադրել, որ գործողությունները կատարվում են երեխայի համաձայնությամբ և ներկայացնում են օրինական սեռական նյութ»: ԵՍԲՆ տերմինն օգտագործելիս մենք վերաբերում ենք նյութին, որը ներկայացնում է երեխայի նկատմամբ սեռական բռնության կամ շահագործման գործողություններ: Սա ներառում է, բայց չի սահմանափակվում դրանով, մեծահասակների կողմից երեխաների նկատմամբ սեռական բռնության մասին արձանագրող նյութեր, սեռական բացահայտ վարքագծի մեջ ներառված երեխաների լուսանկարներ և երեխաների սեռական օրգաններ, երբ լուսանկարներն արտադրվում կամ օգտագործվում են հիմնականում սեռական նպատակներով:

Տե՛ս Լյուքսեմբուրգի ուղեցույցը այնպիսի տերմինների համար, ինչպիսիք են՝ «համակարգչային կամ թվայնորեն ստեղծված երեխաների սեռական բռնության նյութերը»:

Երեխաներ և երիտասարդներ

Նկարագրում է 18 տարեկանից ցածր բոլոր անձանց. «երեխաներն» (այս ՀՄՄ ուղեցույցներում կոչվում են նաև «կրտսեր երեխաներ») ներառում են 15 տարեկանից ցածր բոլոր անձանց, իսկ «երիտասարդները» ներառում են 15-18 տարեկան անձանց խումբը:

Կապակցված խաղալիքներ

Կապակցված խաղալիքները միանում են համացանցին՝ օգտագործելով Wi-Fi և Bluetooth տեխնոլոգիաներ: Սովորաբար գործում են ուղեկից հավելվածների հետ՝ երեխաների համար ինտերակտիվ խաղալու հնարավորություն ստեղծելով: Համաձայն Juniper Research-ի տվյալների՝ 2015 թվականին կապակցված խաղալիքների շուկան հասել է 2,8 միլիարդ ԱՄՆ դոլարի և կանխատեսվում է, որ մինչև 2020 թվակա-

42 Լայնաշերտ Կայուն Զարգացման Հանձնաժողով, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online", 2019; WePROTECT Global Alliance, "Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response", 2016.

նը կավելանա մինչև 11 միլիարդ դոլար: Այս խաղալիքները հավաքում և պահում են երեխաների անձնական տվյալները՝ ներառյալ անունները, աշխարհագրական դիրքը, հասցեները, լուսանկարները, աուդիո և վիդեո ձայնագրությունները:[43]

Կիբերբուլինգ կամ կիբերհալածանք

Կիբերհալածանքը նկարագրում է միտումնավոր ագրեսիվ գործողություն, որը բազմիցս իրականացվել է կամ խմբի կամ անհատի կողմից՝ օգտագործելով թվային տեխնոլոգիաներ և ուղղված է զոհին, որը չի կարող հեշտությամբ պաշտպանել իրեն:[44] Այն սովորաբար ներառում է «թվային տեխնոլոգիաների և համացանցի օգտագործումն՝ ինչ-որ մեկի մասին վիրավորական տեղեկատվություն հրապարակելու համար: Դիտավորյալ հավաքած անձնական տեղեկություններով, լուսանկարներով կամ տեսանյութերով վիրավորող ձևով կիսելը, սպառնալից կամ վիրավորական հաղորդագրություններ ուղարկելը (էլ. փոստի, ակնթարթային հաղորդագրությունների, չաթի կամ տեքստերի միջոցով), լուրեր տարածելը և զոհի մասին կեղծ տեղեկատվություն, կեղծ լուրեր տարածելը կամ նրանց առցանց հաղորդակցությունից դիտավորյալ հեռացնելը:[45]

Կիբերատելություն, խտրականություն և բռնի ծայրահեղականություն

«Կիբերատելությունը, խտրականությունը և բռնի ծայրահեղականությունը կիբերբռնության հստակ ձևեր են, քանի որ դրանք ուղղված են կոլեկտիվ ինքնությանն, այլ ոչ թե անհատներին, ... հաճախ կապված ռասայի, սեռական կողմնորոշման, կրոնի, ազգության կամ ներգաղթի կարգավիճակի, սեռի և քաղաքականության հետ»:[46]

