Բազմակողմանի տեղեկատվության
ինստիտուտ

ԹՎԱՅԻՆ ԻՐԱՎՈՒՆՔՆԵՐԸ ԵՎ ԴՐԱՆՑ ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ ԻՆՖՈՐՄԱՑԻՈՆ ՀԱՍԱՐԱԿՈՒԹՅԱՆ ՀԱՄԱՐ

Դավիթ Սանդուխչյան

ԹՎԱՅԻՆ ԻՐԱՎՈՒՆՔՆԵՐԻ ՀԵՏ ԿԱՊՎԱԾ ՄԱՐՏԱՀՐԱՎԵՐՆԵՐԸ ՀԱՅԱՍՏԱՆՈՒՄ

Սամվել Մարտիրոսյան

Երևան
2021

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

ԹՎԱՅԻՆ ԻՐԱՎՈՒՆՔՆԵՐԸ ԵՎ ԴՐԱՆՑ ԿԱՐԵՎՈՐՈՒԹՅՈՒՆԸ ԻՆՖՈՐՄԱՑԻՈՆ ՀԱՍԱՐԱԿՈՒԹՅԱՆ ՀԱՄԱՐ

Դավիթ Սանդուխչյան

ՆԵՐԱԾՈՒԹՅՈՒՆ

Այս հոդվածը նպատակ ունի ներմուծել թվային իրավունքների հասկացությունն այնպես, ինչպես դրանք ընկալվում են իրավաբանների, հետազոտողների և իրավապաշտպանների կողմից: Թվային տեխնոլոգիաների և հաղորդակցությունների արագընթաց զարգացման արդյունքում ի հայտ են եկել բազմաթիվ նոր իրավական և հանրային քաղաքականության ոլորտներ, օրինակ՝ անձնական տվյալների պաշտպանություն, կիբերոստիկանություն, կիբերանվտանգություն և այլն: Այս հոդվածն անդրադառնում է այդ ոլորտներից միայն մեկին, որը հաճախ անվանում են թվային իրավունքներ: Այն կարող է հետաքրքիր և օգտակար լինել քաղաքացիական հասարակության գործունեության, քաղաքական գործիչների, պետական իշխանության մարմինների և քաղաքականության վերաբերյալ որոշումների կայացման կամ այդ քաղաքականությունների մասին հանրային քննարկումներում ներգրավված անձանց և կազմակերպությունների համար:

Հոդվածն առաջին հերթին ուղղված է հայաստանյան լսարանին, և դրա առաջին մասը պարունակում է հայաստանյան քաղաքականությունների, իրավական և կարգավորող շրջանակների վերլուծություն: Երկրորդ մասը նվիրված է առհասարակ թվային իրավունքների հասկացությանը: Երրորդ մասը նկարագրում է թվային իրավունքների ընդհանուր հասկացությունը և անդրադառնում դրանց ազդեցությունների և համապատասխան միջազգային փաստաթղթերով կարգավորվող կոնկրետ ոլորտներին: Վերջին երկու բաժինները ներկայացնում են հայաստանյան օրենսդրության վերլուծությունը թվային իրավունքների իրացման համատեքստում և առաջարկում մի շարք քայլեր՝ դրանց պաշտպանությունն ուժեղացնելու նպատակով:

Ի՞ՆՉ ԵՆՔ ՀԱՍԿԱՆՈՒՄ «ԹՎԱՅԻՆ ԻՐԱՎՈՒՆՔՆԵՐ» ԱՍԵԼՈՎ

Ցանկացած տեսություն սկսվում է քննարկումը հնարավոր դարձնող հասկացությունների և գաղափարների սահմանմամբ: Դրանց սահմանումը հատկապես կարևոր է այն ժամանակ, երբ քննարկման մասնակիցներն ունեն մասնագիտական, մշակութային և կրթական տարբեր հենքեր: Այս մոտեցումը հատկապես կարևոր է տեխնոլոգիաների և իրավական թեմաների շուրջ միջգիտակարգային և միջոլորտային քննարկումների համար:

