ՄԵԴԻԱ
ՆԱԽԱՁԵՌՆՈՒԹՅՈՒՆՆԵՐԻ
ԿԵՆՏՐՈՆ

Ինտերնետի ազատությունը և առցանց տիրույթում մարդու իրավունքների պաշտպանությունը Հայաստանում

«Մարդու իրավունքները ինտերնետում. կրթություն և պաշտպանություն»

ծրագրի շրջանակներում իրականացված անկախ հետազոտության զեկույց

Հասմիկ ԹԱՄԱՄՅԱՆ

Մովսես ՀԱԿՈԲՅԱՆ

Հունիս 2017 (թարմացվել է 2017 թ. դեկտեմբերին)

Այս զեկույցը պատրաստել է անկախ խորհրդատուների խումբը: Այստեղ արտահայտված տեսակետները պատկանում են խորհրդատուներին և պարտադիր չէ, որ արտացոլեն Մեդիա նախաձեռնությունների կենտրոնի կամ Ամերիկյան իրավաբանների ասոցիացիայի «Օրենքի գերակայության նախաձեռնության» տեսակետները:

ՇՆՈՐՀԱԿԱԼԱԿԱՆ ԽՈՍՔ

Հետազոտական խումբը իր երախտագիտությունն է հայտնում խորքային հարցազրույցներին և ֆոկուս խմբերի քննարկումներին մասնակցած լրագրողներին, քաղաքացիական հասարակության ներկայացուցիչներին, ինչպես նաև SS անվտանգության և մեդիա փորձագետներին՝ արժեքավոր տեսակետների և արձագանքի համար: Հատուկ շնորհակալություն Սամվել Մարտիրոսյանին և Արթուր Պապյանին՝ հետազոտության ողջ ընթացքում մասնագիտական գիտելիքներով կիսվելու և շարունակական աջակցության համար: Հետազոտական խումբը շնորհակալ է ՄՆԿ-ի ծրագրային թիմի ցուցաբերած նշանակալի աջակցության համար, հատկապես Աննա Բարսեղյանին, ինչպես նաև ՄՆԿ-ի անձնակազմին՝ Նունե Սարգսյանին, Արշալույս Մուրադյանին և Գեղամ Վարդանյանին՝ ծրագրին առնչվող գիտելիքներով կիսվելու և հետազոտության գործընթացը համակարգելու համար:

Բովանդակություն

ՇՆՈՐՀԱԿԱԼԱԿԱՆ ԽՈՍՔ 2

I. ՆԵՐԱԾՈՒԹՅՈՒՆ 4

1.1. Նախադրյալներ և համատեքստ 4

II. ՀԵՏԱԶՈՏՈՒԹՅԱՆ ՆՊԱՏԱԿԸ ԵՎ ՄԵԹՈԴՈԼՈԳԻԱՆ 6

2.1. Հետազոտության նպատակը և թիմը 6

2.2. Տվյալների աղբյուրներն ու տվյալների հավաքագրման մեթոդները 6

III. ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ ԵՎ ԱՐԴՅՈՒՆՔՆԵՐ 8

3.1. Հայաստանում մարդու իրավունքների և ազատությունների իրավական վերլուծությունը, որը հավասարապես կիրառելի է նաև կիբերտիրույթում 8

3.2. Ցանցի չեզոքություն 11

3.3. Լրատվամիջոցների և քաղհասարակության ներկայացուցիչներից բաղկացած թիրախ խմբի գիտելիքներն ու փորձը կիբերանվտանգության ոլորտում 18

3.4. Մարդու իրավունքները ցանցում և ցանցից դուրս. եթե դրանք ամբողջովին նույնը չեն, ապա որտե՞ղ են հատվում: Հայաստանի տարածքում վերջին տասնամյակում ինտերնետի սահմանափակումները 21

3.5. Ի՞նչն է լրագրողին կամ շահերի պաշտպանությամբ զբաղվողներին դարձնում կիբերհարձակումների թիրախ, և ո՞վ է պատասխանատու նրանց ստեղծած բովանդակության, անձնական տվյալների և ցանցերի պաշտպանության համար 25

3.6. Առցանց մուլտիմեդիա գործիքակազմի մշակումը ծրագրի շրջանակներում 28

IV. ԵԶՐԱՀԱՆԳՈՒՄՆԵՐ ԵՎ ՀԻՄՆԱԿԱՆ ԱՌԱՋԱՐԿՈՒԹՅՈՒՆՆԵՐ 29

V. ԿԻՑ ՓԱՍՏԱԹՂԹԵՐ 32

5.1. Խորքային հարցազրույցներ և ֆոկուս խմբերի քննարկումներ վարելու ուղեցույց 32

5.2. Խորքային հարցազրույցներ և ֆոկուս խմբերի քննարկումներ վարելու ժամանակացույց 35

I. ՆԵՐԱԾՈՒԹՅՈՒՆ

Սա անկախ հետազոտության զեկույց է, որն ամփոփում է Մեդիա նախաձեռնությունների կենտրոնի իրականացրած՝ «Մարդու իրավունքները ինտերնետում. կրթություն և պաշտպանություն» ծրագրի (Ծրագիր) շրջանակներում կատարված վերլուծությունների, մի շարք խորքային հարցազրույցների և ֆոկուս խմբերի քննարկումների արդյունքները: Սա ամփոփիչ հետազոտություն է, որի նպատակն է գնահատել Հայաստանում ինտերնետի ազատության իրավիճակը և առցանց տիրույթում մարդու հիմնարար իրավունքների պաշտպանությունը: Հետազոտությունը նաև նախատեսված է ոլորտում հնարավոր ծրագրերի և քաղաքականության մշակման համար օգտակար առաջարկություններ և քաղած դասեր ներկայացնելու համար:

1.1. Նախադրյալներ և համատեքստ

Ինչպես նշել է «Ֆրիդոմ Հաուս» կազմակերպությունն իր «Ցանցի ազատությունը 2016» զեկույցում, «[նախորդ] տարում ինտերնետի ազատությունը հիմնականում եղել է առանց խոչընդոտի, չնայած որ արձանագրվեց Հայաստանի ընդհանուր միավորների որոշակի անկում, երբ ոստկանությունը ֆիզիկական բռնություն գործադրեց Երևանում ցույցերը ուղիղ հեռարձակմամբ լուսաբանող լրագրողների նկատմամբ»: Թեև հայերն ընդհանուր առմամբ առցանց միջավայրում ազատորեն արտահայտում են իրենց տեսակետները՝ առանց լուրջ սահմանափակումների կամ պատժվելու մտավախության, «Ֆրիդոմ Հաուս»-ի դիտարկած ժամանակահատվածի ընթացքում և դրանից հետո տեղի ունեցան վերահսկման և գրաքննության որոշ դեպքեր, որոնք հիմնականում համընկան բռնությունների, խռովությունների և Լեռնային Ղարաբաղի հակամարտության սրման ժամանակահատվածի հետ: Իսկ երբ 2017 թ. ապրիլի խորհրդարանական ընտրությունների շրջանում լրագրողական համայնքի մի քանի հայտնի ներկայացուցիչների թվիթերյան հաշիվները կարճ ժամանակով արգելափակվեցին, Հայաստանի ինտերնետի ազատության կարգավիճակը անկում ապրեց «Ֆրիդոմ Հաուս»-ի «Ցանցի ազատություն 2017» զեկույցում ՝ դասակարգվելով որպես «մասնակի ազատ»: 2016 թ. հուլիսին իշխանության նկատմամբ զինված խմբավորման դիմակայության ընթացքում Ֆեյսբուք սոցիալական ցանցը ժամանակավորապես անհասանելի էր: Ինտերնետի օգտատերերին «խորհուրդ» տվեցին դիմել ինքնագրաքննության, երբ Լեռնային Ղարաբաղի հակամարտության գոտում վերսկսվեցին արյունալի բախումները: Ավելի վաղ՝ 2015 թ. հունիսին, ոստիկանությունը թիրախավորեց լրագրողներին և քաղաքացիական ակտիվիստներին, որոնք ուղիղ հեռարձակմամբ լուսաբանում էին մայրաքաղաքում տեղի ունեցող «Էլեկտրիկ Երևան» անվանումը ստացած ցույցը՝ ստիպելով նրանց լքել տարածքը և խլելով նրանց տեսագրման սարքավորումները: Այնուամենայնիվ, Հայաստանում ինտերնետը ավանդաբար մնացել է ազատ՝ արձանագրելով կայուն բարելավումներ մատչելիության և ենթակառուցվածքի տեսանկյունից (ըստ Հեռահաղորդակցության միջազգային միության տվյալների՝ 2016 թ. բնակչության 62%-ն օգտագործում է ինտերնետ): Լրագրողներն ու քաղաքացիական ակտիվիստները լայնորեն օգտագործում են սոցիալական ցանցերը՝ որպես իրենց համոզմունքներն ու շարժումները տարածելու միջոց, զարգանում են ընդդիմադիր և անկախ առցանց լրատվամիջոցները:

Տեղական փորձագետները և «Ֆրիդոմ Հաուս»-ը՝ իր վարկանիշային աղյուսակով, ինտերնետը Հայաստանում դասակարգում են որպես ազատ՝ ինտերնետի մատչելիության ինչ-ինչ խոչընդոտներով, առցանց բովանդակության որոշ սահմանափակումներով և ինտերնետի օգտատերերի իրավունքների խախտումներով: Դիտարկումներն, այնուամենայնիվ, ցույց են տալիս, որ թեև Հայաստանի օրենքները ընդհանուր առմամբ հավասարակշռված են, լուրջ մտավախություններ կան՝ կապված պետության կողմից մի շարք թիրախավորված օգտագործողների առցանց բովանդակությանն ու ինտերնետային թրաֆիքին միջամտելու հետ: Վերլուծության շրջանակներում բարձրացված հարցերը մասնավորապես ներառում են գաղտնալսման, կայքերը և անձնական հաշիվները կոտրելու բավականին շատ դեպքերը և այդ դեպքերի առնչությամբ կառավարության արձագանքի բացակայությունը:

Մեդիա նախաձեռնությունների կենտրոնը իր՝ «Մարդու իրավունքներն ինտերնետում. կրթություն և պաշտպանություն» ծրագրի միջոցով նպատակ ունի գնահատել կիբերավտանգության ոլորտում քաղաքացիական հասարակության ներկայացուցիչների և լրագրողների գիտելիքների ու հմտությունների մակարդակը և ուսումնասիրել այն հիմնախնդիրների շրջանակը, որոնց նրանք բախվում են ինտերնետում առօրյա գործունեության ընթացքում: Ծրագրի նպատակն է հասկանալ՝ ինչ չափով են ծրագրի թիրախ հանդիսացող մասնագետները կարողանում իրացնել իրենց հիմնարար իրավունքները առցանց տիրույթում և ինչպես կարող են արդյունավետ պայքարել կիբերանվտանգության առկա և նոր ի հայտ եկող ռիսկերի ու սպառնալիքների դեմ:

Վերջին մի քանի տասնամյակների ընթացքում տեղի է ունեցել առցանց լրատվամիջոցների անհավանական աճ, ինչը սկսում է գերազանցել ավանդական լրատվամիջոցների զբաղեցրած տարածքը: Ինտերնետը նաև կարծես լուծում է դառնում ներկայացուցչական ժողովրդավարության մեջ քաղաքացիական հասարակության ինտեգրման համար՝ ակտիվացնելով քաղաքացիների և որոշում ընդունողների միջև կապը և խրախուսելով հանրային մասնակցությունը: Ինտերնետը լավ հարթակ է ակտիվ քննարկումների, տեղեկատվության փոխանակման և հանրային մասնակցության համար, ինչն իր հերթին ծառայում է տեղեկատվության ժողովրդավարացման նպատակին: Այնուամենայնիվ, տեղեկատվության ժողովրդավարացումը համաշխարհային ցանցի միջոցով կախված է մատչելիությունից, որը երաշխավորում են ինտերնետի ազատության սկզբունքները, և առանձին օգտատերերի մեդիագրագիտությունից: Ցանցում սեփական ազատությունն ապահովելու նպատակով հասարակություններն ու անհատ մասնագետները պետք է ձգտեն և պահանջեն ավելի ազատ ինտերնետ՝ զերծ բովանդակության նկատմամբ կառավարության վերահսկումից և մեծ բիզնես ուժերի ճնշումներից: Ազատ ինտերնետի իրավունքի կարևորումը և թվային անվտանգության գործիքներ, գիտելիքներ և հմտություններ ունենալը միակ ճանապարհն է, որի միջոցով մեդիա մասնագետները և քաղաքացիական ակտիվիստները կկարողանան օգտագործել ինտերնետի ընձեռած հնարավորությունները՝ նպաստելով տեղեկատվության ժողովրդավարացմանն ու որոշումների կայացման մասնակցային գործընթացին:

ՄՆԿ-ի ծրագրի արդյունքում ստեղծվելու են՝ ա) այս զեկույցը, որն ամփոփում է հետազոտության արդյունքները և բ) առցանց խաղ կիբեր տիրույթի վտանգների մասին: Զեկույցը նշում է ինտերնետի անվտանգությանն առնչվող հիմնական խնդիրները և առաջարկում այդ խնդիրների լուծմանն ուղղված ռազմավարություններ: Հույս ունենք, որ այն աշխատանքային փաստաթուղթ կդառնա քաղաքականություն մշակողների, ծրագրերի շահագրգիռ կողմերի և մասնագետների թիրախ խմբերի համար: Խաղը

հանրությանը կուսուցանի իրենց առցանց իրավունքները և կբարձրացնի իրազեկությունը կիբերանվտանգությանը սպառնացող վտանգների մասին:

II. ՀԵՏԱԶՈՏՈՒԹՅԱՆ ՆՊԱՏԱԿՆ ՈՒ ՄԵԹՈԴԱԲԱՆՈՒԹՅՈՒՆԸ

2.1. Հետազոտության նպատակն ու հետազոտական թիմը

Հետազոտության նպատակն էր.

- Վերլուծել ինտերնետը, ինտերնետի ազատությունը և Հայաստանում կիբերանվտանգությանն առնչվող իրավական շրջանակն ու քաղաքականությունը:
- Գնահատել՝ որքանով են տարածված առցանց տիրույթում մարդու իրավունքների խախտումների դեպքերը:
- Գնահատել՝ որքանով են այս իրավունքներն իրացվում՝ որպես թիրախ սահմանելով մեդիա մասնագետներին և քաղաքացիական ակտիվիստներին:
- Գնահատել թիրախ խմբի մասնագետների/ակտիվիստների գիտելիքներն ու հմտությունները տեղեկատվության անվտանգության ոլորտում:
- Առաջարկել հնարավոր նախաձեռնություններ և հետագա գործողություններ թիրախ խմբի մասնագետների շրջանում ինտերնետի անվտանգ օգտագործման համար:

Հետազոտությունն իրականացրել է անկախ խորհրդատուների խումբը՝ ներառյալ հետազոտողը, ով մասնագիտացած է մեդիա ոլորտի զարգացման և ուսումնասիրությունների գծով, և իրավական փորձագետը, ով ունի ինտերնետի և թվային անվտանգության ոլորտի մեծ փորձ:

Հետազոտական խմբի ղեկավար՝ Հասմիկ Թամամյան

Իրավական փորձագետ՝ Մովսես Հակոբյան

2.2. Տվյալների աղբյուրները և տվյալների հավաքագրման մեթոդները

Հետազոտական թիմն իր եզրահանգումները կատարել է տվյալների հավաքագրման տարբեր մեթոդներից ստացված ապացույցների եռանկյունացման, ինչպես նաև առաջնային/երկրորդական աղբյուրների հիման վրա:

Տվյալների հավաքագրման մեթոդներ

Գնահատումն իրականացնելու համար կիրառվել են տվյալների հավաքագրման հետևյալ մեթոդները.