Թվային քաղաքացիություն

Թվային քաղաքացիությունը վերաբերում է թվային միջավայրում դրական, քննադատաբար և գրագետ ներգրավվելու կարողությանը, հենվելով արդյունավետ հաղորդակցման և ստեղծագործության հմտությունների վրա, կիրառելով սոցիալական մասնակցության ձևեր, որոնք հարգում են մարդու իրավունքները և արժանապատվությունը՝ տեխնոլոգիաների պատասխանատու օգտագործման միջոցով:[47]

---

43 Ջերեմի Գրինբերգ, "Dangerous Games: Connected Toys, COPPA, and Bad Security", Ջորջթաունի իրավունքի տեխնոլոգիայի փեսություն, 2017 թ.
44 Anna Costanza Baldry et al. "Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities", Երեխաների և երիտասարդության ծառայությունների սպուգում, 2019:
45 Լյուքսեմբուրգի ուղեցույցներ, 2016 թվականը և ՅՈՒՆԻՍԵՖ- Global Kids Online, 2019 թվականը (ինչպես վերևում):
46 ՅՈՒՆԻՍԵՖ Global Kids Online report, 2019 (ինչպես վերևում):
47 Լյուքսեմբուրգի ուղեցույցներ, 2016 թվականը և ՅՈՒՆԻՍԵՖ- Global Kids Online, 2019 թվականը (ինչպես վերևում):

Թվային գրագիտություն

Թվային գրագիտություն նշանակում է ունենալ այնպիսի հմտություններ, որոնք անհրաժեշտ են մարդուն ապրելու, սովորելու և աշխատելու համար մի հասարակությունում, որտեղ հաղորդակցությունն ու տեղեկատվության հասանելիությունն ավելի ու ավելի շատ են դառնում թվային տեխնոլոգիաների միջոցով, ինչպիսիք են ինտերնետ հարթակները, սոցիալական լրատվամիջոցները և շարժական սարքերը:[48] Այն ներառում է հստակ հաղորդակցություն, տեխնիկական հմտություններ և քննադատական մտածողություն:

Թվային ճկունություն

Այս տերմինը նկարագրում է երեխայի կարողությունը՝ էմոցիոնալ կերպով հաղթահարելու առցանց հանդիպող վնասը: Այն նաև վերաբերում է հուզական բանականությանը, որն անհրաժեշտ է հասկանալու, թե երբ է երեխան վտանգի տակ գտնվում առցանց, իմանալ, թե ինչպես օգնություն փնտրել, սովորել փորձից և վերականգնվել, երբ ամեն ինչ սխալ է ընթանում:[49]

Կառավարիչներ

Նկարագրում է բոլոր այն անձանց, ովքեր պաշտոն են զբաղեցնում դպրոցի կառավարման կառույցում:

Գրումինգ, առցանց գրումինգ

Գրումինգն, առցանց գրումինգը, ինչպես սահմանված է Լյուքսեմբուրգի Ուղեցույցում, վերաբերում է «երեխայի հետ հարաբերություններ կառուցելու գործընթացին կամ անձամբ, կամ համացանցի, կամ այլ թվային տեխնոլոգիաների օգտագործման միջոցով՝ հեշտացնելու համար նրա հետ առցանց կամ անցանց սեռական շփումը»: Երեխայի հետ ընկերություն անելը հանցավոր գործունեություն է՝ երեխայի հետ սեռական հարաբերություն ունենալու համար համոզելու նպատակով:

Տեղեկատվական և հաղորդակցական տեխնոլոգիաներ

Տեղեկատվական և հաղորդակցական տեխնոլոգիաները (ՏՀՏ) նկարագրում են բոլոր տեղեկատվական տեխնոլոգիաները, որոնք ընդգծում են հաղորդակցության ասպեկտը: Սա ներառում է համացանցին միացող բոլոր ծառայություններն ու սարքերը, ինչպիսիք են՝ համակարգիչները, դյուրակիր համակարգիչները, պլանշետները, սմարթֆոնները, խաղային վահանակները և խելացի ժամացույցները[50]:

---

48 Արևմտյան Սիդնեյի համալսարան, «Ինչ է թվային քաղաքացիությունը»
49 Դոկտոր Էնդրյու Կ. Պրժիբիլսկին և այլք, «Համատեղ պատասխանատվություն. զարգացնել երեխաների առցանց ճկունությունը» Վիրջին Մոսի և Ծնողական տարածք, 2014:
50 ՅՈՒՆԻՍԵՖ և ՀՄՄ, «Երեխաների առցանց անվտանգության մասին ուղեցույց՝ նախատեսված ոլորտի համար», 2014 (Ինչպես վերևում).