Հիմքերը

Հարցերից մեկը, որ հաճախ քննարկում են իրավաբանները, այն է, թե ինչպես են թվային իրավունքները տարբերվում մարդու ավանդական հիմնարար իրավունքներից: Մարդու հիմնարար իրավունքը անհատի բնական իրավունքների՝ մարդու իրավունքների միջազգային պայմանագրերով, օրինակ՝ Մարդու իրավունքների համընդհանուր հռչակագրով և Մարդու իրավունքների եվրոպական կոնվենցիայով պաշտպանվող և քաջ հայտնի իրավական հասկացություն է: Թվային իրավունքը նոր հասկացություն է, որն ինքնին ուղղակիորեն սահմանված չէ միջազգային պայմանագրերում և/կամ հռչակագրում, բայց հաճախ այն անվանում են թվային միջավայրում մարդու իրավունքներ:

Ինչպե՞ս են թվային իրավունքները հարաբերակցվում մարդու իրավունքի ավանդական հասկացություններին, և որո՞նք են դրանց միջև առկա տարբերությունները (եթե այդպիսիք առհասարակ կան)՝ այս հարցին պատասխանելիս հարկ է նկատի առնել միջազգային և եվրոպական պայմանագրերի իրականացման համապատասխան ուղեցույցները: Եվրոպայի խորհուրդն ընդունել է թվային իրավունքների և համացանցին վերաբերող ազատությունների մասին փաստաթղթերի մի ամբողջ գրադարան: Եվրոպայի խորհրդի ընդունած առաջին փաստաթղթերից մեկը Համացանցում հաղորդակցության ազատության հռչակագիրն է, որն ընդունվել է 2003 թվականի մայիսի 28-ին:

Համացանցում հաղորդակցության ազատության հռչակագիրը[1] զրոյից չի գրվել. այն հիմնված է Մարդու իրավունքների եվրոպական դատարանի նախադեպային իրավունքի, Եվրոպական միության՝ համացանցի օգտագործման կոնկրետ ոլորտները ղեկավարող օրենսդրության, օրինակ՝ էլեկտրոնային առևտրի և անձնական տվյալների պաշտպանության ԵՄ դիրեկտիվների վրա: Հռչակագիրն ուրվագծում է համացանցում հաղորդակցության ազատության 7 սկզբունքները, որոնք կարելի է համարել թվային իրավունքների հիմքը. ըստ էության, դրանք հենց այդպես էլ հայտնի են կամ ընկալվում են այսօր իրավաբանների և քաղաքացիական հասարակության ակտիվիստների կողմից: Եվրոպայի խորհրդի հաստատությունների կողմից ընդունված և համացանցային ազատությանը վերաբերող փաստաթղթերը, օրինակ՝ հռչակագրերը, Նախարարների կոմիտեի հանձնարարականները և ուղեցույցները արտացոլում են այս հիմնարար սկզբունքները և կապված են դրանց հետ:

Համացանցում հաղորդակցության ազատության մասին հռչակագրի սկզբունքները սերտորեն կապված են արտահայտվելու ազատության հետ, որը պաշտպանվում է Մարդու իրավունքների եվրոպական կոնվենցիայի 10-րդ հոդվածով: Այնուամենայնիվ, սկզբունքները դուրս են գալիս արտահայտվելու ազատության տիրույթից և ներառում են Մարդու իրավունքների եվրոպական դատարանի (ՄԻԵԴ) պաշտպանությանը ենթակա այլ իրավունքներ: Դա առանցքային փաստ է, որը մենք կքննարկենք այս փաստաթղթում հաջորդիվ:

[1] Համացանցում հաղորդակցության ազատության մասին ԵԽ Նախարարների կոմիտեի հռչակագիրը. ընդունվել է 2003թ. մայիսի 28-ին: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbd5

Առաջին սկզբունքը վերաբերում է բովանդակության կարգավորման կանոններին: **Համացանցային բովանդակության կանոնների** սկզբունքը հռչակում է, որ անդամ պետությունները չպետք է ընդունեն բովանդակության մատուցման այլ տեսակների, այսինքն՝ հաղորդակցության և մեդիայի համար արդեն իսկ գոյություն ունեցող սահմանափակումներից զատ համացանցային բովանդակության այլ սահմանափակումներ: Այսպիսով ստեղծվում է Մարդու իրավունքների եվրոպական կոնվենցիայի 10-րդ հոդվածի ակնհայտ պահանջի բավարարման տպավորություն: Այնուամենայնիվ, դա այնքան էլ ընդունելի չէր 2000-ականների սկզբին և դեռևս վիճարկվում է Եվրոպայի խորհրդի անդամ մի շարք պետություններում:

Երկրորդ սկզբունքը, որը սահմանվում է որպես **Ինքնակարգավորում և համատեղ կարգավորում,** բավականին լայն է և ոչ հստակ: Այն սահմանում է, որ «անդամ պետությունները պետք է քաջալերեն համացանցում բովանդակության տարածմանն առնչվող ինքնակարգավորումը և համատեղ կարգավորումը»: Այնուհանդերձ, նույնիսկ խիստ դեկլարատիվ սկզբունքները կարող են օգտակար լինել, երբ կառավարությունը կամ օրենսդիր մարմինը որոշում է կոնկրետ մեխանիզմ՝ անդրադառնալու հանրային քաղաքականության կոնկրետ խնդիրներին: Օրինակ՝ եթե պետությունը ցանկանում է անդրադառնալ համացանցում ատելության խոսքի խնդրին, այն պետք է կոչ անի կոնկրետ ոլորտի ներկայացուցիչներին կամ ասոցիացիաներին առաջարկել ոչ օրենսդրական, այսինքն՝ ինքնակարգավորող լուծում կամ մոդել, որում նախատեսված կլինեն երկուսն էլ՝ կառավարության ակտիվ ներգրավվածությունը՝ ոլորտը ներկայացնող կազմակերպությունների ակտիվ մասնակցությանը զուգահեռ:

Հռչակագրով սահմանվող ամենավճռորոշ սկզբունքներից մեկը, որն ուղղակիորեն կապված է Մարդու իրավունքների եվրոպական հռչակագրի 10-րդ հոդվածի հետ, **Նախնական պետական հսկողության բացակայության** երրորդ սկզբունքն է: Սկզբունքները կարող են և պետք է մեկնաբանվեն որպես արգելք՝ զտելու կամ արգելափակելու հավանաբար անօրինական կամ հակասական բովանդակություն պարունակող տեղեկատվությունը: Սկզբունքը կարող է նաև անվանվել համացանցային գրաքննություն: Սա չի նշանակում, որ ոչ պետական դերակատարները, օրինակ՝ դպրոցները, համալսարանները կամ համացանցին հանրային հասանելիություն տրամադրողները չեն կարող օգտագործել անչափահասների համար չնախատեսված համապատասխան բովանդակության զտիչներ: Ակնհայտորեն, սկզբունքը վերաբերելի չէ նրանց նկատմամբ, ովքեր կամավոր հիմունքով են սահմանափակում ռեսուրսների որևէ կատեգորիային իրենց հասանելիությունը:

Նախնական պետական հսկողության բացակայության սկզբունքը բացարձակ չէ. համացանցային բովանդակության արգելափակումը կարող է իրավաչափ միջոց լինել՝ կանխելու հանցագործությունը, երբ այն վտանգ է ներկայացնում հանրության համար կամ ենթադրում է որևէ անձի իրավունքների ոտնահարում: Տվյալ դեպքում պետական իշխանությունները պետք է դիմեն դատական ատյաններին՝ դատական կարգով խնդրի վերանայման, կամ օրենքով լիազորված համապատասխան մարմնի որոշման համար:

Չորրորդ սկզբունքը սահմանվում է հռչակագրի ներքո հետևյալ կերպ՝ **Տեղեկատվական հասարակությունում անհատների մասնակցության** արգելքների վերացում: Այս սկզբունքը ենթադրում է անդամ-պետությունների դրական պարտավորությունը՝ ապահովել տեղեկատվական ծառայությունների հասանելիությունը քաղաքացիների համար և վերացնել Մարդու իրավունքների եվրոպական կոնվենցիայի 10-րդ հոդվածի ներքո երաշխավորվող նրանց իրավունքների իրացման սահմանափակումները: Հռչակագրի ընդունման ժամանակ եվրոպական երկրների մեծ մասն արդեն ընդունել էր հայեցակարգը, և համապատասխան կարգավորող գործիքները սովորաբար անվանվում են «համընդհանուր ծառայություններ»:

Չորրորդ սկզբունքը ենթադրում է, որ անդամ պետությունները պետք է ունենան թե՛ պասիվ, թե՛ ակտիվ պարտավորություններ՝ վերացնելու անհատների կողմից համացանցի օգտագործման արգելքները: Առաջին հերթին, անդամ-պետությունները չպետք է սահմանափակեն անհատների համար ազատ, այսինքն՝ առանց թույլտվության, հատուկ գրանցման կամ որևէ այլ վարչական ընթացակարգի համացանցի հասանելիության իրավունքը: Դա նորմալ գործելաոճ է թվում, սակայն իրականությունն այլ է. մի շարք ոչ անդամ պետություններում անհատներին համացանցի հասանելիություն է տրվում գրանցման և օգտատերերի ինքնության պարտադիր ստուգման արդյունքում շնորհվող թույլտվության միջոցով:

Այնուամենայնիվ, Հռչակագրի չորրորդ սկզբունքն ուղղված է ոչ միայն համացանցային ծառայությունների հասանելիության ու դրանց ազատ օգտագործման հնարավոր սահմանափակմանը: Համացանցի օգտագործման արգելքների վերացումը կարող է և պետք է մեկնաբանվի որպես դոմենային անուն (ծագման կամ օտարերկրյա պետության ծածկագիրը) ունենալու և կոնկրետ ոլորտային կարգավորման չենթարկվող տեղեկատվությունն ազատ հրապարակելու իրավունք (տե՛ս Առաջին սկզբունքը):

Հաջորդ՝ հինգերորդ սկզբունքը նույնպես կապված է համացանցի օգտագործման ազատությունների հետ, բայց արդեն ավելի շուտ տնտեսական, քան՝ տեղեկատվության և հաղորդակցության ազատության համատեքստում: Սկզբունքը սահմանվում է որպես **Համացանցի միջոցով ծառայություն մատուցելու ազատություն**: Այն նախատեսում է, որ համացանցային ծառայությունները չպետք է ենթակա լինեն հատուկ թույլտվության կամ լիազորման բացառապես այն հիմքով, որ իրականացվում են էլեկտրոնային հաղորդակցման միջոցներով: Այս սկզբունքը շատ է տարբերվում ավանդական, այն է՝ Մարդու իրավունքների եվրոպական կոնվեցիայով պաշտպանվող իրավունքներից և ազատություններից, քանի որ դե ֆակտո հռչակում է առանց արգելքների և վարչական խոչընդոտների տնտեսական գործունեության երաշխիքների տրամադրում: Այս սկզբունքը փաստացի հռչակում է, որ համացանցի միջոցով տնտեսական գործունեություն իրականացնելու իրավունքը կենսական է բոլոր անհատների համար և չպետք է սահմանափակվի առանց օրինական պատճառի:

Վեցերորդ սկզբունքը նույնպես ավելի շատ վերաբերում է համացանցում գործող բիզնեսների տնտեսական գործունեությանը: Արտասովոր է թվում, որ Եվրոպայի խորհրդի փաստաթուղթն անդրադառնում է տնտեսական, սակայն ոչ քաղաքացիական իրավունքներին և հիմնարար ազատություններին: Այն հանրահայտ է դարձել էլեկտրոնային առևտրի՝ Եվրամիության վաղ շրջանի կարգավորումներից և սահմանվում է որպես համացանցային բովանդակության համար ծառայություններ մատուցողների սահմանափակ պատասխանատվություն: Սկզբունքը հիմնված է այն գաղափարի վրա, որ համացանցային ծառայություններ մատուցողները չպետք է պատասխանատվություն կրեն իրենց կողմից չստեղծված բովանդակության համար և չպետք է պարտավորվեն համացանցային բովանդակության մշտադիտարկում իրականացնել:

Այնուամենայնիվ, այս սկզբունքի նկարագրությունը բացատրում է, որ ծառայություն մատուցողները կարող են համատեղ պատասխանատվություն կրել այն դեպքերում, երբ գիտակցաբար հրաժարվել են հեռացնել կամ արգելափակել անօրինական բովանդակությունը հայտնաբերումից կամ հեռացման կամ արգելափակման մասին օրինական պահանջը ստանալուց հետո: Այս դեպքում, ծառայություն մատուցողները պետք է բաց տեքստով, հստակ ցուցումներ ստանան իրավապահ մարմիններից: Անդամ-պետությունները պետք է սահմանեն այնպիսի ընթացակարգեր, որոնք կհավասարակշռեն արտահայտման ազատության հանրային շահը և անօրինական կամ վնասակար բովանդակությունից հասարակության պաշտպանությունը:

Ի վերջո, յոթերորդ սկզբունքը վերաբերում է այսօր ամբողջ աշխարհում հաճախ քննարկվող թվային իրավունքներին: Սկզբունքը սահմանվում է ընդամենը մեկ բառով, բայց այն առավել հաճախ ոտնահարվող սկզբունքն է ներկայիս համացանցին առնչվող քաղաքականություններում՝ թե՛ կայացած, թե՛ նորահայտ ժողովրդավարություններում: Սա **Անանունության** սկզբունքն է՝ իրավունք, որը բնորոշ է բացառապես թվային դարաշրջանին և չի եղել պայքարի առարկա դեռ անգամ մեկ սերունդ առաջ:

Համացանցի օգտատերերի անանունությունը կարևորվել է համացանցում անհատների թողած ավելի ու ավելի մեծաթիվ հետքերի, տվյալների մշակման հզորությունների արագընթաց զարգացման և օգտատերերի պրոֆիլների դուրսբերման համար արհեստական բանականության կիրառման պատճառով: Այնուամենայնիվ, Հռչակագիրը սահմանում է, որ օգտատերերի անանունության նկատմամբ հարգանքը չպետք է խոչընդոտի «անդամ-պետությունների՝ համապատասխան միջոցներ ձեռնարկելը և ներպետական օրենսդրությամբ սահմանվող հանցավոր արարքների համար պատասխանատուներին գտնելուն ուղղված համագործակցության քայլերը»:

Հռչակագիրը հստակ սահմանում է, որ հարկ է քայլեր ձեռնարկել՝ հետևելու հանցավոր արարքների համար պատասխանատուներին: Այս դրույթը կարևոր է, որովհետև այն անդամ-պետություններին կոչ է անում ձեռնպահ մնալ համացանցի օգտատերերի ինքնությունը պարտադիր ստուգելուց: Համացանցային հաղորդակցություններում անանունության սկզբունքի պաշտպանությունը և անշեղ կիրարկումը խիստ արդարացված է: Հիմնական պատճառն այն է, որ անհատները պետք է համոզված լինեն, որ անվտանգ են կիբերտարածքում: Նույնականացված անձինք ամենախոցելին են երկու շահագրգիռ կողմերի՝ կիբերհանցագործների և պաշտոնեական դիրքը չարաշահողների գործողությունների համար:

«Անանունություն» եզրով նկարագրվող սկզբունքը չի սահմանափակվում պետությունների այն պարտավորությամբ, ըստ որի նրանք պետք է ձեռնպահ մնան ծառայություններ մատուցողներից պարտադիր կերպով օգտատերերին նույնականացնել ու հետագայում այդ տվյալներն իրավապահ մարմիններին և անվտանգության գերատեսչություններին ներկայացնել պահանջելուց: Այս սկզբունքը շատ ավելի լայն է և ընդգրկում է պետությունների և մասնավոր հատվածի դերակատարների համար մի շարք այլ պարտավորություններ: Մասնավորապես՝ դա նշանակում է, որ անդամ պետությունները պետք է սահմանափակումներ դնեն անհատների և բիզնեսների կողմից գաղտնագրման (կրիպտոգրաֆիկ) միջոցների գործածման վրա: Սա նաև նշանակում է, որ չպետք է լինեն հաղորդակցության ապահով արձանագրությունների, օրինակ՝ վիրտուալ մասնավոր ցանցերի (VPN), անվտանգ պատյանաշերտի (SSH) կամ անվտանգության սերտիֆիկատների կոնկրետ տեսակների կիրառման վրա դրվող սահմանափակումներ:

Վերը նշված սահմանափակումներն անհեթեթ կարող են հնչել, սակայն դրանք իրականում առկա են մի շարք երկրներում, այդ թվում նաև Եվրոպայի խորհրդի անդամ պետություններից մեկում: 2020թ. Ռուսաստանի կառավարությունը շրջանառության մեջ դրեց մի օրինագիծ[2], որը նախատեսում էր անվտանգ պատյանաշերտի (SSL) և տրանսպորտային մակարդակի անվտանգության արձանագրությունների (TSL) ու մի շարք այլ սահմանափակումներ, որոնք թույլ չէին տալիս օգտատերերին համացանցային որոնումներ կատարել՝ այցելած ռեսուրսների օգտագործմամբ պրոֆայլինգի ռիսկի չենթարկվելով: 2019թ. հունիսին Ղազախստանի կառավարությունը փորձեց ստիպել օգտատերերին՝ տեղադրել կառավարության կողմից թողարկված անվտանգության սերտիֆիկատներ, որոնք անվտանգության ծառայություններին թույլ կտային հետևել օգտատերերի թրաֆիքին[3]: Թեև այս միջոցները հիմնականում ձախողվել են տեխնոլոգիական հսկաների (Apple, Mozilla և Google) կողմից պատշաճ արձագանքի չարժանանալու և մի շարք տեխնոլոգիական սահմանափակումների պատճառով, փաստն ինքնին արժանի է ուշադրության և բավականին մտահոգիչ է:

Ի՞նչ իրավունքներ ենք մենք ստացել

Ճիշտ կլիներ ասել, որ Համացանցում հաղորդակցության ազատության մասին Նախարարների կոմիտեի հռչակագիրը հիմնարար փաստաթուղթ է, որը սահմանում է ամբողջ Եվրոպայում համացանցի կարգավորման շրջանակի հետագա զարգացումը կողմնորոշող հիմնական սկզբունքները: Հռչակագիրն ընդունվել է 2003թ. և հիմնված է տվյալ ժամանակի իրողությունների և ընկալումների վրա: Տեխնոլոգիաներն այնքան արագ են զարգացել, որ մինչև 2020թ. համացանցին վերաբերող մարդու իրավունքների խնդիրները գրեթե կրկնապատկվել են: Ավելին, Սահմանադրությամբ ամրագրված սկզբունքների իրագործումն այնքան է բարդացել, որ պահանջվել են տարբեր ոլորտներ ներկայացնող մասնագիտական խմբերի ջանքերը:

---

[2] Տեխնոլոգիաների մասին գրող ռուսաստանյան և միջազգային մի շարք ամսագրեր սեպտեմբերի կեսերին հաղորդեցին այն մասին, որ Ռուսաստանի կառավարությունը շրջանառության մեջ է դրել անվտանգ արձանագրությունների օգտագործումը սահմանափակող օրինագիծ: https://regulation.gov.ru/projects#npa=108513

[3] 2019թ. Ղազախստանի կառավարությունը խնդրեց համացանցային ծառայություններ մատուցողներին կասեցնել այն օգտատերերին մատուցվող ծառայությունները, որոնք չեն օգտվում կառավարության կողմից թողարկված սերտիֆիկատից: Ավելի ուշ, երբ տեխնոլոգիական հսկաները (Google և Mozilla) արգելափակեցին այս սերտիֆիկատները, Ղազախստանի կառավարությունը փոխեց քաղաքականությունը՝ պարտադրելով սերտիֆիկատների օգտագործումը միայն երկրում գտնվող կոնկրետ ռեսուրսներից օգտվելու համար: https://en.wikipedia.org/wiki/Kazakhstan_man-in-the-middle_attack

Կարևոր է այն փաստը, որ Հռչակագիրը սահմանում է 7 վճռորոշ սկզբունքներ և հիմք է հանդիսանում թվային իրավունքների հասկացության հետագա զարգացման համար: Այն չի վերաբերում բոլոր իրավունքներին, որոնք կարող ենք թվայինների շարքին դասել, սակայն վերաբերում է այն իրավունքներին, որոնք անդամ-պետությունները համաձայնել են համարել հիմնարար այդ ժամանակ: Ավելին, եթե ամփոփելու լինենք, սկզբունքները կարող էին համադրվել՝ սահմանելու կոնկրետ թվային իրավունքը մեզ այսօր հայտնի տեսքով: Իրավունքները՝ որպես սկզբունքների համադրում, կարող են ձևակերպվել հետևյալ կերպ.