1. **Օրենսդրության ուսումնասիրություն/փաստաթղթերի վերլուծություն**. ՀՀ օրենքների և օրենսդրական ակտերի, ինչպես նաև Հայաստանի կողմից ստորագրված/վավերացված միջազգային դաշնագրերի վերլուծություն: Փաստաթղթերի վերլուծությունը ներառում է նաև պետական մարմինների կողմից տրամադրված հաշվետվություններն ու վիճակագրությունը: Իրավական փաստաթղթերի և տեղական ու միջազգային զեկույցների համակողմանի ուսումնասիրությունը հիմք են ապահովել այս հետազոտության համար:

2. **Անհատական խորքային հարցազրույցներ** մեդիա մասնագետների և քաղաքացիական ակտիվիստների թիրախ խմբերից ընտրված փորձագետների և ներկայացուցիչների հետ: Խորքային հարցազրույցներն անցկացվել են ցանցի չեզոքության, առցանց տիրույթում մարդու իրավունքների ճանաչման և ընդունման, իրենց առօրյա գործունեության ընթացքում թիրախ խմբի մասնագետների հանդիպած խնդիրների մասին համակողմանի տեղեկատվություն և կարծիքներ ստանալու նպատակով: Խորքային հարցազրույցներն անցկացվել են SS անվտանգության ընտրված փորձագետների և մեդիա մասնագետների, ինչպես նաև քաղաքացիական հասարակության ներկայացուցիչների հետ: Հետազոտական խմբի կողմից մշակվել է կիսակառուցվածքային հարցազրույցների ուղեցույց (տես՝ կից փաստաթուղթ 5.1-ը): Անցկացվել է 14 դեմ առ դեմ հարցազրույց (կից փաստաթուղթ 5.2) նպատակային ընտրանքի տեխնիկայի հիման վրա, որի շրջանակներում հիմնական փորձագետների ընտրությունը կատարվել է հաշվի առնելով ոլորտում նրանց ունեցած գիտելիքների և ներգրավվածության մակարդակը:

3. **Ֆոկուս խմբերի քննարկումներ** լրագրողների, քաղաքացիական ակտիվիստների և ՀԿ-ների ներկայացուցիչների հետ: Այս մեթոդի օգտագործման նպատակն է SS անվտանգության ինքնաստեղծ և արտաքին ռիսկերի մասին քննարկումներին նպաստելը, առցանց տիրույթում մարդու իրավունքների ճանաչումն ու առաջխաղացումը և այլն: Հետազոտական խումբը նաև ուսումնասիրել և վերհանել է, թե ինչպես են այս հարցերին անդրադառնում անհատական, ինստիտուցիոնալ և քաղաքականության մակարդակներում՝ քննարկումներ վարելով լրագրողական համայնքի և քաղաքացիական հասարակության այն ներկայացուցիչների հետ, ովքեր ինտերնետն ու սոցիալական ցանցերն օգտագործում են իրենց համոզմունքներն ու իրենց ստեղծած բովանդակությունը առաջ տանելու նպատակով: Ֆոկուս խմբերի ուղեցույցը ներառված է կից փաստուղթ 5.1-ում:

Ֆոկուս խմբերի քննարկումների մասնակիցներ

ՖԽ-եր	Մասնակիցների տեսակը	ՖԽ-ի թիվը	Մասնակից ների թիվը ՖԽ-ում	Ընտրանքի տեսակը	Ընտրության չափանիշը (կին/տղամարդ)
ՖԽ1	Անհատ քաղաքացիական ակտիվիստներ	1	7	Նպատակային ընտրանք	5-կին/2 տղամարդ
ՖԽ2	ՀԿ ներկայացուցիչներ	1	7	Նպատակային ընտրանք	5-կին/2-տղամարդ
ՖԽ3	Լրագրողներ	1	6	Նպատատային ընտրանք	4-կին/2-տղամարդ

III. ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ ԵՎ ԱՐԴՅՈՒՆՔՆԵՐ

3.1. Հայաստանում մարդու իրավունքների և ազատությունների իրավական վերլուծությունը, որը հավասարապես կիրառելի է նաև կիբերտիրույթում

Հայաստանի օրենսդրությունը տարբերություն չի սահմանում առցանց և ինտերնետից դուրս իրավահարաբերությունների միջև, ոչ էլ առանձնացնում է անհատների թվային իրավունքներն ու ազատությունները: Այնուամենայնիվ, գործող իրավական ակտերի մեկնաբանությունը ենթադրում է այդ օրենքների կիրառելիությունը կիբերտիրույթում: Հայաստանը մի շարք միջազգային կազմակերպությունների անդամ է և ստորագրել է մարդու իրավունքների ոլորտում հիմնական միջազգային և տարածաշրջանային դաշնագրերը, ուստի իրավաբանորեն պարտավորված է կատարել ստանձնած պարտավորությունները՝ ներառյալ նրանք, որոնք ուղղակի կամ անուղղակի կերպով երաշխավորում են թվային միջավայրում իրավունքներն ու ազատությունները: Հայաստանը Միավորված ազգերի կազմակերպության անդամ է, ուստի միացել է նաև Քաղաքացիական և քաղաքական իրավունքների մասին միջազգային դաշնագրին (վավերացվել է 1993 թ. հունիսի 23-ին), որի 19-րդ հոդվածը սահմանում է «կարծիքներ ունենալու» և «տեղեկատվություն և գաղափարներ փնտրելու, ստանալու և հաղորդելու ազատություն՝ բոլոր միջոցներով և անկախ սահմաններից»: Որպես Եվրոպայում անվտանգության և համագործակցության կազմակերպության անդամ (1992 թ. հունվարից)՝ Հայաստանը ստանձնել է Հելսինկյան Եզրափակիչ ակտում և այլ հռչակագրերում սահմանված չափորոշիչները հարգելու պարտավորություն: Որպես Եվրոպայի խորհրդի անդամ պետություն՝ Հայաստանը ստորագրել (2001թ. հունվարի 25-ին) և վավերացրել է (2002 թ. ապրիլի 26) Մարդու իրավունքների եվրոպական կոնվենցիան (ՄԻԵԿ), որի 10-րդ հոդվածը պաշտպանում է կարծիք հայտնելու և արտահայտվելու ազատությունը:

2015 թ. դեկտեմբերին ընդունված ՀՀ Սահմանադրությունը ներառում է բոլոր հիմնարար իրավունքներն ու ազատությունները, որոնք ամրագրված են վերոհիշյալ միջազգային դաշնագրերում: Վենետիկի

հանձնաժողով անունով հայտնի «Ժողովրդավարություն՝ իրավունքի միջոցով» եվրոպական հանձնաժողովի կարծիքով ՀՀ Սահմանադրության 2015 թ. փոփոխությունները համապատասխանում են հիմնական միջազգային չափանիշներին: Սահմանադրության երկրորդ գլուխը (Մարդու և քաղաքացու հիմնարար իրավունքներն և ազատությունները), ի թիվս այլ իրավունքների, ամբողջությամբ նվիրված է այնպիսի իրավունքներին և ազատություններին, ինչպիսիք են՝ (1) արտահայտվելու ազատությունը, (մասնավոր կյանք և անձնական տվյալների պաշտպանություն), (3) տեղեկատվություն ստանալու իրավունքը: Մասնավորապես 31-րդ հոդվածը (Մասնավոր և ընտանեկան կյանքի, պատվի ու բարի համբավի անձեռնմխելիությունը) նախատեսում է, որ յուրաքանչյուր ոք ունի մասնավոր և ընտանեկան կյանքի, պատվի ու բարի համբավի անձեռնմխելիության իրավունք, որը կարող է սահմանափակվել միայն օրենքով՝ պետական անվտանգության, երկրի տնտեսական բարեկեցության, հանցագործությունների կանխման կամ բացահայտման, հասարակական կարգի, առողջության և բարոյականության կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով:

33-րդ հոդվածում (Հաղորդակցության ազատությունը և գաղտնիությունը) Սահմանադրությամբ ամրագրվում է բոլորի նամակագրության, հեռախոսային խոսակցությունների և հաղորդակցության այլ ձևերի ազատության և գաղտնիության իրավունքը: Հաղորդակցության ազատությունը և գաղտնիությունը կարող են սահմանափակվել միայն օրենքով՝ պետական անվտանգության, երկրի տնտեսական բարեկեցության, հանցագործությունների կանխման կամ բացահայտման, հասարակական կարգի, առողջության և բարոյականության կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով: Գաղտնալսման, միջամտության կամ հաղորդակցության գաղտնիության այլ սահմանափակումների թույլտվությունը կարող է տրվել միայն դատարանի որոշմամբ՝ օրենքով սահմանված նպատակներով:

Հայաստանի Սահմանադրությունը նաև տեղեկատվություն ստանալու իրավունքը սահմանում է որպես մարդու հիմնարար իրավունք (51-րդ հոդված), որը ուղղակիորեն կապված է պետական մարմինների թափանցիկությունն ու հաշվետվողականությունը ապահովելու հետ: Սահմանադրությամբ մասնավորապես ամրագրվում է, որ յուրաքանչյուր ոք ունի պետական և տեղական ինքնակառավարման մարմինների ու պաշտոնատար անձանց գործունեության մասին տեղեկություններ ստանալու և փաստաթղթերին ծանոթանալու իրավունք: Հոդվածի երկրորդ մասով նախատեսվում է, որ տեղեկություններ ստանալու իրավունքը կարող է սահմանափակվել միայն օրենքով՝ հանրային շահերի կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով:

Կարծիքի արտահայտման ազատությունը 42-րդ հոդվածով ամրագրված կարևոր սկզբունքներից է: Այն սահմանում է սեփական կարծիք ունենալու, ինչպես նաև առանց պետական և տեղական ինքնակառավարման մարմինների միջամտության և անկախ պետական սահմաններից՝ տեղեկատվության որևէ միջոցով տեղեկություններ ու գաղափարներ փնտրելու, ստանալու և տարածելու ազատությունը: Հարկ է նշել, որ այս նորմը տեխնոլոգիապես չեզոք է և տարբերություն չի սահմանում տեղեկատվության և հաղորդակցության միջոցների միջև: Այլ կերպ ասած, այն հավասարապես կիրառելի է կիբերտիրույթում խոսքի, լրատվամիջոցների և տեղեկատվության ազատության համար:

Միևնույն ձևակերպումներն առկա են 2012 թ. հունվարի 29-ին ՄԱԿ-ի Մարդու իրավունքների խորհրդի ընդունած՝ Ինտերնետում մարդու իրավունքների խթանման, պաշտպանության և կիրառման մասին բանաձևում: Արտահայտվելու ազատության սահմանափակումները կարող են սահմանվել միայն օրենքով՝ պետական անվտանգության, հասարակական կարգի, առողջության և բարոյականության կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով:

34-րդ հոդվածի համաձայն՝ յուրաքանչյուր ոք ունի իրեն վերաբերող տվյալների պաշտպանության իրավունք: Անձնական տվյալների մշակումը պետք է կատարվի բարեխղճորեն, օրենքով սահմանված նպատակով, անձի համաձայնությամբ կամ առանց այդ համաձայնության՝ օրենքով սահմանված այլ իրավաչափ հիմքի առկայությամբ: Յուրաքանչյուր ոք իրավունք ունի ծանոթանալու պետական և տեղական ինքնակառավարման մարմիններում իր մասին հավաքված տվյալներին և պահանջելու ոչ հավաստի տվյալների շտկում, ինչպես նաև ապօրինի ձեռք բերված կամ այլևս իրավական հիմքեր չունեցող տվյալների վերացում: Անձնական տվյալներին ծանոթանալու իրավունքը կարող է սահմանափակվել միայն օրենքով՝ պետական անվտանգության, երկրի տնտեսական բարեկեցության, հանցագործությունների կանխման կամ բացահայտման, հասարակական կարգի, առողջության և բարոյականության կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով: Անձնական տվյալների պաշտպանությանը վերաբերող մանրամասները սահմանվում են օրենքով (Հոդված 78): Վերջին կետի շրջանակներում Արդարադատության նախարարությունում գործում է Անձնական տվյալների պաշտպանության գործակալություն: Գործակալությունը, որպես լիազոր մարմին, պատասխանատու է անձնական տվյալների պաշտպանության ոլորտում օրենքի պահանջների կիրառումը վերահսկելու համար և մշակում է ուղեցույցներ, կարգավորումներ, ինչպես նաև տրամադրում է իրավաբանական աջակցություն:

ՄԻԵԿ-ի դրույթներին համապատասխան, ՀՀ Սահմանադրությունն ամրագրում է համաչափության սկզբունքը (Հոդված 78) և որոշակիության սկզբունքը (Հոդված 79), որոնք վերաբերում են հիմնարար իրավունքների և ազատությունների բոլոր սահմանափակումներին: Սահմանադրությամբ ամրագրվում է նաև հիմնարար իրավունքների և ազատությունների վերաբերյալ դրույթների էության անխախտելիությունը (Հոդված 80): Մյուս կողմից, Սահմանադրության 76-րդ հոդվածը հնարավոր է դարձնում վերոհիշյալ իրավունքների և ազատությունների սահմանափակումը արտակարգ կամ ռազմական դրության ժամանակ:

Հիմնարար իրավունքների ու ազատությունների կարգավորման նպատակով Սահմանադրության 75-րդ հոդվածով նախատեսվում է նաև, որ օրենքները նախատեսեն այդ իրավունքների և ազատությունների արդյունավետ իրականացման համար անհրաժեշտ կազմակերպական կառուցակարգեր և ընթացակարգեր: 75-րդ հոդվածի համաձայն՝ Հայաստանի օրենսդիր մարմինն ընդունել է հետևյալ օրենքները, որոնք վերաբերում են տեղեկատվության ազատությանը և որոնք կարող են կիբերտիրույթում կիրառվել և սահմանափակվել.

ՀՀ օրենքը զանգվածային լրատվության մասին, 13 դեկտեմբերի, 2003թ.

ՀՀ օրենքը տեղեկատվության ազատության մասին, 23 սեպտեմբերի, 2003թ.

ՀՀ օրենքը անձնական տվյալների պաշտպանության մասին, 18 մայիսի, 2015թ.

ՀՀ քրեական դատավարության օրենսգիրք, 1 հուլիսի, 1998թ.

ՀՀ քրեական օրենսգիրք, 18 ապրիլի 2003 թ.

ՀՀ օրենքը պետական և ծառայողական գաղտնիքի մասին, 3 դեկտեմբերի 1996թ.

ՀՀ օրենքը օպերատիվ-հետախուզական գործունեության մասին, 22 հոկտեմբերի 2007թ.

ՀՀ կառավարության որոշումը օպերատիվ-հետախուզական միջոցառումների անցկացման ընթացքում օգտագործվող հատուկ (մշակված, ծրագրված, հարմարեցված) տեխնիկական միջոցների ցանկը հաստատելու մասին, 31 հուլիսի 2008թ.

ՀՀ օրենքը էլեկտրոնային հաղորդակցության մասին, 13 օգոստոսի, 2005թ.

ՀՀ օրենքը հեղինակային իրավունքի և հարակից իրավունքների մասին, 15 հունիսի 2006թ.

ՀՀ օրենքը հեռուստատեսության և ռադիոյի մասին, 9 հոկտեմբերի, 2000թ.

3. 2 Ցանցի չեզոքություն

Հայաստանյան օրենսդրությունը չի սահմանում ցանցի չեզոքությունը, սակայն հեռահաղորդակցության օպերատորները և ծառայություն մատուցողները պարտավոր են հրապարակել և տեղեկացնել բաժանորդներին, եթե ցանցում չեն սատարում որոշ արձանագրություններ կամ առավելություն են տալիս որոշակի թրաֆիքին (ՀՀ Հանրային ծառայությունները կարգավորող հանձնաժողովի որոշում (471-N, սեպտեմբերի 8, 2008 թ.):

Արգելափակում/ֆիլտրում և ոչ օրինական բովանդակություն. Առցանց բովանդակության արգելափակումն ու ֆիլտրումը Հայաստանի օրենսդրությամբ չի կարգավորվում, և համապատասխան դատական պրակտիկա (նախադեպային իրավունք) դեռևս չի ձևավորվել: Ավելին՝ հանրային հաղորդակցության կամ հանրային ռեսուրսների մատչելիության սահմանափակումների մասին հաղորդումները Հայաստանի հաղորդակցության և մեդիա դաշտը կարգավորող օրենսդրության անորոշ ոլորտներից են:

Հայաստանը միացել է Կիբերհանցագործությունների մասին եվրոպական կոնվենցիային 2006 թ.-ին և պաշտոնապես հանձնառու է այդ մեխանիզմի իրականացմանը՝ որպես կիբերհանցագործությունների դեմ պայքարի լավագույն մոտեցում: Համապատասխանաբար Հայաստանը Քրեական օրենսգրքում փոփոխություններ է կատարել Կիբերհանցագործությունների մասին կոնվենցիայում նշված իրավախախտումները քրեականացնելու համար: Թեև Հայաստանը ստորագրել է Կոնվենցիան, կիբերհանցագործությունների մասին հանրության համար մատչելի շատ քիչ էմպիրիկ տվյալներ կան: Հետազոտության համար առկա չեն ո՛չ համակարգային և ո՛չ էլ վերլուծական տվյալներ: Սահմանափակ տեղեկատվություն կարելի է ստանալ Ոստիկանության, Գլխավոր դատախազության, անվտանգության մասնավոր ծառայությունների և ՋԼՄ-ների տարածած հայտարարություններից և մամուլի հաղորդագրություններից:

Քրեական օրենսգիրքը նախատեսում է բովանդակության ընդհանուր սահմանափակումներ՝ առանց նշելու տարածելու միջոցը: Մասնավորապես պոռնկագրական նյութերի տարածումը, ատելություն սերմանող

խոսքը և սահմանադրական կարգի տապալման մասին կոչերը դասակարգված են որպես քրեական հանցանքներ: Այնուամենայնիվ, Հայաստանի օրենսդրությամբ չի պահանջվում, որպեսզի հեռահաղորդակցության ծառայություն մատուցողները արգելափակեն կամ ֆիլտրեն առցանց բովանդակությունը:

Ինտերնետ հոսթինգ կամ ծառայություններ տրամադրողները, որոնք գրանցված են որպես տեղական ընկերություններ, ապօրինի բովանդակության համար պատասխանատվության կարող են ենթարկվել միայն այն դեպքերում, եթե ապացուցվի, որ նրանք նախապես տեղյակ են եղել այդ բովանդակության մասին: Նման իրավախախտումները դիտվում են կորպորատիվ պատասխանատվության շրջանակներում և հանգեցնում են միայն վարչական տուգանքի: Ավելին, այս ընկերությունները պարտավոր չեն հետևել հաղորդված կամ պահեստավորված բովանդակությանը, քանի որ օրենքով նման պարտավորություն սահմանված չէ: Այնուամենայնիվ, եթե օպերատորի համապատասխան պատասխանատու աշխատակիցը իր ցանկությամբ և գիտակցաբար, ուստի միտումնավոր կերպով տարածում է ապօրինի բովանդակություն, ինչպիսիք են պոռնկագրական նյութերը, նրան կարող են պատասխանատվության ենթարկել Քրեական օրենսգրքի 263-րդ հոդվածի դրույթներով:

Ի տարբերություն վերոհիշյալի, էլեկտրոնային ԶԼՄ-ները, այդ թվում՝ առցանց ռեսուրսներն ու հեռարձակող լրատվամիջոցները, հստակ պարտավորություն են կրում Զանգվածային լրատվության մասին օրենքով (Հոդված 7), ինչպես նաև Հեռուստատեսության և ռադիոյի մասին օրենքով (Հոդված 22, խոսքի ազատության սահմանափակումները զանգվածային լրատվամիջոցներում՝ ատելություն սերմանող խոսք, էրոտիկ/պոռնկագրական բովանդակություն, էթնիկ, կրոնական կամ ռասակայան խտրականություն, անչափահասների պաշտպանություն, պետական կամ օրենքով պաշտպանված այլ գաղտնիք) սահմանված բովանդակության համար:

Վերահսկում. Հայաստանում ապօրինի վերահսկման դեպքերը տարածում չունեն: Այնուահանդերձ իրավական միջավայրը իշխանությանը լայն իրավասություններով է օժտում լավ ձևավորված օրենսդրական շրջանակներում օրինական վերահսկում իրականացնելու համար: Սահմանադրության 33-րդ հոդվածը (Հաղորդակցության ազատությունը և գաղտնիությունը) ամրագրում է, որ «Յուրաքանչյուր ոք ունի նամակագրության, հեռախոսային խոսակցությունների և հաղորդակցության այլ ձևերի ազատության և գաղտնիության իրավունք, [….] որը կարող է սահմանափակվել միայն օրենքով՝ պետական անվտանգության, երկրի տնտեսական բարեկեցության, հանցագործությունների կանխման կամ բացահայտման, հասարակական կարգի, առողջության և բարոյականության կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով [….] միայն դատարանի որոշմամբ՝ ի բացառություն այն դեպքերի, երբ դա անհրաժեշտ է ազգային անվտանգության և և պայմանավորված է հաղորդակցվողների՝ օրենքով սահմանված առանձնահատուկ կարգավիճակով»:

Քրեական դատավարության օրենսգիրքը սահմանում է գաղտնիության սահմանները, ինչպես նաև հեռախոսազանգերի, նամակագրության և հաղորդակցության այլ միջոցների միջամտության կամ գաղտնալսման օրինական հիմքերը: Առանց դատարանի որոշման կամ միջամտության ենթարկվող անձի համաձայնության վերահսկումը համարվում է հանցանք:

Ազգային անվտանգության ծառայության գլխավոր վարչությունը միակ մարմինն է, որն իրավասու է վերահսկելու մասնավոր հաղորդակցությունն ու գաղտնալսելու հեռախոսային խոսակցությունները, ինչպես նաև մուտք ունենալու դեպի հեռախոսային օպերատորների տարածքում գտնվող սարքավորումները: Որևէ անհատի վերահսկելու/գաղտնալսելու համար հետախուզական մարմինը պետք է նախ ձեռք բերի դատարանի վճիռը: Հարկ է նշել, որ Քրեական դատավարության օրենսգիրքը (Հոդված 284) հստակ իրավական չափանիշներ չի նշում միջամտության մասին դատարանի որոշման համար, ոչ էլ հետախուզական մարմինների կողմից միջնորդություն ներկայացնելու համար: Գործնականում դատավորները նման միջնորդությունները քննում են ըստ կոնկրետ դեպքի, արդյունքում դատարանի որոշումներին պակասում է հետևողականությունը և կանխատեսելիությունը:

Օպերատիվ հետախուզական գործունեության համար անհրաժեշտ հատուկ տեխնիկական միջոցների ցանկը սահմանվում է Կառավարության որոշմամբ, որտեղ նշված են այն գործիքներն ու հավելվածները, որոնք անրաժեշտ են օրինական վերահսկում իրականացնելու համար: Տեխնոլոգիական պահանջների ցանկը բավականին լայն է: Ցանկով թույլատրվում է տեխնիկական գործիքների մշակումը, այդ թվում՝ նաև ծրագրային, որոնք ստեղծված են համակարգչային ցանցեր և համակարգեր ներթափանցելու, տեղեկատվություն կորզելու և էլեկտրոնային հաղորդակցությունների բոլոր տեսակներին միջամտելու համար, այդ թվում՝ տեքստային, ձայնային և մուլտիմեդիա բովանդակությանը: Հայաստանի իշխանությունները առաջադեմ տեխնիկական հմտություններ են զարգացնում՝ առցանց գործունեությունը վերահսկելու և հետախուզելու համար, թեև մշակված է նաև ստուգիչ և հավասարակշռող մանրակրկիտ օրենսդրական դաշտ՝ ապահովելու պետության կողմից այս իրավասությունների չարաշահման կանխումը: Հեռահաղորդակցության օպերատորները պարտավոր են համապատասխան մարմիններին տրամադրել օպերատիվ-հետախուզական միջոցառումներ իրականացնելու համար աջակցություն և հարմարություններ: Ավելին, «Օպերատիվ-հետախուզական գործունեության մասին» ՀՀ օրենքի 31-րդ հոդվածի համաձայն հեռահաղորդակցության և փոստային ընկերությունները պարտավոր են Ազգային անվտանգության ծառայության գլխավոր վարչության պահանջով տրամադրել տեխնիկական համակարգեր և անհրաժեշտ պայմաններ ստեղծել օպերատիվ-հետախուզական միջոցառումներ իրականացնելու համար: Վերջին պահանջը կարող է մեկնաբանվել (և ամենայն հավանականությամբ մեկնաբանվում է) որպես հստակ պահանջ առ այն, որ հաղորդակցության օպերատորները վերահսկման սարքավորումները տրամադրեն իրենց հաշվին: Բացառիկ դեպքերում, երբ վերահսկումը անհրաժեշտ է անմիջապես կամ նրա հապաղումը կարող է հանգեցնել ահաբեկչական ակտի կատարման կամ պետական, ռազմական կամ բնապահպանական անվտանգությանը սպառնացող իրադարձությունների, հետախուզական մարմնի ղեկավարը կարող է պահանջել, որպեսզի Ազգային անվտանգության ծառայության գլխավոր վարչությանը տեղեկատվության մատչելիությունն ապահովվի դատարանի որոշումից 48 ժամ առաջ: Եթե դատարանը մերժում է միջնորդությունը, հետախուզական մարմինը պետք է անմիջապես ոչնչացնի ձեռք բերված տվյալները (Քրեական դատավարության օրենսգիրք, Հոդված 284): Հետախուզական մարմիններին չի թույլատրվում պահպանել կամ բացահայտել տվյալները՝ բացի օրենքով նախատեսված դեպքերից (Էլեկտրոնային հաղորդակցության մասին օրենք, Հոդված 50):

Մասնավոր տվյալների պաշտպանություն/հաղորդակցության գաղտնիություն

Անձնական տվյալների պաշտպանության մասին օրենքն ընդունվել է 2015 թ. մայիսի 18-ին՝ ի կատարումն Եվրոպայի խորհրդի «Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին» կոնվենցիայի (108) պահանջների: Օրենքը կարգավորում է պետական կառավարման կամ տեղական ինքնակառավարման մարմինների, պետական կամ համայնքային հիմնարկների կամ կազմակերպությունների, իրավաբանական կամ ֆիզիկական անձանց կողմից անձնական տվյալները մշակելու, դրանց նկատմամբ պետական հսկողություն իրականացնելու կարգն ու պայմանները: Ստեղծվել է նաև Անձնական տվյալների պաշտպանության գործակալություն, որը օրենքով սահմանված իրավունքի պաշտպանությամբ զբաղվող լիազոր մարմին է: Օրենքը սահմանում է անձնական տվյալների մշակման հիմնական սկզբունքները, այդ թվում.

(1) Օրինականության սկզբունք. Անձնական տվյալները մշակվում են օրինական և որոշակի նպատակներով և առանց տվյալների սուբյեկտի համաձայնության չեն կարող օգտագործվել այլ նպատակներով:

(2) Համաչափության սկզբունք. Տվյալների մշակումը պետք է ունենա օրինական նպատակ, դրան հասնելու միջոցները պետք է լինեն պիտանի, անհրաժեշտ և չափավոր՝ այն նվազագույն քանակով, որն անհրաժեշտ է օրինական նպատակներին հասնելու համար: Արգելվում է այնպիսի անձնական տվյալների մշակումը, որոնք անհրաժեշտ չեն տվյալները մշակելու նպատակի համար կամ անհամատեղելի են դրա հետ: Արգելվում է անձնական տվյալների մշակումը, եթե տվյալները մշակելու նպատակին հնարավոր է հասնել ապանձնավորված կերպով: Անձնական տվյալները պետք է պահպանվեն այնպես, որ բացառվի տվյալների սուբյեկտի հետ դրանց նույնականացումն ավելի երկար ժամկետով, քան անհրաժեշտ է դրանց նախօրոք որոշված նպատակներին հասնելու համար:
(3) Հավաստիության սկզբունք. Մշակվող անձնական տվյալը պետք է լինի ամբողջական, ճշգրիտ, պարզ և հնարավորինս թարմացված:

(4) Սուբյեկտների նվազագույն ներգրավման սկզբունքը. Այն դեպքում, երբ պետական կառավարման կամ տեղական ինքնակառավարման մարմինը, նոտարը միասնական էլեկտրոնային տեղեկատվական համակարգի միջոցով կարող են անձնական տվյալը ձեռք բերել այլ մարմնից, ապա անձնական տվյալների սուբյեկտից չի պահանջվում ներկայացնել որոշակի գործողությունների համար անհրաժեշտ անձնական տվյալը: Անձնական տվյալների սուբյեկտի գրավոր համաձայնության դեպքում անձնական տվյալներ մշակող համարվող ֆիզիկական կամ իրավաբանական անձինք կարող են պետական կամ տեղական ինքնակառավարման մարմնից ստանալ որոշակի գործողության համար անհրաժեշտ և անձնական տվյալների սուբյեկտի գրավոր համաձայնության մեջ ուղղակիորեն մատնանշված անձնական տվյալը:

«Էլեկտրոնային հաղորդակցության մասին ՀՀ օրենքը» սահմանում է այն հանգամանքները, որոնց առկայության պարագայում ծառայություն տրամադրողները կարող են կամ պետք է տրամադրեն իրենց օգտագործողների անձնական տվյալները: Այդ հանգամանքները հետևյալն են.

«Հոդված 49. Հաճախորդների տեղեկությունների գաղտնիությունը

[…] 2. Օպերատորը կամ ծառայություններ մատուցողն իրավասու է բացահայտել այդ տեղեկությունները՝

1) օրենքով նախատեսված դեպքերում և կարգով՝ քրեական հանցագործության կամ ազգային անվտանգության նկատմամբ որևէ սպառնալիքի հետախուզման, հետաքննման կամ քրեական հետապնդման առնչությամբ.

2) հաճախորդի գրավոր համաձայնության հիման վրա.

3) եթե բացահայտումն անհրաժեշտ է ի պաշտպանություն օպերատորի կամ ծառայություններ մատուցողի (ընթանում են վարույթներ ընդդեմ այդ օպերատորի կամ ծառայություններ մատուցողի): Հաճախորդը կարող է պահանջել, որպեսզի բացահայտումը կատարվի գաղտնիության կարգով՝ դռնփակ վարույթների միջոցով»:

Որպես հիմնական կանոն՝ հեռահաղորդակցության օպերատորներին չի թույլատրվում պահեստավորել կամ բացահայտել հաղորդակցությունը (բովանդակությունը)՝ բացառությամբ օրենքով սահմանված դեպքերի: Այսպիսով, «Էլեկտրոնային հաղորդակցության մասին» ՀՀ օրենքի 50-րդ հոդվածը սահմանում է, որ. «Էլեկտրոնային հաղորդակցության ցանկացած միջոցով փոխանցվող հաղորդագրության կողմ չհանդիսացող որևէ անձ կարող է միջամտել, ձայնագրել հաղորդագրությունը կամ բացահայտել դրա պարունակությունը միայն տվյալ հաղորդագրության կողմերի գրավոր համաձայնությամբ կամ դատարանի որոշմամբ՝ օրենքով նախատեսված դեպքերում և կարգով:»

Իրավական պաշտպանությունը. Անհատական իրավունքների պաշտպանությունն իրականացվում է դատարանին, իրավապահ մարմիններին, պատասխանող մարմնի վերադաս մարմին, մասնագիտացված մարմիններին, ինչպիսին է՝ Անձնական տվյալների պաշտպանության գործակալությունը կամ Մարդու իրավունքների պաշտպանի գրասենյակին հայցադիմումներ, դիմումներ և բողոքներ ներկայացնելու միջոցով: Բացի ներպետական օրենսդրությունից՝ անհատական իրավունքների պաշտպանության շրջանակներում որպես դրական պարտավորություն Հայաստանի համար սահմանված է առաջատար դեր ստանձնել անհատական իրավունքների իրականացման հարցում թե՛ առցանց և թե՛ ցանցից դուրս միջավայրում:

Մասնավորապես առցանց իրավունքների պաշտպանությունը ամրագրված է միջազգային իրավական փաստաթղթերով, ինչպիսին է Եվրոպայի խորհրդի նախարարների խորհրդի՝ անդամ պետություններին ուղղված *CM/Rec(2014)6 հանձնարարականը՝ Ինտերնետի օգտագործողների համար Մարդու իրավունքների ուղեցույցի մասին*, որտեղ նշվում է՝. «*Իրենց իրավասության ներքո գտնվող յուրաքանչյուր մարդու համար ապահովել Մարդու իրավունքների եվրոպական կոնվենցիայով ամրագրված իրավունքներն ու ազատությունները (ETS No. 5, Կոնվենցիա): Այս իրավունքները ուժի մեջ են մնում նաև ինտերնետի օգտագործման համատեքստում: Եվրոպայի խորհրդի այլ կոնվենցիաներն ու գործիքները, որոնք առնչվում են խոսքի ազատության պաշտպանության իրավունքին, տեղեկատվության մատչելիությանը, հավաքների ազատության իրավունքին, կիբերհանցագործություններից պաշտպանությունը և մասնավոր կյանքի իրավունքն ու անձնական տվյալների պաշտպանությունը նույնպես կիրառելի են*»:

Միջազգային չափանիշներ/առաջարկություններ

Ներկայում թվային գործիքներն ու տեխնոլոգիաները լուրջ մարտահրավերներ են բերում մարդու հիմնարար իրավունքների իրացման համար, հատկապես՝ մասնավոր կյանքի գաղտնիության, խոսքի, լրատվամիջոցների ազատության և հարակից իրավունքների համար: Մեկ անձի արտահայտվելու իրավունքը կարող է խախտել մյուսի մասնավոր կյանքի գաղտնիության իրավունքը, կամ ազգային անվտանգության հետ կապված մտահոգությունները կարող են հակադրվել քաղաքացիական ազատությունների հետ: Թվային տեխնոլոգիաների ներթափանցումը ավելի ու ավելի շատ մարդկանց առօրյա ավելի է թեժացնում այս լարվածությունը: Թեև թվային տեխնոլոգիաները առանցքային դեր ունեն արտահայտման ազատության և տեղեկատվության տարածման համար, դրանց օգտագործումը նաև զգալիորեն բարձրացնում է իրավունքերի խախտման և ազատությունների սահմանափակման հավանականությունը: Թվային տեխնոլոգիաները հատկապես լուրջ խնդիրներ են ստեղծում մասնավոր կյանքի իրավունքի իրականացման համար, քանի որ անձնական տվյալները կարելի է հավաքել և տարածել աննախադեպ ծավալով և նվազագույն ծախսերով թե' ընկերությունների և թե' պետությունների համար: Միևնույն ժամանակ անձնական տվյալների պաշտպանության օրենքների կիրառումը և մասնավոր կյանքի գաղտիությունը պաշտապանելուն ուղղված այլ միջոցառումներ կարող են անհամաչափ ազդեցություն ունենալ խոսքի ազատության օրինական կիրառման վրա:

Այս հարցերին անդրադառնալու, վերոնշյալ երկու հակադիր հասկացությունների հատման կետը գտնելու և հավասարակշռված մոտեցում ձևավորելու համար անհրաժեշտ է միավորել հանրության ջանքերը: Բարեբախտաբար, համաշխարհային համայնքը ձգտում է համընդհանուր թվային իրավունքներ մշակել՝ նպատակ ունենալով ձևակերպել ինտերնետում իրավունքների կանոններ կամ ինտերնետի Մագնա Կարտա, որը թվային դարաշրջանում իրավունքների նոր շարք կսահմանի: Ստորև ներկայացված են թվային իրավունքների այն հիմնական չափանիշները, որոնք կարող են դիտակարկվել Հայաստանի հանրության կողմից.