Այն ներառում է նաև այնպիսի ծառայություններ, ինչպիսիք են՝ ռադիոն և հեռուստատեսությունը, ինչպես նաև՝ լայնաշերտ, ցանցային սարքավորումներ և արբանյակային համակարգեր:

Առցանց խաղ

Առցանց խաղը սահմանվում է որպես ցանկացած տեսակի մեկ կամ բազմախաղացող կոմերցիոն թվային խաղ՝ համացանցին միացված ցանկացած սարքի միջոցով՝ ներառյալ հատուկ կոնսուլներ, աշխատասեղան համակարգիչներ, դյուրակիր համակարգիչներ, պլանշետներ և բջջային հեռախոսներ: «Առցանց խաղերի էկոհամակարգը» սահմանվում է այնպես, որ ներառում է ուրիշների՝ տեսախաղեր խաղալու պրոցեսի դիտումն էլեկտրոնային սպորտի կամ տեսանյութերի փոխանակման հարթակների միջոցով, որոնք սովորաբար հնարավորություն են տալիս դիտողներին մեկնաբանել կամ շփվել խաղացողների և դիտող այլ անդամների հետ:[51]

Ծնողական վերահսկողության գործիքներ

Ծրագրային ապահովում, որը թույլ է տալիս օգտվողներին, սովորաբար՝ ծնողներին, կառավարել համակարգչի կամ համացանցին միացված այլ սարքի որոշ կամ բոլոր գործառույթները: Սովորաբար, նման ծրագրերը կարող են սահմանափակել մուտքը դեպի որոշակի տեսակի կամ դասի կայքեր կամ առցանց ծառայություններ: Ոմանք նաև հնարավորություն են տալիս ժամանակի կառավարման համար, այսինքն՝ սարքը կարող է կարգավորվել այնպես, որ համացանցին հասանելիություն ունենա միայն որոշակի ժամերի ընթացքում: Ավելի առաջադեմ տարբերակները կարող են ձայնագրել սարքից ուղարկված կամ ստացված բոլոր տեքստերը: Ծրագրերը սովորաբար պաշտպանված կլինեն գաղտնաբառով:[52]

Անձնական տվյալներ

Այս տերմինը նկարագրում է անձի վերաբերյալ անհատական ճանաչելի տեղեկատվություն, որը հավաքագրվում է առցանց: Սա ներառում է լրիվ անունը, կոնտակտային տվյալները, ինչպիսիք են տան և էլեկտրոնային հասցեները, հեռախոսահամարները, մատնահետքերը կամ դեմքի ճանաչումը, ապահովագրական համարները կամ որևէ այլ տվյալ, որը թույլ է տալիս ֆիզիկական կամ առցանց շփումը կամ տեղայնացումը: Այս համատեքստում այն նաև վերաբերում է երեխայի և նրա շրջապատի մասին ցանկացած տեղեկատվության, որը հավաքագրվում է առցանց ծառայություններ մատուցողների կողմից՝ ներառյալ կապակցված խաղալիքները և իրերի ինտերնետը և ցանկացած այլ համացանցին միացված տեխնոլոգիա:

---

51 ՅՈՒՆԻՍԵՖ, «Երեխաների իրավունքները և առցանց խաղերը. հնարավորություններ և մարտահրավերներ երեխաների և արդյունաբերության համար», 2019:
52 ՅՈՒՆԻՍԵՖ և ՀՄՄ, «Ուղեցույց երեխաների առցանց անվտանգության վերաբերյալ՝ նախատեսված ոլորտի համար», 2014 (ինչպես վերևում):

Գաղտնիություն

Գաղտնիությունը հաճախ չափվում է առցանց անձնական տեղեկատվության փոխանակման, սոցիալական մեդիայի հանրային պրոֆիլ ունենալու, առցանց ծանոթացած մարդկանց հետ տեղեկատվության փոխանակման, գաղտնիության կարգավորումների օգտագործման, ընկերների հետ գաղտնաբառերի փոխանակման և գաղտնիության հետ կապված մտահոգությունների տեսանկյունից:[53]