- **Միջցանցային փոխազդեցության իրավունք**. Յուրաքանչյուր ոք իրավունք ունի օգտվելու ինտերնետի ճարտարապետական կառուցվածքից, որը հիմնված է ապակենտրոնացման, բաց գործելակերպի, համատեղելիության և փոպկապակցվածության սկզբունքի վրա:

- **Մատչելիության իրավունք**. Յուրանքանչյուր ոք իրավունք ունի տեղեկատվական հասարակության մաս լինելու և, անկախ աշխարհագրական վայրից, օգտվելու ինտերնետային ծառայություններից՝ ողջամիտ գնով:

- **Ցանցի չեզոքություն.** Յուրաքանչյուր ոք իրավունք ունի ստանալու ինտերնետի անդրսահմանային թրաֆիքի անխոչընդոտ հոսք:

- **Անանուն հանդես գալու իրավունք.** Յուրաքանչյուր ոք իրավունք ունի ինտերնետից օգտվելիս մնալու չբացահայտված և չբացահայտելու սեփական ինքնությունը:

- **Գաղտնագրման իրավունք.** Յուրաքանչյուր ոք իրավունք ունի օգտագործելու հաղորդակցության ապահով գործիքներ, մասնավորապես գաղտնագրման սարքեր և ծրագրեր և այլ կրիպտոգրաֆիկ մեթոդներ՝ սեփական ընտրությամբ:

- **Վերահսկումից ազատ լինելու իրավունք.** Յուրաքանչյուր ոք իրավունք ունի վերահսկումից, միջամտությունից և պետության, առևտրային կազմակերպությունների և այլ մարմինների կողմից դիտարկումից ազատ լինելու իրավունք:

- **Բլոգ վարելու իրավունք.** Յուրաքանչյուր ոք ունի ինտերնետի և թվային տեխնոլոգիաների օգնությամբ տեղեկատվություն և գաղափարներ տարածելու իրավունք՝ առանց թույլտվության, արտոնագրի կամ գրանցման:

- **Ստեղծագործելու իրավունք.** Յուրաքանչյուր ոք ունի առցանց բովանդակություն ստեղծելու իրավունք:

- **Տարածելու իրավունք.** Յուրաքանչյուր ոք ունի առցանց միջավայրում մշակութային բարիքները ստանալու, հաղորդելու և անձամբ վայելելու իրավունք:

- **Թվային ցույցերի իրավունք**. Յուրաքանչյուր ոք ունի թվային գործիքների օգտագործման միջոցով անհատական կամ խմբային ցույցերին մասնակցելու իրավունք:

- **Հակադրվելու, վիրավորելու և վիրավորվելու իրավունք.** Յուրաքանչյուր ոք իրավունք ունի թվային տեխնոլոգիաների օգտագործման միջոցով արտահայտելու, տարածելու և ստանալու ընդդիմադիր, այլախոհ, ակտիվ և ճկուն տեսակետներ և արժեքներ:

- **Պատասխանատվությունից ազատ լինելու իրավունք.** Յուրաքանչյուր ոք ունի այլոց առցանց բովանդակության համար պատասխանատվությունից ազատ լինելու իրավունք: Այս իրավունքը ներառում է պատասխանատությունից անձեռնմխելիությունը հետևյալ դեպքերում՝
  ա) երրորդ կողմերի բովանդակությունը, որը փոփոխելու գործում ներգրավվածություն չի եղել,
  բ) օրինական բովանդակությունը սահմանափակել չկարողանալը,
  գ) երրորդ կողմերի ապօրինի բովանդակությունը ստանալը,
  դ) այլոց բովանդակությանը պրոակտիվ ձևով հետևել չկարողանալը:

- **Հաքերության իրավունք.** Յուրաքանչյուր ոք ունի հանրային շահ հետապնդելով և ոչ առևտրային նպատակով ուսումնասիրելու և կոտրելու թվային ծածկագրերը, մասնավորապես՝ հաղթահարելու տեխնոլոգիական խոչընդոտները, որոնք թույլ չեն տալիս ստանալ այն բովանդակությունը, որը պետք է լիներ հասանելի և մատչելի:

- **(ՎՄՅ) Ինքնուրույն գործունեության իրավունք**. Յուրաքանչյուր ոք ունի սեփական սերվերներն ու ծառայությունները աշխատեցնելու, վիրտուալ մասնավոր ցանց ստեղծելու և ցանցում այլոց ծառայություններ տրամադրելու իրավունք:

- **Ազատ և բաց ծրագրային ապահովման իրավունք**. Յուրաքանչյուր ոք իրավունք ունի մուտք գործելու և օգտվելու ազատ և բաց ծրագրային ապահովումից:

- **Տվյալները տնօրինելու իրավունք.** Յուրաքանչյուր ոք ունի իր անձնական տվյալները լիարժեք տնօրինելու իրավունք: Անձնական տվյալները կարող են մշակվել միայն այն դեպքում, երբ անձը տալիս է մշակման համար իր լիարժեք և իրազեկ համաձայնությունը**:**

- **Գիտելիքները զարգացնելու իրավունք.** Յուրաքանչյուր ոք ունի թվային միջավայրում իրենց իրավունքները կիրառելու նպատակով անվճար թվային կրթության և գիտելիքի իրավունք:

- [Մասնակցության իրավունք](). Յուրաքանչյուր ոք ունի իրազեկ ընտրության և ինտերնետի կառավարմանը մասնակցելու, մասնավորապես՝ կառավարման մեխանիզմների և ինտերնետին առնչվող հանրային քաղաքականության մշակմանը ազատ և վստահ մասնակցելու իրավունք:

3. 3 Թիրախ խմբի՝ մեդիա մասնագետների և քաղաքացիական հասարակության ներկայացուցիչների՝ ինտերնետի ազատության և կիբերանվտանգության մասին գիտելիքն ու փորձը

Զուր չէ, որ լրագրողներն ու շահերի պաշտպանությամբ զբաղվող անձինք անհանգստանում են իրենց թվային անվտանգության և ցանցում ազատության համար: Թեև համակարգիչն ու ինտերնետը կարող են իսկապես օգտակար գործիք լինել անհրաժեշտ տեղեկատվությունը հավաքելու և տարածելու, ինչպես նաև տարբեր նպատակների առաջխաղացման համար, դրանք նաև նոր սպառնալիքների են ենթարկում վերոհիշյալ խմբերին: Որքան այս խմբերը շատ են օգտագործում նոր տեխնոլոգիաներն ու ինտերնետը իրենց ուսումնասիրությունների, բովանդակության մշակման և հանրային ներգրավման նպատակներով, այնքան մեծանում են ռիսկերը: Այս ամենը հաշվի առնելով՝ մենք թիրախ խմբի լրագրողների և քաղհասարակության ներկայացուցիչների հետ մեր հարցազրույցներն ու քննարկումները սկսեցինք հիմնական հարցից՝ իրենց առօրյա աշխատանքի և հաղորդակցության որքա՞ն մասն են իրականացնում ինտերնետի միջոցով և արդյո՞ք իրենց համարում են ինտերնետի վարժ օգտատերեր:

Ֆոկուս խմբի մասնակիցներն ու հարցազրույցներին մասնակցած լրագրողները/քաղաքացիական ակտիվիստները սովորաբար իրենց ներկայացնում էին որպես ոչ այնքան վարժ օգտատերեր, չնայած այն հանգամանքին, որ ինտերնետն օգտագործում են թե՛ մասնագիտական և թե՛ անձնական նպատակների համար: Այսօր արդեն նրանք դժվարանում են իրենց կյանքը պատկերացնել առանց Facebook, Twitter, Skype, WhatsApp, Viber և այլ սոցիալական կայքերի և հաղորդակցության հարթակների: Այնուամենայնիվ, նրանք չնշեցին, որ ունեն լավ կամ խորը գիտելիքներ և հմտություններ իրենց սարքերի, հաշիվների և աղբյուրների անվտանգությունն ապահովելու համար: Հարցազրույցին մասնակցած լրագրողների և քաղհասարակության ներկայացուցիչների զգալի մասը պատասխանատու է իրենց կայքերում նոր բովանդակության թարմացման և վերբեռնման համար: Նրանցից բոլորն էլ իրենց աշխատանքին առնչվող

ուսումնասիրությունների համար օգտագործում են ինտերնետը՝ ամեն օր հանդիպելով նոր վեբկայքերի և առցանց ռեսուրսների և գնահատելով դրանց վստահելիությունը: Վերջապես նրանք կապ են պահպանում իրենց աղբյուրների, հիմնական տեղեկացնողների և շահառուների/շահագրգիռ անձանց հետ հաղորդակցության վերը նշված խողովակների միջոցով, ուստի նրանց պետք է մտահոգի իրենց տեղեկատվության և աղբյուրների գաղտնիությունն ու պաշտպանությունը:

Հայաստանի լրագրողների և քաղհասարակության անդամների գիտելիքների և հմտությունների մակարդակը (ինչպես հենց իրենք են նշում) բարելավման մեծ կարիք ունի: Նրանցից շատերը փորձում են օգտագործել երկար և բարդ ծածկագրեր և հաճախ էլ միացնում են ինքնության հաստատման երկաստիճան համակարգը՝ իրենց հաշիվներ մուտք գործելու համար: Նրանք հետևում են նաև միևնույն ծածկագիրը բոլոր հաշիվների համար չօգտագործելու կամ 1-2 ամիսը մեկ ծածկագիրը փոխելու պարզ պահանջներին: Նրանցից շատերը նշեցին նաև, որ տեղեկատվության նոր աղբյուրներ գտնելու նպատակով ինտերնետն ուսումնասիրելիս զգուշություն են ցուցաբերում՝ հանդիպելով անծանոթ հասցեների: Բայց սա անվտանգության միջոցների այն ամբողջական ցանկն է, որին հետևում են թիրախ խմբի անդամները: Նրանցից միայն քչերը նշեցին, որ իրենց շարժական սարքերն ունեն ծածկագրեր, և նրանց շրջանում միայն մի քանիսը գիտեին, թե ինչ պետք է անել, եթե նրանց շարժական սարքերը, որոնք լի են զգայուն տեղեկատվությամբ և կոնտակտային տվյալներով, առգրավեն, գողանան և/կամ կորչեն:

Հարցազրույցների մասնակցած բոլոր լրագրողներն ու քաղհասարակության ներկայացուցիչները, ինչպես նաև ֆոկուս խմբերի մասնակիցները իրական պատմություններ են լսել հանրային Wi-Fi-ի օգտագործումից բխող ռիսկերի մասին: Այնուամենայնիվ, սա նրանցից շատերին հետ չի պահում ժամանակ առ ժամանակ հանրային Wi-Fi-ից օգտվելուց, եթե կա դրա շտապ անհրաժեշտությունը՝ առանց լիովին իրազեկ լինելու իրենց տեղեկատվական թրաֆիքի և տվյալների վրա դրա հետևանքների և ռիսկերի մասին և առանց գիտակցելու, որ դրա արդյունքում կարող է հեշտությամբ տեղի ունենալ իրենց անձնական և կազմակերպության տվյալների արտահոսք:

Բացառությամբ մի քանի դեպքերի, երբ կազմակերպությունը հանրային Wi-Fi օգտագործման հետ կապված խիստ քաղաքականություն ունի, հարցազրույցին մասնակցած լրագրողների/քաղհասարակության ներկայացուցչների մեծ մասն ընդունեց, որ շտապել են ցանցին միանալ ոչ միայն գործնական, այլև անձնական պատճառներով:

Հարզազրույցին մասնակցած բոլոր լրագրողներն ու ակտիվիստները համոզված են, որ իրենց ներկայացրած կազմակերպությունն օգտագործում է արտոնագրված ծրագրային փաթեթներ և ծրագրեր, բայց քչերը նշեցին, որ նման ծրագրեր ունեն իրենց շարժական սարքերում: Այնուամենայնիվ, Հայաստանի SS անվտանգության փորձագետների հետ ունեցած հարցազրույցներից կատարած եզրահանգումները և Սոֆթվեյր Ալիանսի կողմից վերջերս տրամադրված վիճակագրությունը լիովին կասկածի տակ է դնում այն վստահությունը, որը լրագրողներն ու ՀԿ-ների ներկայացուցիչներն ունեն իրենց կազմակերպությունների LAN ցանցերում օգտագործվող ծրագրերի վերաբերյալ: BSA-ի՝ համակարգչային ծրագրերի համաշխարհային ուսումնասիրության (2015) համաձայն՝ Հայաստանում չարտոնագրված ծրագրերի օգտագործումը հասնում է 86%-ի՝ ամբողջ աշխարհում ընդհանուր 39%-ի համեմատ: Բացատրությունները, թե ինչու են ընկերություններն ու անհատները չարտոնագրված ծրագրերը նախընտրում արտոնագրվածից

կարող են բարդ լինել, բայց դրանք կարելի է դասակարգել հետևյալ երկու պատճառաբանությունների խմբում՝ ֆինանսական միջոցների սղություն և SS անվտանգության ռիսկերի անբավարար գնահատում: ԶԼՄ-ների և ՀԿ-ների միայն մի քանի ներկայացուցիչներ նշեցին, որ իրենց կազմակերպությունները գործարկում են բաց աղբյուրներով օպերացիան համակարգեր, մասնավորապես՝ Ubuntu/Linux, մնացած մեծ մասը դեռևս օգտագործում են Windows:

Հարցազրույցներին և ֆոկուս խմբերին մասնակցած միայն մի քանի լրագրողներ և քաղհասարակության ներկայացուցիչներ նշեցին, որ իրենց թվային ինքնությունը պաշտպանելու համար օգատագործում են Tor դիտարկիչ՝ չնայած այն անհարմարությանը, որ բերում է ինտերնետի ավելի դանդաղ աշխատանքը: Մի քանի պատասխանողներ նույնիսկ նշեցին, որ իրենց գործընկերների, աղբյուրների և տարբեր շահագրգիռ կողմերի հետ շփվելիս օգտագործում են PGP գաղտնագրման գործիքներ (հիմնականում Mailvelope և հազվադեպ՝ FTP վիդեո ներբեռնիչ) և ստիպված էին դա անել, որովհետև դա էր իրենց արտասահմանյան կամ միջազգային գործընկերների, համագործակցող կողմերի պահանջը: Նրանք, ովքեր նախընտրում են գաղտնագրում չօգտագործել, կարծում են, որ դա ավելի շատ ժամանակ է խլում հաղորդագրություններ ուղարկելու/ստանալու/ապակոդավորելու համար, նրանք գտնում են նաև, որ մեծ ջանքեր են պահանջվում գաղտնագրման և տվյալների գաղտնիության պահպանման այլ գործիքներն օգտագործելու համար:

Հարցազրույցներին և ֆոկուս խմբերին մասնակցած լրագրողները համաձայն էին, որ ամենից շատ ինքնագրաքննությունն է օգնում անցանկալի ուշադրությունից, ինտերնետում և հատկապես սոցիալական ցանցերում հարձակումներից պաշտպանվելու հարցում: Սա մի բան է, որ արվում է այլոց համար զգայուն թեմաներ շոշափելու վախից ելնելով՝ փորձելով մնալ նրանց իրական կամ ենթադրյալ նախընտրությունների շրջանակներում (հատկապես քաղաքական գործիչների և բիզնես ուժերի)՝ առանց կոնկրետ հաստատության կամ իշխանությունների կողմից ակնհայտ ճնշման: Ֆոկուս խմբերի քննարկումների ընթացքում, սակայն, լրագրողները իրական դեպքեր ներկայացրին սոցիալական ցանցերում իրենց հաշիվների վրա շարունակական հարձակումների մասին (շատ հաճախ կեղծ հաշիվներից), պարզապես որովհետև որևէ անհատի կամ խմբի դուր չի եկել իրենց տարածած բովանդակությունը (դիտարկում, տեսանյութ կամ լուսանկար): Լրագրողները հաճախ դիմել են լրատվական նյութերի ինքնագրաքննության՝ դրանցում ներգրավված անձանց անվտանգության հետ կապված մտավախություններից ելնելով:

Իրավական տեսանկյունից ՀՀ Սահմանադրությունը երաշխավորում է խոսքի, տեղեկատվության և ԶԼՄ-ների ազատությունը և ընդհանուր առմամբ օրենսդրությունը բավականին ազատական է համարվում, սակայն կան այդ ազատությունների իրականացումը խոչընդոտող ռիսկեր: Դրա ապացույցներից մեկն այն է, որ 2008 թ. իր պաշտոնավորումն ավարտող ՀՀ Նախագահի կողմից երկրում հայտարարված արտակարգ դրության պայմաններում Հայաստանի պատմության մեջ առաջին անգամ ԶԼՄ-ներին պահանջ ներկայացվեց պետական և ներքաղաքական թեմաների մասին հրապարակել միայն «պետական մարմինների տրամադրած պաշտոնական տեղեկատվությունը»: 2016 թ. Երևանում քաղաքական պատանդառության ճգնաժամի շուրջ կազմակերպված ցույցերի արդյունքում ձևավորված քաղաքացիական ընդվզումների ընթացքում Ֆեյսբուք սոցիալական ցանցը մոտ մեկ ժամ անհասանելի էր: Բացի այդ՝ թիրախավորվեցին տեղում ուղիղ հեռարձակմամբ իրենց մասնագիտական գործունեությունն իրականացնող լրագրողները, խոչընդոտվեց լուսաբանումը: Այս ամենի արդյունքում «Ֆրիդոմ Հաուսի»

«Ազատությունը ցանցում 2017» զեկույցում Հայաստանը երկու միավոր կորցրեց՝ դասվելով մասնակի ազատ երկրների շարքում: Այս հանգամանքը բացասաբար է անդրադառնում Հայաստանի ժողովրդավարության պատկերի վրա, եթե չխոսենք Մամուլի ազատության իրավիճակի մասին, որը 2003 թ. սկսած գնահատվում է որպես անազատ: Կարգավիճակի նման անկումը պայմանավորված էր երկրի առաջատար անկախ հեռուստաընկերությունը՝ A1+-ը փակելով և կառավարության՝ մամուլում քննադատական խոսքը լռեցնելու համառ ջանքերով: Վերոնշյալի ենթադրվող պատճառը իշխանության տարբեր ճյուղերի միջև ստուգման և հավասարակշռման պակասն է, հանրային մասնակցության և քաղաքացիական հասարակության ինստիտուցիոնալ կարողությունների ցածր մակարդակը: Իբրև ամփոփում, ինտերնետի ազատության վիճակը ոչ միայն իրավական միջավայրի արտացոլումն է, այլև քաղաքական իրականություն է, որը կարող է ուղղակիորեն անդրադառնալ օրենքով երաշխավորված ազատությունների վրա:

3. 4 Մարդու իրավունքները ցանցում և ցանցից դուրս. եթե դրանք նույնը չեն, ապա որտե՞ղ են հատվում: Վերջին տասնամյակում Հայաստանի տարածքում ինտերնետի սահմանափակումները:

Համարյա մեկ տարի է անցել, ինչ ինտերնետի մատչելիությունը հռչակվել է որպես մարդու իրավունք, իսկ խախտումները դեռևս շարունակվում են: 2016 թ. հուլիսին ընդունած A/HRC/32/L.20 Բանաձևում ՄԱԿ-ի Մարդու իրավունքների խորհուրդը ինտերնետը բնութագրել է որպես «մարդկային առաջընթացը խթանելու հզոր ներուժ»՝ դատապարտելով «այն միջոցները, որոնք ուղղված են առցանց տեղեկատվության մատչելիության կամ տարածման միտումնավոր կանխմանը»: Պարտադիր ուժ չունեցող այս բանաձևն ընդգծել է, որ գնալով աճում է ինտերնետում մարդու իրավունքների իրացման (մասնավորապես խոսքի ազատության) նկատմամբ հետաքրքրությունն ու կարևորությունը: Վերջին մի քանի տարիների ընթացքում Մարդու իրավունքների խորհուրդը (ՄԻԽ) նշել է, որ այն իրավունքները, որոնցով անհատն օժտված է ցանցից դուրս, կիրառելի են նաև առցանց միջավայրում: Այնուհանդերձ մարդու իրավունքների մասին միջազգային և ներպետական օրենքներում շատ քիչ բան կա (եթե առհասարակ կա), որը կարձանագրեր, որ յուրաքանչյուր ոք ունի ինտերնետի իրավունք: Միակ անդրադարձը Մարդու իրավունքների համընդհանուր հռչակագիրն է և Քաղաքացիական և քաղաքական իրավունքների միջազգային դաշնագիրը, որոնց 19-րդ հոդվածը ներառում է համապատասխան չափորոշիչը և նշում, որ «յուրաքանչյուր ոք ունի կարծիքի և արտահայտվելու ազատություն: Այս իրավունքը ներառում է առանց միջամտությունների կարծիքներ ունենալու և տեղեկատվություն և գաղափարներ փնտրելու, գտնելու և տարածելու ազատությունը բոլոր միջոցներով՝ անկախ սահմաններից»:

Որպեսզի հասկանանք, թե սա ինչ է նշանակում Հայաստանում գործող լրագրողների, քաղհասարակության ներկայացուցիչների և SS անվտանգության փորձագետների համար, մենք այս թեմայով քննարկում անցկացրինք խորքային հարցազրույցների և ֆոկուս խմբերի հանդիպումների ընթացքում: Որքանո՞վ է ինտերնետի մատչելիությունը մարդու իրավունք: Արդյո՞ք այն հիմնարար իրավունքները, որոնք մարդն ունի իրական կյանքում, կիրառելի են նաև առցանց միջավայրում: Վերջին շրջանում եղե՞լ են դեպքեր, երբ կառավարությունը արգելափակել է ինտերնետը կամ սոցիալական ցանցերը, և ի՞նչ կարելի է անել նման դեպքերում: Որո՞նք են ցանցն ու հոսքերը վերահսկելու իրավական հիմնավորումները: Սրանք էին այն հարցերը, որոնք հիմք դարձան քննարկումների համար:

2008 թ. մարտին Հայաստանի «Ինտերնետ հանրությունը» սառեցրեց մի քանի ընդդիմադիր թերթերի դոմեյնները հանրության լայն զանգվածների կարծիքով տեղի ունեցած ընտրակեղծիքների դեմ մի շարք ցույցերից հետո: Երկրում հայտարարված արտակարգ իրավիճակի պայմաններում ՋԼՄ-ները կարող էին հրապարակել միայն պետական մարմիններից ստացված պաշտոնական տեղեկատվություն: Արգելափակվեցին մի շարք ընդդիմադիր ՋԼՄ-ներ, այդ թվում՝ A1+-ը և «Հայկական ժամանակ»-ը: Դադարեցվեց «Ազատություն» ռադիոկայանի հայաստանյան ծառայության աշխատանքը, Հայաստանի իշխանությունների կողմից արգելափակվեց նույնիսկ ծառայության կայքը: YouTube կայքը մեկ շաբաթ շարունակ արգելափակված էր՝ դեպքի վայրում ներկա անձանց տեսանյութերի տարածումը թույլ չտալու համար: Դրանից հետո բոլոր համապետական ընտրությունները ուղեկցվել են կայքերի արգելափակման ինչ-ինչ դեպքերով: Սակայն միշտ չէ, որ պարզ է՝ արդյոք մենք գործ ունենք այսպես կոչված DDoS հարձակման հետ, թե դրանք դոմեյն հոսթինգի ինչ-որ տեխնիկական սահմանափակումներ են կամ կայքերը չեն դիմանում մեծ թրաֆիքի, երբ ընտրակեղծիքներին առնչվող բովանդակությունը չափազանց մեծ տարածում է ստանում: Ամենաթարմ օրինակներից է www.sut.am–ը՝ «Իրազեկ քաղաքացիների միավորում» ՀԿ-ի հիմնած անկախ լրատվամիջոցի կայքը, որը ապացույցներ էր հավաքել, բացահայտել և հրապարակել էր 2017 թ. խորհրդարանական ընտրություններից առաջ դպրոցներում և մանկապարտեզներում վարչական ռեսուրսի չարաշահման լայն տարածում գտած դեպքերի մասին:

Լրատվական համայնքի ներկայացուցիչների և ակտիվիստների սոցիալական մեդիա հաշիվները նույնպես ընտրությունների ընթացքում գտնվել են նշանակետում: Վերջին շրջանի դեպքերից էր Հայաստանում հայտնի լրագրողների թվիթերյան հաշիվների մի քանի ժամով սառեցումը 2017 թ. խորհրդարանական ընտրություններից մեկ օր առաջ:

Ավելի վաղ՝ 2016 թ.-ին, Լեռնային Ղարաբաղի հակամարտության գոտում ռազմական գործողությունների վերսկսման ընթացքում Հայաստանի իշխանությունների կողմից գրաքննություն կիրառվեց ՋԼՄ-ների աշխատանքի նկատմամբ: Սահմանամերձ գոտում աշխատող լրագրողները հայտնեցին ինտերնետի սահմանափակ մատչելիության մասին, ինչն ամենայն հավանականությամբ ազգային անվտանգության նկատառումներով էր: Ազգային անվտանգության և հասարակական կարգի պաշտպանության օրինական նպատակին հասնելու համար ժամանակավորապես անհասանելի էր նաև Ֆեյսբուք սոցիալական կայքը, երբ 2016 թ. զինված խմբավորումը գրավել էր ոստիկանության պարեկապահակային ծառայության գնդի տարածքը՝ վերցնելով պատանդներ:

2015 թ. հունիսին մայրաքաղաքում տեղի ունեցող «Էլեկտրիկ Երևան» անունը կրող ցույցերի ուղիղ հեռարձակման ժամանակ ոստիկանությունը թիրախավորեց լրագրողներին և քաղաքացիական ակտիվիստներին՝ առգրավելով նրանց տեսագրման սարքերը: Բաղրամյան պողոտայում ցույցերը լուսաբանող լրագրողները հայտնեցին, որ տեղի են ունեցել ինտերնետ կապի համատարած ընդհատումներ, թեև պետք է ընդունել, որ դա կարող էր տեղի ունենալ մեկ ֆիզիկական տարածքում ինտերնետին միացած օգտվողների մեծ թվի պատճառով: 2015 թ. YouTube-ից հեռացվեց Երևանում տեղի ունեցող ցույցերի վերաբերյալ ոստիկանության պատասխանի ծաղրանմանակումը: Ոստիկանության խոսքերով «Նյութը հեռացվել է հեղինակային իրավունքի խախտման պատճառով, քանի որ այն պարունակում էր լրատվական ռեպորտաժից վերցված, հեղինակային իրավունքով պատկանող տեսանյութ»: Սակայն հավանական է, որ նյութը թիրախավորվեց, որովհետև ծաղրում էր ոստիկանության վարքագիծը: Այս դեպքից հետո

Հայաստանի ոստիկանությունը նյութի հեղինակի՝ SOS հեռուստաընկերության դեմ հայցադիմում ներկայացրեց դատարան՝ նշելով, որ նյութում ոստիկանության նկատմամբ վիրավորական արտահայտություններ կան:

Այս դեպքերն իրենց արտացոլումը գտան «Ֆրիդոմ Հաուս»-ի՝ ԱՄՆ-ում գործող և խոսքի ազատության իրավիճակին հետևող կազմակերպության զեկույցում, որտեղ նշվեց, որ վերջին մի քանի տարիներին Հայաստանում ինտերնետի ազատությունը մի փոքր անկում է ապրել: Կազմակերպության կողմից նշվեց, որ առհասարակ առցանց բովանդակությունը մատչելի է Հայաստանում ինտերնետից օգտվողների համար: Սակայն հանրային ընդվզումների և Լեռնային Ղարաբաղի հակամարտության սրման ժամանակահատվածում կառավարությունը սահմանափակել է մուտքը սոցիալական ցանցեր և այլ կայքեր՝ թիրախավորելով լրագրողներին, բլոգերներին և քաղաքացիական ակտիվիստներին, ինչը հստակ միջամտություն է արտահայտվելու ազատությանը:

Մարդու իրավունքների մասին օրենքներում հիմնական կանոնն այն է, որ խոսքի ազատության որևէ սահմանափակում կամ անձնական տվյալների գաղտնիության որևէ խախտում պետք է սահմանված լինի օրենքով, անհրաժեշտ և համաչափ լինի և ուղղված լինի կոնկրետ նպատակի՝ հիմնականում այլոց իրավունքների և համբավի պաշտպանությանը, ազգային անվտանգությանը և հասարակական կարգի պաշտպանությանը: Երբ պետությունն արգելափակում է կայքը կամ անջատում է ինտերնետը, բազմաթիվ հարցեր են ծագում: Ֆոկուս խմբին և հարցազրույցին մասնակցողներից շատերը համաձայնեցին, որ պետության համար միայն կայքերի արգելափակումը թույլատրող օրենքներ ունենալը բավական չէ, էլ չխոսենք շարժական կապի օպերատորների հետ չգրված պայմանավորվածությունների մասին: Հաճախ, երբ պետությունը միջամտում է ինտերնետային թրաֆիքին և արգելափակում է որոշակի կայքեր, չի հիմնավորում, թե ինչով է դա անհրաժեշտ օրինական նպատակներին հասնելու համար, ինչպիսին ազգային անվտանգությունն է, և արդյոք այլընտրանքային ճանապարհներ չկան ազգային անվտանգության և հասարակական կարգի պահպանման սպառնալիքների դեմ պայքարելու համար:

Ֆոկուս խմբին և հարցազրույցին մասնակցողներից շատերը համաձայնեցին, որ այն իրավունքները, որոնք անհատն ունի իրական կյանքում, պետք է հավասարապես պաշտպանվեն նաև առցանց միջավայրում: Ինտերնետը հսկայական տարածք և հնարավորություններ է ընձեռում խոսքի ազատության և այլ հիմնարար իրավունքների իրացման համար: Սակայն այն նաև պարարտ հող է առցանց հալածանքների և անանուն սպառնալիքների և հարձակումների համար: Լրագրողներն ու քաղհասարակության ներկայացուցիչները սեփական փորձից բազմաթիվ պատմություններ ներկայացրին՝ նշելով, որ առցանց հետապնդումների ամեն մի զոհ ստիպված էր ինքնուրույն զբաղվել կոնկրետ դեպքով՝ չունենալով մասնագիտական համայնքների ո՛չ աջակցությունը, ո՛չ էլ մասնակցությունը: Հաշվի առնելով պետության, իրավապահ մարմինների նկատմամբ վստահության բացակայությունը՝ նրանք նույնիսկ չեն էլ փորձել պաշտպանություն ստանալ իրավական ճանապարհով:

Օրինական նպատակների (ինչպիսիք են ազգային անվտանգությունը, այլոց բարի համբավի պաշտպանությունը) և ազատ ինտերնետի միջև սահմանը շատ նուրբ է: Որքանո՞վ է պետությունը իրավասու միջամտելու ցանցին և կառավարելու տեղեկատվական թրաֆիքը. սա է ոլորտի քաղաքականությանն առնչվող ամենաէական հարցը: Արդյո՞ք պետությունն իրավասու է պայքարելու

միայն երկրի տարածքում կատարված կիբերհանցագործությունների դեմ, թե՞ կան այս հարցում կիրառելի այլ սկզբունքներ: Ահա այն հարցերը, որոնք լրագրողների և քաղհասարակության ներկայացուցիչների շրջանում ակտիվ քննարկման առարկա դարձան ֆոկուս խմբի հանդիպման ժամանակ՝ չհանգելով վերջնական եզրակացության: Հարցազրույցին մասնակցած SS համայնքի ներկայացուցիչները այս հարցի շուրջ հիմնականում համակարծիք են: Նրանք կարծում են, որ ինտերնետը կարգավորող օրենքների կամ քաղաքականության բացակայությունը ինտերնետի կառավարումը դարձնում են ավելի ազատական, քան կարելի է ակնկալել: Որքան էլ որ դա պարադոքսալ է, Հայաստանը չի գնում այն ուղով, որը վերջերս որդեգրել է Ռուսաստանը իր երկրի տարածքում ինտերնետի թրաֆիքը կառավարելու համար: Հայաստանում որոշումներ կայացնողներն ու SS համայնքը առավել հակված են դեպի ինտերնետի կառավարման արևմտյան մոտեցումը, որը ձևավորվել է ցանցի բազմաշերտ առանձնահատկությունների և պատմական զարգացման հիման վրա:

Ցանցի բարդ, բազմաշերտ բնույթ ասելով հասկանում ենք, որ չկա ինտերնետի բոլոր ասպեկտների մեկ վերահսկող: Ինտերնետի զարգացումը՝ որպես համակարգչային ցանցերի հավաքածու, որն օգտագործում է ծրագրերի ընդհանուր արձանագրություններ, և որն աշխատեցնում են մասնավոր ընկերությունները, հանգեցրել է տարբեր շահագրգիռ կողմերից բաղկացած կառավարման մոդելի, որը ենթադրում է կառավարությունների, մասնավոր հատվածի, քաղհասարակության, ինչպես նաև վերջնական օգտագործողի մասնակցությունը[1]: Այս մոդելը ինտերնետը տարանջատում է հաղորդակցության նախկին բոլոր ուղիներից և տեխնոլոգիաներից, ինչպիսիք են՝ հեռագիրն ու հեռախոսը, որոնք ամբողջ աշխարհում ղեկավարվում էին կառավարությունների կողմից՝ կերտելով նոր իրականություն և ինտերնետի զարգացման նոր հարցեր և սկզբունքներ: Վերջին տարիների ընթացքում ցանցի չեզոքության մասին քննարկումները և կարգավորումները բյուրեղացրել են հետևյալ հիմնական սկզբունքները[2]՝:

- **Թափանցիկություն**. Օպերատորները պետք է իրենց բաժանորդներին համակողմանի և ճշգրիտ տեղեկատվություն տրամադրեն ցանցի կառավարման և ծառայությունների որակի մասին:
- **Խտրականության բացակայություն**. Օպերատորները պետք է զերծ մնան թրաֆիքի նկատմամբ խտրականությունից՝ անկախ ուղարկողից, ստացողից և բովանդակության տեսակից, ինչպես նաև հավելվածի և/կամ ծառայության տեսակից:
- **Մատչելիություն**. Օգտագործողները պետք է անխոչընդոտ մուտք ունենան դեպի ՕՐԻՆԱԿԱՆ բովանդակություն, ծառայություններ կամ հավելվածներ (երաշխավորելով ծառայության նվազագույն որակի ապահովում բարեխիղճ օգտագործման համար) կամ միանալ որևէ սարքի, որը ցանցը չի վնասում:

Ելնելով հարցազրույցներից և ֆոկուս խմբերի հետ քննարկումներից՝ պարզ է դառնում, որ ցավոք Հայաստանում շարժական կապի և հեռահաղորդակցության հիմնական ընկերությունները այդքան էլ շատ հնարավորություններ չունեն վերոհիշյալ սկզբունքներին հետևելու և կառավարության կողմից սահմանափակումները զսպելու համար: Եթե կառավարությունը պահանջի արգելափակել ինտերնետը կամ լիարժեք մուտք ապահովել վերահսկման նպատակով, այդ ընկերությունների համար դժվար կլինի մերժելը: Պետք է ընկերություններին խրախուսել, որպեսզի պաշտպանեն իրենց հաճախորդների շահերը և

[1]«Մեդիա զարգացումը թվային դարաշրջանում. ինտերնետի կառավարման հինգ ուղի» Կորին Քեթ, Նիլս Թեն Էվեր, Դանիել Օ'Մարլի, 2017

[2] Ինտերնետի կառավարման ուղեցույց (6-րդ հրատ.), Յովան Քուրբալայջա, DiploFoundation, Ժնև, Շվեյցարիա 2014

հնարավորության դեպքում մերժեն նման պահանջները և պահանջեն դատարանի որոշում: Ընկերությունները վստահաբար ինտերնետի անջատումների ժամանակ կորցնում են իրենց եկամտի մի մասը, ուստի պետք է կատարեն շահութաբերության վերլուծություն և փորձեն հասկանալ՝ ինչ տնտեսական լծակներ ունեն նման սահնափակումները հետ մղելու համար: Գաղտնիք չէ, որ նրանք այդքան էլ ճկուն չեն կարող լինել կառավարության պահաջներին արձագանքելու հարցում, ուստի օգտագործողների իրավունքների պաշտպանության մեխանիզմները պետք է նաև այլ տեղ փնտրել: Այն մարդիկ, ովքեր զբաղվում են ազատ ինտերնետի առաջխաղացմամբ և անձնական տվյալների պաշտպանությամբ, լրագրողներն ու ակտիվիստները պետք է հետևողականորեն պահանջեն այնպիսի օրենքների և փորձի ձևավորում, որը պաշտպանում է թվային միջավայրը, ինչպես նաև պահանջեն, որ կառավարությունները կատարեն իրենց պարտականությունները թվային ոլորտում այնպես, ինչպես ոչ թվային միջավայրում:

Այն համոզվածությունը, որով ֆոկուս խմբի անդամները խոսում էին իրենց և իրենց գործընկերների նկատմամբ իրականացվող շարունակական վերահսկման և գաղտնալսման մասին, ցույց է տալիս, թե որքան տարածված են այդ դեպքերը, նաև փաստում են պետական մարմինների (Անվտանգության ազգային ծառայության) անսահմանափակ հնարավորությունները այդ վերահսկումն իրականացնելու հարցում, անգամ առանց շարժական կապի օպերատորներին նախապես տեղյակ պահելու: Այս դեպքերի մասին ստուգված փաստեր չկան, այնուամենայնիվ, հատկապես քաղաքացիական ակտիվիստները կարծում են, որ քանի որ իրենք զբաղվում են կոնկրետ նպատակների առաջխաղացմամբ և իրենց տարածած զգայուն բովանդակությամբ և գաղափարախոսությամբ քննադատում են կառավարությանն ու նրանց մոտ կանգնած բիզնեսներին, նրանց հեռախոսազրույցներին ու հաղորդակցությանը միշտ էլ հետևել և գրաքննել են, իսկ նրանց բլոգներն ու կայքերը հաճախ ենթարկվել են հարձակումների և արգելափակման: Ի լրումն կայքերին ուղղված DDoS հարձակումներին՝ սոցիալական ցանցերում նրանց հաշիվները նույնպես թիրախավորվում են կեղծ այցելուների կողմից, ինչը համարյա անհնար է դարձնում պարզելը, թե ով է կանգած հարձակումների հետևում:

3.5. Ի՞նչն է լրագրողին կամ շահերի պաշտպանությամբ զբաղվողներին դարձնում կիբերհարձակումների թիրախ և ո՞վ է պատասխանատու նրանց ստեղծած բովանդակության, անձնական տվյալների և ցանցերի պաշտպանության համար:

Մեդիա մասնագետներից և քաղաքացիական հասարակության ներկայացուցիչներից բաղկացած թիրախ լսարանին ուղղված մեր հարցերին անդրադառնալու համար մենք քննարկում նախաձեռնեցինք այն մասին, թե ինչու են նրանք կարծում, որ իրենց ստեղծած բովանդակությունը այնքան հրապուրիչ է (կամ հրապուրիչ չէ որևէ մեկի համար), որ դրա պատճառով կարող են կոտրել կազմակերպության տեղեկատվական համակարգը: Ինչու՞ պետք է որևէ մեկը փորձի կոտրել նրանց հաշիվներն ու կորզի այն բովանդակությունը, որը նրանք են ստեղծում: Հետազոտական խումբը կարծիքներ էր փնտրում՝ որն է պատճառը, որ նրանք դադարում են լինել ինտերնետի սովորական օգտատեր և դառնում են ցանց ներխուժումների կամ վերահսկման հավանական թիրախ: Հարցազրույցին մասնակցած լրագրողներին ու քաղհասարակության ներկայացուցիչներին, ինչպես նաև ֆոկուս խմբերի մասնակիցներին խնդրել էինք մանրամասներ տրամադրել ինտերնետում իրենց հաշիվներին և թվային ինքնությանն ուղղված ռիսկերի և դրանց պատճառների մասին և կիսվել իրենց փորձով, թե որտեղից են գալիս այդ ռիսկերը:

Թե' SS անվտանգության գծով փորձագետների, և թե' ԶԼՄ-ների և ՀԿ-ների ներկայացուցիչների կարծիքով՝ այն ակնհայտ ռիսկը, որը ինտերնետի սովորական օգտատերին դարձնում է ներխուժման հնարավոր թիրախ, նրանց ունեցած կապերի թիվն է/լսարանի չափը: Լրագրողներն ու ակտիվիստները սովորաբար սոցիալական կայքերում ունեն հետևողների մեծ թիվ, ինչը նրանց օգնում է տվյալներ հավաքելու, բովանդակություն տարածելու, հանրային իրազեկումն ու շահերի պաշտպանությունն ավելի արդյունավետ

կազմակերպելու և իրենց նպատակների համար ավելի շատ աղբյուրներ մոբիլիզացնելու հարցում: Մյուս կողմից՝ մեծ լսարանը նրանց խոցելի է դարձնում ամեն տեսակի կիբերհանցագործությունների համար: Զարմանալին այն է, որ հարցազրույցներին մասնակցած լրագրողների և քաղհասարակության ներկայացուցիչներից շատերը լիովին գիտակցում են, որ իրենց մեծ լսարանն ու հանրաճանաչ լինելը կարող են նրանց շարունակական վերահսկման և կիբերհարձակումների թիրախ դարձնել, ասենք, Ազգային անվտանգության ծառայության կողմից, բայց չեն կարծում, որ այս ռիսկերը գալիս են տվյալներ հափշտակողներից, անձնական տվյալներ կորզող կեղծ նամակների զոհը դառնալուց կամ անձնական տվյալների գաղտնիության խախտումներից, որոնք հաճախ կապված են մեծ կորպորացիաների կողմից տեղեկատվության արտահոսքի դեպքերի հետ:

Կարծիքներն այն մասին՝ արդյոք թիրախ խմբին պատկանող մեդիա մասնագետներն ու քաղհասարակության ներկայացուցիչները տնօրինում են թե՛ կոմերցիոն և թե՛ իրավական կարևորություն ներկայացնող արժեքավոր տեղեկատվություն և բովանդակություն, չափազանց տարբեր էին: Որոշ SS անվտանգության փորձագետներ գտնում են, որ Հայաստանում գործող լրագրողները և քաղաքացիական հասարակության ներկայացուցիչները այնքան էլ շատ բան չունեն կորցնելու և որ այն բովանդակությունը, որի վրա նրանք աշխատում են կամ որը ստեղծում են չունի այն կոմերցիոն կամ այլ արժեքը, որը կարժենար նրանց տեղեկատվական համակարգերը ջարդելուն ուղղված ջանքերն ու ծախսերը: Հիմնական տրամաբանությունն այստեղ այն է, որ եթե Հայաստանում իշխանությունները ցանկանան թիրախավորել կամ լռեցնել որևէ մեկին, նրանք, երևի թե, կարող են օգտագործել ոչ այնքան ծախսատար մեթոդներ: Իրենց հերթին որոշ լրագրողներ և քաղաքացիական ակտիվիստներ կարծում են, որ իրենք թաքցնելու բան չունեն՝ այդ թվում իրենց աղբյուրների/շահագրգիռ կողմերի հետ հաղորդակցությունը, և որ անվտանգության լրացուցիչ միջոցները ավելի շատ կհրավիրեն պետական մարմինների անցանկալի ուշադրությունը, քան կօգնեն պաշտպանել իրենց և տեղեկատվության աղբյուրները:

Հարցազրույցին մասնակցած SS անվտանգության փորձագետների և մեդիա մասնագետների/ քաղհասարակության ներկայացուցիչների թվում կային նաև այնպիսիք, ովքեր բավականաչափ կարևորություն են տալիս վերջինների ստեղծած բովանդակությանը և թե ինչպես են նրանք կառավարում իրենց մոտ եղած տվյալները: Շահերի պաշտպանությամբ զբաղվող անձինք, ովքեր առնչվում են զգայուն հարցերի հետ, և լրագրողները, ովքեր աշխատում են կոնֆիդենցիալ և շտապ հրապարակվելիք նյութերի վրա, միշտ էլ առնչվել են թվային անվտանգության և մասնավոր կյանքին վերաբերող սպառնալիքներին: Նրանք վստահ են, որ այն ծրագրերը, որոնցում ներգրավված են, նրանց դարձնում են հաքերների հնարավոր թիրախ: Ոմանք նույնիսկ նշեցին, որ իրենց ունեցած գաղափարախոսությամբ կամ արժեհամակարգով տարբերվում են մյուսներից՝ դրանով իսկ լրացուցիչ բացասական ուշադրություն գրավելով դեպի իրենց սոցիալական ցանցերի և այլ հաշիվներն ու շարժական կապի սարքավորումները: Սա հատկապես վերաբերում է հետաքննող լրագրողներին և քաղաքացիական ակտիվիստներին, քանի որ նրանք ստեղծում և տարածում են այնպիսի բովանդակություն, որով քննադատում են պետական և կառավարական մարմիններին և ընկերություններին: Ելնելով ֆոկուս խմբի քննարկումներից՝ բնապահպանական հարցեր հետաքննող և/կամ խաղաղասիրական օրակարգ առաջ մղող լրագրողներն ու քաղհասարակության խմբերը, որոնք ակտիվ հետևում են բանակին առնչվող զարգացումներին և Լեռնային Ղարաբաղի հակամարտության շուրջ ռազմական գործողություններին, շատ հաճախ իշխանությունների կողմից ստանում են սպառնալիքներ, ենթարկվում են հարձակումների և ավելի լավ են գիտակցում տեղեկատվության անվտանգության ու իրենց թվային ինքնության պաշտպանության արժեքը:

Անդրադառնալով այն անհատների և խմբերի ցանկին, որոնք կարող են հատուկ հետաքրքրություն ունենալ իրենց անձնական տվյալների և իրենց կազմակերպությունների համակարգ ներխուժելու նկատմամբ, հարցազրույցին մասնակցած/ֆոկուս խմբի անդամ լրագրողներն ու ակտիվիստները լիովին կիսում էին այն

կարծիքը, որ առաջին տեղում են պետական մարմիններն ու մասնավորապես Ազգային անվտանգության ծառայությունը: Վստահությունը, թե վերջին շրջանում իրենց անձնական էլեկտրոնային հաշիվների և կայքերի վրա կատարված կիբերհարձակումների հետևում կանգած են պետական մարմինների ներկայացուցիչները, ձևավորվել է այն բանի շնորհիվ, որ լրագրողները ու հատկապես քաղաքացիական ակտիվիստները նրանցից ֆիզիկական սպառնալիքներ են ստանում հենց այն ժամանակ, երբ հարձակման են ենթարկվում նրանց հաշիվներն ու կայքի բովանդակությունը: Երկրորդ, և որ զարմանալի է, վարձու հաքերների կողմից անձնական տվյալներ հափշտակելու մասին իրական պատմություններ ներկայացնելով՝ նրանք նշեցին իրենց անձնական թշնամիների և մրցակիցների կողմից կիբերհարձակումների ռիսկի մասին: Թվային անվտանգության դեմ սպառնալիքների մեկ այլ աղբյուրը, որը շատերի կողմից նշվեց և որին հատկապես Հայաստանի լրատվամիջոցներն են հանդիպում, ադրբեջանական հաքերների խմբերն են, որոնք կոտրում են «. am» դոմեյնի կայքերը և հայ օգտատերերի էջերը: Հարցազրույցին մասնակցած միայն մի քանի լրագրող և քաղհասարակության ներկայացուցիչ նշեցին թվային տիրույթում գլոբալ սպառնալիքների մասին՝ անդրադառնալով անձնական տվյալները կորզելու նպատակով ստացվող և այլ կասկածելի էլեկտրոնային նամակներին:

Չնայած համացանում մեծ քանակությամբ տեղեկատվության և խորհրդատվական նյութերի առկայությանը, ինչպես նաև կիբերանվտանգության թեմաներով հաճախակի կազմակերպված դասընթացներին՝ հարցազրույցին մասնակցած մեդիա մասնագետները և քաղհասարակության ներկայացուցիչները նշեցին, որ քիչ գիտելիք և հմտություններ ունեն ինտերնետում ի հայտ եկող անվտանգության սպառնալիքներին դիմակայելու համար: Ինչ վերաբերում է SS անվտանգության հետ կապված հարցերին կամ խնդիրներին, որոնց նրանք հանդիպում են, առավել հաջողակները դիմում են տեխնիկական հարցերի գիտակ իրենց ընկերներին կամ պրոֆեսիոնալ SS մասնագետներին՝ սովորաբար LAN ադմինիստրատորներին, որոնք աշխատում են իրենց կազմակերպություններում: Թիրախ խմբի լրագրողների և ակտիվիստների հիմնական խնդիր են մնում թվային անվտանգության մասին անբավարար գիտելիքները, ինչպես նաև ինքնակրթությամբ զբաղվելու ժամանակի և հետաքրքրության պակասը: Մյուս կողմից, կան միայն մի քանի ՋԼՄ-ներ և ՀԿ-ներ, որոնք մշակել են կորպորատիվ քաղաքականություն կամ կանոններ՝ ապահովելու իրենց սարքավորումների, ցանցերի և կայքերի անվտանգությունը: Երբ կազմակերպություններն ունեն տվյալների անվտանգության խիստ կանոններ և ընթացակարգեր, աշխատակիցները չեն էլ փորձում խախտել ընդունված կանոններն ու կարգը: Սա, թերևս, ամենից արդյունավետ միջոցն է հասնելու տեղեկատվության անվտանգ փոխանակմանը լրագրողների, քաղհասարակության ներկայացուցիչների և նրանց աղբյուրների/շահագրգիռ կողմերի հետ՝ ելնելով այն տեղեկատվությունից, որ մենք ստացանք ֆոկուս խմբերի քննարկումների և խորքային հարցազրույցների արդյունքում: Անհատ լրագրողների և ակտիվիստների կիբերանվտանգության իրազեկության և անվտանգության կանոնների պահպանման սովորույթին ապավինելը երբեք արդյունավետ չի լինի տվյալների կորպորատիվ պաշտպանությանը հասնելու և կազմակերպության ցանցերի միջոցով տեղեկատվության անվանգությունն ապահովելու համար, քանի որ նախ կա մասնագիտական միջամտության կարիք՝ հաշվի առնելով կիբերանվտանգության համաշխարհային սպառնալիքները: Ցավոք, Հայաստանում ոչ բոլոր ՋԼՄ-ներն ու ՀԿ-ները կուզենան և կկարողանան իրենց թույլ տալ տեղեկատվական անվտանգությունը կազմակերպել ու դրանից բխող ծախսերը սահմանել որպես առաջնահերթություն և նախընտրում են կենտրոնանալ իրենց հիմնական առաքելության վրա՝ լրատվությանն ու շահերի պաշտպանությանը՝ կիբերռիսկերին ենթարկվելու գնով:

Եվ վերջապես, հարցազրույցին մասնակցած լրագրողների և ՀԿ-ների ներկայացուցիչների մեծ մասը ցանկություն չունի իր հիմնական պարտականությունների կատարման և առօրյա միջոցառումների հաշվին շարունակաբար ժամանակ և ջանքեր տրամադրել գիտելիք և հմտություններ ձեռք բերելուն: Նրանց նշած պատճառները շեշտակիորեն տարբերվում էին միմյանցից: Ոմանք մտածում են, որ իրենց անհատական ջանքերը ծովում կաթիլի նման կլինեն, քանի որ ո՛չ իրենց գործընկերները, ո՛չ էլ նրանց հետ կապի մեջ

գտնվող կողմերը չեն հետևում SS անվտանգության չափանիշներին և ընթացակարգերին: Մյուսները պնդում են, որ ինչ ջանքեր էլ ներդնեն իրենց անձնական տվյալները պաշտպանելու ուղղությամբ, չեն կարող լիարժեք պաշտպանվել կիբերհարձակումներից կամ անձնական տվյալների արտահոսքից: Ֆոկուս խմբի անդամներից շատերը սխալմամբ կարծում էին, որ հենց միայն անձնական տվյալների գաղտնիության քաղաքականության և կարգավորումների առկայությունը ցույց է տալիս, որ իրենց օգտագործած սոցիալական կայքերը կամ վեբկայքերը առանց իրենց համաձայնության չեն տարածի իրենց անձնական տեղեկատվությունը: Այս ցանկը սպառիչ չէ, և չկա գիտելիքի հատուկ տեսակ կամ քանակ, որը ստանալով կարելի է լիովին պաշտպանվել առցանց միջավայրում բոլոր սպառնալիքներից և ռիսկերից, որոնց ինտերնետի օգտագործողները դեռևս հանդիպելու են: Ինչպես հաստատեցին հարցազրույցին մասնակցած SS անվտանգության փորձագետներից շատերը, այսօր հիմնական խնդիրը լրագրողներին, ակտիվիստներին և բոլոր շարքային օգտատերերին կիբերանվտանգության առկա և նոր ի հայտ եկող սպառնալիքների նկատմամբ զգոն պահելն է և այնպիսի փորձի և սովորությունների ձևավորում խրախուսելը, որոնք կհանգեցնեն առցանց միջավայրում տեղեկատվության առավել անվտանգ փոխանակմանը: Ամփոփելով ծրագրի թիրախ խմբի անդամների նշած փորձն ու ընդհանուր խնդիրները, ՋԼՄ-ներն ու քաղհասարակության կազմակերպությունները պետք է հատուկ ուշադրության դարձնեն հետևյալ, բայց ոչ միայն այս ոլորտներին.

- Ինչպես կարելի է հնարավորինս անվտանգ օգտագործել անձնական համակարգիչը, բջջային հեռախոսները և այլ սարքավորումներ:
- Ինչպես պաշտպանել սարքավորումներն ու զգայուն տեղեկատվությունը ֆիզիկական սպառնալիքներից:
- Ինչպես ստեղծել անվտանգ գաղտնաբառեր և պաշտպանել էլեկտրոնային հաշիվները:
- Ինչպես օգտագործել գաղտնագրումն ու հաղորդակցության անվտանգ աղբյուրները:
- Ինչպես օգտագործել սոցիալական ցանցերն ու այնտեղ պահվող անհատական տվյալները:
- Ինչպես համակարգիչն ու այլ սարքավորումները պաշտպանել վիրուսներից և կեղծ ծրագրերից, և ինչպես ճշգրտել աղբյուրներն ու անծանոթ URL-ները:
- Ինչպես արխիվացնել և պահեստավորել կարևոր տեղեկատվությունը, և ինչպես վերականգնել կորցրած տեղեկատվությունը:
- Ինչպես վերացնել զգայուն տեղեկատվությունը Ձեր սարքավորումների կորստի, գողանալու կամ առգրավման դեպքում:
- Ինչպես խուսափել սոցիալական ինժեներների և անձնական տվյալներ կորզող հաղորդագրությունների զոհը դառնալուց:
- Ինչպես տեղեկատվություն ստանալ օգտատերերի իրավունքների և կիբերանվտանգության ոլորտում գործող օրենսդրության մասին:
- Ինչպես ապահովել և կիրառել կիբերանվտանգության արդյունավետ քաղաքականություն և փորձ:
- Ինչպես ապահովել կազմակերպության կայքի և ցանցի անվտանգությունը:

3.6. Առցանց մուլտիմեդիա գործիքակազմի մշակումը ծրագրի շրջանակներում

«Մարդու իրավունքները ինտերնետում. կրթություն և պաշտպանություն» ծրագրի շրջանակներում կատարված հետազոտության արդյունքներն այս զեկույցում ամփոփելուց բացի, ծրագրի թիմը նաև նախաձեռնել է առցանց մուլտիմեդիա գործիքակազմ՝ կիբերանվտանգության առկա և նոր ի հայտ եկող սպառնալիքների մասին իրազեկությունը բարձրացնելու և դրանց դեմ պայքարելու համար անհրաժեշտ լուծումներ, ռազմավարություն, գիտելիք և հմտություններ տրամադրելու նպատակով: Օնլայն մուլտիմեդիա գործիքակազմը նախատեսված է ծրագրի թիրախ խմբերի համար՝ լրագրողների և քաղաքացիական հասարակության ներկայացուցիչների, բայց որպես գործիքակազմ՝ հուսով ենք կծառայի

նաև ինտերնետի այլ օգտատերերին: Ֆոկուս խմբերի քննարկումների և հարցազրույցների ընթացքում լրագրողներին ու քաղաքացիական ակտիվիստներին խնդրել էինք մանրամասնել իրենց նախընտրությունները խաղի բովանդակության, ծավալի, գաղափարի և ձևաչափի մասին: Նախորդ գլխի ամփոփման մեջ նշված թեմաների ցանկը այն թեմաների և հարցերի ամփոփումն է, որոնցով թիրախ մասնագետներն ու հարցազրույցին մասնակցած SS փորձագետները ամենից շատ էին մտահոգված: Խաղի գաղափարի մշակումը, ելնելով կիբերանվտանգության վերոհիշյալ ոլորտներից, չափազանց ողջունելի էր: Ի լրումն նշվածի, ֆոկուս խմբի մասնակիցներն առաջարկեցին նաև հատուկ ուշադրություն դարձնել այնպիսի հարցերին, ինչպիսիք են՝ 1) երեխաների իրավունքներն ու երեխաների անձնական տվյալների հրապարակումը ինտերնետում, 2) մոռացված լինելու իրավունքը և 3) առցանց հալածանք:

Խաղի հնարավոր կառուցվածքը ֆոկուս խմբի անդամների շրջանում լայն քննարկումների առիթ դարձավ: Նրանցից շատերն առաջարկեցին, որ այն կիբերանվտանգության մասին տեղեկատվություն և խորհուրդներ տրամադրող՝ վիկտորինա հիշեցնող խաղ լինի՝ նշելով նաև, որ հարցուպատասխանի ձևաչափը նույնպես գրավիչ է նրանց համար: Որպես առավել բարդ տարբերակ՝ առաջարկվեց մտացածին իրավիճակներով խաղի ձևաչափը՝ հնարավորություն ունենալով ընտրել և պատասխանել մի շարք իրավիճակային հարցերի՝ անդրադառնալով կիբերանվտանգության այս կամ այն սպառնալիքին: Սա նշանակում է նաև, որ յուրաքանչյուր հարց կունենա իր կշիռը ելնելով բարդության աստիճանից, և ամեն անգամ ճիշտ պատասխան տալով՝ խաղացողը կանցնի դեպի ավելի բարդ հարցերը: Խաղի բազմամակարդակ բնույթը կապահովի խաղացողների շարունակական հետաքրքրությունը և կխթանի առաջ շարժվելու ցանկությունը:

Խաղի տևողության հետ կապված ընդհանուր համաձայնություն չեղավ: Որոշ մասնակիցներ նշեցին, որ խաղին օրական կտրամադրեին 5-10 րոպե, մինչդեռ մյուսները պատրաստ են անցկացնել ավելի քան 1 ժամ՝ հատկապես եթե խաղը նախատեսված է նաև շարժական սարքերի համար: Խաղի տևողության հետ կապված ամենակարևոր նախընտրությունն այն էր, որ հնարավոր լինի խաղը շարունակել այն պահից, որտեղ խաղացողը կանգ է առել, եթե օգտագործում է միևնույն սարքը և/կամ հաշիվը:

ԵԶՐԱՀԱՆԳՈՒՄՆԵՐ ԵՎ ՀԻՄՆԱԿԱՆ ԱՌԱՋԱՐԿՈՒԹՅՈՒՆՆԵՐ

Թեև տեխնոլոգիաներն ու ինտերնետը շատ հզոր և օգտակար գործիքներ են տեղեկատվության ստեղծման և տարածման համար, դրանք նաև կիբերանվտանգության զգալի ռիսկերի են ենթարկում այնպիսի մասնագիտական խմբերի, ինչպիսիք են լրագրողներն ու քաղաքացիական հասարակության ներկայացուցիչները: Որքան շատ են լրագրողներն ու շահերի պաշտպանությամբ զբաղվողները օգտվում թվային տեխնոլոգիաներից, այնքան տեսանելի ու խոցելի են նրանք դառնում առցանց միջավայրում: Թեև ինտերնետն օգնել է նվազեցնել բազմաթիվ ծախսեր, կիբերտիրույթում կատարված մեկ հասարակ սխալը կարող է շատ թանկ արժենալ: Մեկ լրագրողի, բլոգերի կամ քաղաքացական ակտիվիստի անվտանգությունը վնասելը նշանակում է վտանգի տակ դնել բոլոր այն մարդկանց անվտանգությունը, ում հետ նա հաղորդակցվում է առցանց: Ինչպես ցույց տվեց մեր հետազոտությունը, մեդիա մասնագետներից և քաղաքացիական հասարակության ներկայացուցիչներից շատերը մեծ կարևորություն չեն տալիս առկա կիբերռիսկերին և շատ քիչ գիտելիք ունեն, թե ինչպես պաշտպանեն իրենց և իրենց սարքավորումները, աղբյուրները և համացացնում շահագրգիռ կողմերին: Նրանք իրազեկված չեն այն ռիսկերի և սպառնալիքների մասին, որոնք կապված են մեծ կորպորացիաների կողմից կիրառվող ալգորիթմների հետ՝ ամեն մի օգտագործողի մասին տվյալներ հավաքելու, ընդհանրացնելու և օգտագործելու նպատակով, եթե չխոսենք կառավարությունների կողմից գրաքննության և վերահսկման մասին: Google-ը և Facebook-ը մեզ անընդհատ ցուց են տալիս գովազդներ՝ հաշվի առնելով այն բովանդակությունը, որը մենք հավանել ենք

կամ տարածել: Դեռևս լավ չգիտակցելով կիբերանվտանգության սպառնալիքները՝ մենք շուտով ստիպված կլինենք որպես նորահայտ սպառնալիք գործ ունենալ «գրաքննության այնպիսի համակարգերի հետ, որոնք այնքան մանրակրկիտ են հարմարեցված օգտագործողների տեղեկատվական կարիքներին, որքան այն վարքագծային գովազդները, որոնց մենք ամեն օր հանդիպում ենք[3]»:

Մեդիա մասնագետների և քաղաքացիական հասարակության ներկայացուցիչների խնդիրները չեն կարող հեշտությամբ լուծվել, քանի որ խորը արմատներ ունեն նրանց՝ որպես օգտատերերի սովորություններում և մոտեցումներում, ինչպես նաև ինտերնետի ընդհանուր մշակույթում և կոնկրետ մասնագիտական պրակտիկայում: Այդուհանդերձ, SS անվտանգության փորձագետներից և թիրախ հանդիսացող մասնագիտական խմբերից, ինչպես նաև տվյալների եռանկյունացված վերլուծությունից ստացված տեղեկատվության հիման վրա հետազոտական թիմն առաձնացրել է մի քանի ոլորտ և ներկայացնում է հետևյալ առաջարկությունները լրագրողների, քաղաքացիական ակտիվիստների, ծրագրի շահագրգիռ կողմ հաստատությունների և քաղաքականություն մշակողների համար.

Շահագրգիռ հաստատություններին՝

- Հիմնել մի քանի շահագրգիռ հաստատություններից բաղկացած հիմնադրամ՝ երկրում ինտերնետին առնչվող զարգացումներին հետևելու, ինչպես նաև ինտերնետից օգտվողների իրավունքները պաշտպանելու համար՝ ապահովելով այն սկզբունքը, որ նրանց համարեն ոչ թե պարզապես օգտատերեր, այլ քաղաքացիներ, որոնց հիմնարար մարդու իրավունքները պետք է իրացվեն առցանց միջավայրում:
- Թիրախ մասնագետների և SS անվտանգության մասնագետների համայնքի համար՝ գտնել համագործակցության, վերապատրաստման և տեղեկատվության փոխանակման նոր հնարավորություններ՝ ինտերնետի անվտանգության խախտման և հնարավոր ռիսկերի դեմ արդյունավետ պայքարելու համար:
- Կորպորատիվ պատասխանատվության ստանձնել հաճախորդների կիբերանվտանգության համար: Ղեկավարների ու ընկերությունների սեփականատերերի համար՝ վերագնահատել կիբերանվտանգության ռիսկերն ու հնարավոր արժեքը և ապահովել, որ իրենց ցանցերում օգտագործվող ծրագրերը լիցենզավորված լինեն: Ավելի շատ օգտագործել բաց աղբյուրներով օպերացիոն համակարգեր:
- Զնավորել անվտանգության մասին իրազեկության մշակույթ և լրացնել աշխատակազմի՝ կիբերանտանգության մասին գիտելիքի և հմտությունների պակասը՝ ներդնելով կորպորատիվ քաղաքականություն և ընթացակարգեր՝ ապահովելու թիմի անդամների և գործընկերների/շահագրգիռ կողմերի միջև տեղեկատվության փոխանակման անվտանգությունը: Աշխատակիցներին ապահովել անհրաժեշտ ուսուցում և տեխնոլոգիներ՝ կազմակերպությունների մարդկային ռեսուրս-պաշտպանությունն ուժեղացնելու և կիբերհարձակումների հնարավորութ-յունը նվազեցնելու համար:
- Մշակել կազմակերպության տնօրինած զգայուն տեղեկատվության արխիվացման և պահպանման ռազմավարություններ: Մտածել տեղեկատվության կորստի դեպքում այն վերականգնելու հնարավոր միջոցների մասին: Սա հատկապես վերաբերում է այն ՋԼՄ-ներին և ՀԿ-ներին, որոնք ունեն տվյալների մեծ շտեմարաններ և մեծածավալ նյութեր:

Անհատներին՝

- Տեղեկացված լինել հանրային WiFi-ի օգտագործումից բխող ապառնալիքների մասին և WiFi-ից օգտվելիս օգտագործել առնվազն VPN:

[3] «Ցանցի անհիրականությունը. ինտերնետի ազատության մութ կողմերը», Եվգենի Մորոզով, Public Affairs, Նյու Յորք 2011

- Օգտագործել չկրկնվող և բարդ գաղտնաբառեր և հաշիվների երկաստիճան պաշտպանություն:
- Զգուշանալ անծանոթ կայքեր այցելելուց: Չափազանց զգույշ լինել էլեկտրոնային փոստին կցված փաստաթղթերը բացելիս՝ հատկապես, եթե դրանք ստացվել են անծանոթ աղբյուրներից:
- Հեռախոսներն ու այլ շարժական սարքավորումները առանց հսկողության չթողնել: Գաղտնաբառեր ունենալ այդ սարքավորումները մուտք գործելու համար և ռազմավարություններ մշակել սարքավորումներում զգայուն տեղեկատվության ոչնչացման համար այն դեպքերում, եթե այդ սարքավորումները գողանան, կորչեն կամ առգրավվեն:
- Սովորել՝ ինչպես զգայուն տեղեկատվությունն ու ինտերնետում հաղորդակցությունը գաղտնի պահել՝ տիրապետելով գաղտնագրման գործիքներին և տեխնիկային:
- Տեղեկացված լինել, թե ինչպես են աշխատում սոցիալական ցանցերը և չվստահել դրանց գաղտնիության կարգավորումներին և քաղաքականությանը:

Առաջարկությունների այս ցուցակը սպառիչ չէ և հարկավոր է շարունակաբար իրազեկ լինել կիբերանվտանգության առկա և նորահայտ սպառնալիքներին, ինչպես նաև փնտրել ամենաարդյունավետ ձևերն ու գործիքները այդ ռիսկերի դեմ պայքարելու համար:

V. Կից փաստաթղթեր

5.1. Խորքային հարցազրույցների և ֆոկուս խմբերով քննարկումների ուղեցույց

ՆԵՐԱԾՈՒԹՅՈՒՆ

1. Վարողի և ՖԽ կոորդինատորի անունները, և ով ինչ է անելու ՖԽ-ի հետ հանդիպման ժամանակ:
2. Քննարկման նպատակը.