Հանրային ծառայության մեդիա

Սրանք ազգային հեռարձակողներ կամ լրատվամիջոցներ են, որոնք ստացել են իրենց հեռարձակման լիցենզիան պետության կամ կառավարության հետ պայմանագրային մի շարք պարտավորությունների հիման վրա: Այս պարտավորությունները վերջին տարիներին ընդլայնվել են բազմաթիվ երկրներում՝ մեդիա և թվային գրագիտության ծրագրերի միջոցով՝ թվային փոխակերպման հետևանքները լուծելու և թվային անջրպետը վերացնելու պարտավորությունների միջոցով:

Սեքսփինգ

Սեքստինգը սովորաբար սահմանվում է որպես բջջային հեռախոսների կամ համացանցի միջոցով[54] ինքնաարտադրվող սեքսուալ բովանդակության՝ ներառյալ լուսանկարներ, հաղորդագրությունների կամ տեսանյութերի ուղարկում, ստացում կամ փոխանակում: Երեխաների սեքսուալ պատկերների ստեղծումը, տարածումը և պահպանումն անօրինական է շատ երկրներում: Եթե բացահայտվում են երեխաների սեռական նկարները, ապա մեծահասակները չպետք է դիտեն դրանք: Երեխայի հետ չափահասի կողմից սեռական նկարների փոխանակումը միշտ հանցավոր արարք է, որը կարող է վնասակար լինել, հնարավոր է անհրաժեշտ լինի նման լուսանկարների մասին հաղորդել և հեռացնել դրանք:

Սեռավարություն (sextortion) կամ երեխաների սեռական հարկադրանք (Sexual extortion of children)

Սեռավարությունը կամ երեխաների սեռական շորթումն («առցանց սեռական հարկադրանք և շորթում») անձի հանդեպ շանտաժն է, որը նպատակ է հետապնդում այդ անձի՝ սեփական ձեռքերով ստեղծված նկարների օգնությամբ նրանից սեռական բարեհաճություն, փող կամ այլ օգուտներ կորզել՝ տվյալ անձի համաձայնությունից դուրս նյութը տարածելու սպառնալիքի ներքո (օրինակ՝ լուսանկարները տեղադրել սոցիալական ցանցերում)[55]»:

---

53 ԱՄՆ Առևտրի դաշնային հանձնաժողով, «Երեխաների առցանց գաղտնիության պաշտպանության ակտ», 1998 թ.
54 Լյուքսեմբուրգի ուղեցույցներ, 2016 (ինչպես վերևում)
55 Լյուքսեմբուրգի ուղեցույցներ, 2016 (ինչպես վերևում)

Իրերի ինտերնետ

«Իրերի ինտերնետը (IoT) ներկայացնում է հաջորդ քայլը դեպի մեր հասարակության և տնտեսության թվայնացումը, որտեղ օբյեկտներն ու մարդիկ փոխկապակցված են հաղորդակցման ցանցերի միջոցով և հայտնում է նրանց կարգավիճակի կամ շրջակա միջավայրի մասին»:[56]

ՄՌՈ (URL)

Այս հապավումը նշանակում է «միատեսակ ռեսուրսների որոնիչ», ինտերնետային էջի հասցեն:[57]

Վիրտուալ իրականություն

«Վիրտուալ իրականությունը համակարգչային տեխնոլոգիաների օգտագործումն է՝ ինտերակտիվ եռաչափ աշխարհի էֆեկտ ստեղծելու համար, որտեղ օբյեկտներն ունեն տարածական ներկայության զգացում»:[58]

ՎայՖայ (Wi-Fi)

Wi-Fi (Wireless Fidelity) տեխնիկական ստանդարտների խումբ է, որը թույլ է տալիս տվյալների փոխանցումը անլար ցանցերի միջոցով: [59]

56 Եվրոպական Հանձնաժողով, "Policy: The Internet of Things"
57 ՅՈՒՆԻՍԵՖ և ՀՄՄ, «Երեխաների առցանց պաշտպանության ուղեցույց՝ նախատեսված ոլորտի համար», 2014 (ինչպես վերևում):
58 ՆԱՍԱ, "Virtual Reality: Definition and Requirements".
59 ԱՄՆ Առևտրի դաշնային հանձնաժողով, "Children's Online Privacy Protection Act", 1998.