   Ձեր կարծիքը և փորձը շատ կարևոր են մեզ համար, և մենք ցանկանում ենք, որ քննարկման ընթացքում լինեք ակտիվ և անկեղծ :

ԸՆԴՀԱՆՈՒՐ ԿԱՆՈՆՆԵՐ

1. Այս քննարկումը տևելու է մոտ 2 ժամ:
2. Քննարկումը տեսագրվելու է/ձայնագրվելու է, և մենք շնորհակալ ենք Ձեր գրավոր համաձայնության համար:
3. Մեր կողմից քննարկվելիք թեմայի վերաբերյալ սխալ պատասխաններ չկան: Մենք ակնկալում ենք լսել տարբեր տեսակետներ և համոզված ենք, որ ձեզանից յուրաքանչյուրը քննարկմանը լրացնող ասելիքներ ունի: Ուստի ցանկանում եմ խրախուսել, որպեսզի խոսեք, բայց պարտադիր չէ, որ պատասխանեք յուրաքանչյուր հարցին:
4. Խնդրում եմ խոսել մեկ առ մեկ, որքան հրավոր է հստակ, և խնդրում եմ խուսափեք առանձին զրույցներից: Դա շեղում է խմբի անդամների ուշադրությունը, և ես չէի ցանկանա ձեզանից որևէ մեկի դիտարկումները բաց թողնել:
5. Միմյանց հետ կարող եք կիսվել տեսակետներով. պարտադիր չէ, որ բոլոր պատասխաններն ինձ ուղղեք:
6. Նախքան սկսելը, հարցեր ունե՞ք:
7. Եվ վերջում, խնդրում եմ անջատել բջջային հեռախոսները:

Սկսել տեսա/ձայնագրությունը

I. Ընդհանուր տեղեկություններ (5-7 րոպե)

1. Խնդրում եմ հակիրճ ներկայացեք՝ նշելով.
2. Ո՞վ եք դուք,
3. Ի՞նչ մասնագիտական/այլ գործունեությամբ եք զբաղվում:
4. Կարո՞ղ եք նաև նշել՝ Ձեր առօրյա աշխատանքի/հաղորդակցության որքան մասն է իրականացվում ինտերնետի միջոցով և արդյո՞ք կարծում եք, որ դուք ինտերնետի վարժ օգտագործող եք:

II. Մարդու իրավունքներն առցանց և ցանցից դուրս. եթե սրանք ամբողջովին նույնը չեն, ապա որտե՞ղ են հատվում (15-20 minutes)

5. Ցանցի չեզոքության առավելություններն ու թերությունները. ո՞րն է Ձեր տեսանկյունը (փաստարկները) «ինտերնետի զարգացումն ընդդեմ հոսքերի կառավարման» մասին՝ վերջնական օգտագործողի տեսանկյունից:

6. Վերջին տարիներին քաղաքականության մասին քննարկումներն և կարգավորումները բյուրեղացրել են մի քանի հիմնական սկզբունքներ[4]:
   - **Թափանցիկություն**. Օպերատորները պետք է իրենց բաժանորդներին համակողմանի և ճշգրիտ տեղեկատվություն տրամադրեն ցանցի կառավարման և ծառայությունների որակի մասին:
   - **Խտրականության բացակայություն**. Օպերատորները պետք է թրաֆիքի խտրկանություն չցուցաբերեն՝ ելնելով ուղարկողից և ստացողից և բովանդակության տեսակից, ինչպես նաև հավելվածի և/կամ ծառայության տեսակից:
   - **Մատչելիություն**. Օգտագործողները պետք է անխոչընդոտ մուտք ունենան դեպի ՕՐԻՆԱԿԱՆ բովանդակություն, ծառայություններ կամ հավելվածներ (երաշխավորելով ծառայության նվազագույն որակի ապահովում բարեխիղճ օգտագործման համար) կամ միանալ որևէ սարքի, որը ցանցը չի վնասում:

Այլ հարցեր, որոնց հաճախ են անդրադառնում միջազգային ֆորումներում. Արտահայտվելու ազատություն, տեղեկատվության մատչելիություն և ընտրություն, մասնավոր կյանքի գաղտնիություն և անձնական տեղեկատվության պաշտպանություն, նվազագույն որակի և անվտանգության ապահովում և ցանցի դիմացկունություն, ներգրավված բոլոր կողմերի իրավունքների, դերերի և հաշվետվողականության սահմանում (ծառայություններ տրամադրողներ, կարգավորողներ, օգտատերեր և այլն):

7. Ձեր կարծիքով ինչպիսի՞ն է առցանց տիրույթում մարդու իրավունքների վիճակը Հայաստանում: Արդյո՞ք կարողանում եք ազատորեն իրացնել Ձեր իրավունքները ինտերնետի միջոցով: Խնդրում ենք մանրամասնել:
8. Որո՞նք են Հայաստանում գործող կարգավորիչ մեխանիզմները, որոնք ապահովում են/սահմանափակում են/միջամտում են ինտերնետի ազատությանը:
9. Որքա՞ն հաճախ և/կամ որքա՞ն դյուրին կարող են Ձեր կամ Ձեր գործընկերների իրավունքները սահամանափակվել առցանց տիրույթում: Տեղյա՞կ եք վերջին շրջանում ինտերնետի ազատության սահմանափակման դեպքերի մասին:

III. Ձեր ստեղծած բովանդակությունը ինտերնետում. ո՞վ է փորձում գտնել այն (25-30 րոպե)

10. Ինչու՞ եք կարծում, որ Ձեր ստեղծած բովանդակությունը այնքան հրապուրիչ է կամ հրապուրիչ չէ որևէ մեկի համար, որ նա փորձի կոտրել Ձեր կամ Ձեր գործընկերների համակարգը: Ինչու՞ պետք է որևէ մեկը փորձի կոտրել Ձեր համակարգը կամ վտանգի տակ դնի Ձեր ստեղծած բովանդակությունը:

11. Ինտերնետի սովորական օգտվողից մինչև հնարավոր թիրախ. ի՞նչն է Ձեզ առանձահատուկ դարձնում Ձեր գործունեության ոլորտում և ավելի լայն լսարանի համար:

[4] Ինտերնետի կառավարման ուղեցույց (6-րդ հրատ.), Յովան Քուրբալիջա, DiploFoundation, Ժնև, Շվեյցարիա 2014

12. Ո՞վ կարող է լինել այն անձը/խումբը, ով սպառնում է Ձեր կամ Ձեր կազմակերպության տեղեկատվական համակարգերին: Դուք կամ Ձեր կազմակերպությունը նման սպառնալիքների հետ առերեսվե՞լ եք:
13. Կարո՞ղ եք մանրամասնել տեղեկատվության անվտանգությանն առնչվող առավել տարածված խնդիրները կամ կոնկրետ դեպքերը, որոնց մինչև հիմա հանդիպել եք:

IV. Տեղեկատվական անվտանգության հիմունքները. ի՞նչ եք անում դուք և Ձեր կազմակերպությունը առօրյա աշխատանքում անվտանգ առցանց միջավայր ապահովելու նպատակով (20-25 րոպե)

«Հաքերին միայն անվտանգության սողանցք է պետք գտնել, մինչդեռ ՏՏ և անվտանգության մասնագետները պետք է գտնեն և փակեն դրանք»[5]:

14. Անհատական մակարդակ. Ինչպե՞ս եք գնահատում Ձեր գիտելիքներն ու հմտությունները տեղեկատվության անվտանգության ոլորտում: Ի՞նչ հատուկ քայլեր եք ձեռնարկում ցանցի միջոցով տեղեկատվության անվտանգ փոխանակման համար: Անձնական հաշիվներ, գաղտնաբառեր (երկաստիճան պաշտպանություն), ճշգրտում/աղբյուրների գնահատում, շարժական սարքերի պաշտպանություն, էլեկտրոնային փոստի գաղտնագրման ծրագրեր և այլն:
15. Ինստիտուցիոնալ մակարդակ. Ո՞րն է Ձեր հաստատության քաղաքականությունը (եթե այդպիսին կա ՏՏ անվտանգության և տեղեկատվական սահուն հոսքերի ոլորտում. արտոնագրված ծագրե՞ր/ծրագրային փաթեթնե՞ր, բաց աղբյուրներով օպերացիոն համակարգե՞ր (OS X, Linux) և այլն:
16. Շարժական օպերատորների և քաղաքականության մակարդակով. Կա՞ քաղաքականություն և/կամ կարգավորումներ Ձեզ կամ Ձեր կազմակերպության տեղեկատվական համակարգերի անվտանգությունն ապահելու համար:

V. ՏՏ անվտանգության տարրական և խորը հմտություններ. բարելավման կարիք կա՞ (15-20 րոպե)

17. Որքանո՞վ եք ինքներդ Ձեզ իրազեկ համարում ՏՏ հիգիենայի և անվտանգության կանոնների վերաբերյալ: Մի՞շտ եք դրանք առաջնահերթ համարում: Հե՞շտ է արդյոք հավասարակշռություն գտնել Ձեր հիմնական մասնագիտական գործունեության և տեղեկատվական անվտանգության հնարավոր սպառնալիքներից Ձեզ և Ձեր սոցիալական ցանցերը պաշտպանելու պարտականության միջև: Ինչքանո՞վ պետք է «մտասևեռված» լինել սեփական սարքավորումների առողջության և անվտանգության խախտումների կանխման նկատմամբ:

18. Որո՞նք են այն հիմնական աղբյուրները, որոնցից դուք կարող եք օգտակար խորհուրդներ ստանալ: Որո՞նք են այն աղբյուրները, որոնց երբեք չեք վստահի և ինչու՞: Ձեզանից քանի՞սը կօգտվի այս խնդրով զբաղվող առցանց ռեսուրսներից: Եթե չեք օգտվի, ինչու՞:

VI. Խաղի մշակում (5-10 րոպե)

19. ՄՆԿ-ը պատրաստվում է խաղ մշակել առցանց տիրույթում մարդու իրավունքների ուսուցման և առաջխաղացման համար՝ մասնավորապես նպատակ ունենալով լրագրողներին, քաղաքացիական հասարակության ներկայացուցիչներին տրամադրել այն գործիքները, որոնք անհատներին և կազմակերպություններին անհրաժեշտ են արագ զարգացող առցանց միջավայրում տեղեկատվական անվտանգության սպառնալիքներից և խոցելիությունից պաշտպանվելու համար:

[5] https://archive.org/details/Wiley.Hacking.5th.Edition.Jan.2016.ISBN.1119154685.Profescience.blogspot.com

Ի՞նչ եք կարծում այս նախաձեռնության մասին և ի՞նչ հիմնական գծեր կուզենայիք տեսնել նորաստեղծ խաղում:

VII. ԵԶՐԱՓԱԿԻՉ ԽՈՍՔ (5 րոպե)

Շատ շնորհակալություն Ձեր տրամադրած ժամանակի և ակտիվ մասնակցության համար: Սա կարծիքների արժեքավոր փոխանակում էր: Խնդրում եմ հայտնել ինձ, եթե մեր կողմից քննարկված հարցերի վերաբերյալ ավելացնելու բան ունեք: Եվս մեկ անգամ շնորհակալություն!

Խորքային հարցազրույցի և ֆոկուս խմբի քննարկման ժամանակացույցը

Ամսաթիվը/ ժամը	Անուն	Կազմակերպություն/պաշտոն
26/04/2017; 1:00pm	Միքայել ՂԱԶԱՐՅԱՆ	Teamable ծրագրային պլատֆորմ/ծրագրերի պատասխանատու
26/04/2017; 2:30pm	Էդգար ՄԱՐՈՒՔՅԱՆ	RenderForest/Տեխնիկական տնօրեն
27/04/2017; 11:00am	Ռուբեն ՄՈՒՐԱԴՅԱՆ	UCOM/SS աուդիտոր; Պանարմենիան Մեդիա Գրուպի խորհրդի անդամ
27/04/2017; 1:30pm	Նորայր ՉԻԼԻՆԳԱՐՅԱՆ	Տվյալների գծով պատասխանատու
27/04/2017; 4:30pm	Նարինե ԴԱՆՂՅԱՆ	Մեդիամաքս
27/04/2017; 5:30pm	Դավիթ ԱԼԱՎԵՐԴՅԱՆ	Մեդիամաքս
29/04/2017; 12:00pm	Գրիգորի Սաղյան	«Ինտերնետ Հանրություն» Հայաստան/փոխնախագահ
29/04/2017; 2:30pm	Հասմիկ ԱԼԱՎԵՐԴՅԱՆ	Պանարմենիան Մեդիա Գրուպ
4/05/2017; 12:00pm	Գևորգ ՀԱՅՐԱՊԵՏՅԱՆ	ՀՀ Արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության Վարչական վարույթների իրականացման վարչության պետ
4/05/2017; 2:00pm	Քրիստինե ԱՂԱԼԱՐՅԱՆ	«Հետք»
12/05/2017; 4:00pm	Վահագն ԱՆՏՈՆՅԱՆ	«Խաղաղության երկխոսություն»/Վանաձոր
13/05/2017; 12:00pm	Անժելա ՍՏԵՓԱՆՅԱՆ	ԱԼՏ ՀԸ/Արմավիր
13/05/2017; 2:00pm	Անահիտ ԲԱՂԴԱՍԱՐՅԱՆ	Մեդիա ակումբ/Գորիս, «Հետք»
15/05/2017; 2:00pm	Արմինե ՍԱԴԻԿՅԱՆ	Հելսինկյան քաղաքացիական ասամբլեա/Վանաձոր

Ամսաթիվը/ժամը	Անուն	Կազմակերպություն
3/05/2017; 12:00pm	Աննա ՇԱՀՆԱԶԱՐՅԱՆ	Քաղաքացիական ակտիվիստ
	Շահեն ՀԱՐՈՒԹՅՈՒՆՅԱՆ	Քաղաքացիական ակտիվիստ
	Արփինե ԶԱՐԳԱՐՅԱՆ	Քաղաքացիական ակտիվիստ
	Հելենա ՄԵԼՔՈՆՅԱՆ	Քաղաքացիական ակտիվիստ
	Վաղինակ ՇՈՒՇԱՆՅԱՆ	Քաղաքացիական ակտիվիստ
	Փիրուզա ՊԵՏՐՈՍՅԱՆ	Քաղաքացիական ակտիվիստ
	Զարուհի ՀՈՎՀԱՆՆԻՍՅԱՆ	Քաղաքացիական ակտիվիստ
3/05/2017; 4:00pm	Գոհար ՈՍԿԱՆՅԱՆ	Հայաստանի Հելսինկյան կոմիտե

	Մարիամ ՍԱՐԳՍՅԱՆ	Քաղաքացիական հասարակության ինստիտուտ
	Աննա ԺԱՄԿՈՉՅԱՆ	Socioscope
	Մամիկոն ՀՈՎՍԵՓՅԱՆ	ՓԻՆՔ Արմենիա
	Էդուարդ ԴԱՆԻԵԼՅԱՆ	Հելսինկյան ասոցիացիա
	Արման ՂԱՐԻԲՅԱՆ	Իրավունքի գերակայություն ՀԿ
	Լիլիթ ՀՈՎՀԱՆՆԻՍՅԱՆ	Խոսքի Ազատության պաշտպանության կոմիտե
4/05/2017; 6:00pm	Քրիստինա ՍԼՈՅԱՆ	Սիվիլնեթ
	Գայանե ԱՍՐՅԱՆ	Media.am
	Հովհաննես ՄՈՎՍԻՍՅԱՆ	«Ազատություն» ռադիոկայան
	Գևորգ ԹՈՍՈՒՆՅԱՆ	Iravaban.net
	Քնարիկ ԽՈՒԴՈՅԱՆ	Epress.am
	Կարինե ԱՍԱՏՐՅԱՆ	A1+ առցանց հեռուստաընկերություն