- Տեղեկատվություն որոնելու, ստանալու և տարածելու համար համացանցի հասանելիության և օգտագործման իրավունքը՝ առանց նախնական հսկողության և բովանդակության նկատմամբ ըստ տարածման մեդիայի սահմանափակման: Այս սահմանումը առաջին, երրորդ և չորրորդ սկզբունքների համակցումն է:

- Համացանցում ծառայություններ մատուցելու իրավունքը՝ առանց հաղորդման համար օգտագործված եղանակի բացառիկ հիմքով կոնկրետ սուբյեկտի լիազորման և առանց ծառայություն մատուցողների՝ իրենց ծառայությունների միջոցով հաղորդված բովանդակությունը մշտադիտարկելու պարտավորության,

- Համացանցի անանուն օգտագործման, այդ թվում՝ առանց նախնական պարտադիր թույլտվության և ինքնության հաստատման անանուն որոնումների, տեղեկություններ ստանալու և հաղորդելու իրավունքը: Թվային այս էական իրավունքը նորություն է անգամ Եվրոպայի խորհրդի հիմնարար փաստաթղթի՝ Մարդու իրավունքների եվրոպական հռչակագրի համատեքստում:

Հռչակագրում լավ չներկայացված ևս մի սկզբունք է համացանցի օգտատերերի անձնական կյանքի անձեռնմխելիության իրավունքը: Այնուամենայնիվ, այն լավ ներկայացված չէ այս փաստաթղթում, ոչ թե այն պատճառով, որ անձնական կյանքի անձեռնմխելիության իրավունքը անտեսվել է Եվրոպայի խորհրդի կողմից: Ընդհակառակը, անհատների անձնական կյանքի անձեռնմխելիության իրավունքն այն ոլորտներից մեկն է, որին Եվրոպայի խորհուրդը մշտապես անդրադարձել է: Թվային ժամանակներում անձնական կյանքի անձեռնմխելիության իրավունքը հատկապես ներառված է Եվրոպայի խորհրդի փաստաթղթերում, որոնք քննարկվում են հաջորդիվ:

Անձնական կյանքի անձեռնմխելիության իրավունքը

Իսկապես, Հռչակագիրը դարձել է իրավագիտության և մարդու իրավունքների տեսության մեջ նոր հասկացության՝ այժմ մեր կողմից «թվային իրավունքներ» կոչվողի ձևավորման էական հիմք: Ինչպես նշված է վերը, այն չի ընդգրկում թվային իրավունքների ամբողջ շրջանակը և բաց է թողնում այնպիսի էական իրավունքներ, ինչպիսին է անձնական կյանքի անձեռնմխելիության իրավունքը: Այնուամենայնիվ, անարդարացի կլիներ ասել, որ Նախարարների կոմիտեն անտեսել կամ մոռացել է անձնական կյանքի անձեռնմխելիության իրավունքը: Եվրոպայի խորհուրդը մշտապես առաջատար դերակատարություն է ունեցել անձնական կյանքի չափորոշիչներն ու սկզբունքները խթանելու հարցում, իսկ 1981թ. բացել է անձնական տվյալների պաշտպանության մասին կոնվենցիան՝ հնարավորություն տալով անդամ-պետություններին ստորագրել այն: Եվրոպական միության առաջին փաստաթուղթը, որը նպատակ ուներ ներդաշնակեցնել անդամ-պետությունների օրենսդրությունը Եվրոպայի խորհրդի չափորոշիչների հետ, ընդունվեց միայն 14 տարի անց՝ 1995-ին:

«Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին Եվրոպայի խորհրդի կոնվենցիան» (Անձնական տվյալների պաշտպանության կոնվենցիա) մշակվել է այն ժամանակ, երբ թե՛ հանրային, թե՛ մասնավոր կազմակերպությունները առաջին քայլերն էին անում համակարգիչների օգտագործման ուղղությամբ՝ մեծացնելու գործառնությունների արդյունավետությունը: Այս գործողությունն առաջ մղող ուժը բիզնեսների և կառավարությունների կողմից հավաքված և մշակվող անձնական տվյալների մեծացող ծավալն

էր: Եվրոպայի խորհրդի կայքում այն նկարագրված է որպես «*իրավական պարտադիր ուժ ունեցող առաջին միջազգային գործիքը, որը պաշտպանում է անհատին այնպիսի չարաշահումներից, որոնք կարող են տեղ գտնել անձնական տվյալների հավաքման և մշակման գործընթացներին զուգահեռ, միևնույն ժամանակ ձգտում է կարգավորել անձնական տվյալների անդրսահմանային հոսքը*»:

Այն ժամանակ, երբ մշակվել էր «Անձնական տվյալների պաշտպանության կոնվենցիան», անձնական տվյալների հավաքման և մշակման հնարավոր չարաշահումը սահմանափակվել էր այնպիսի տվյալների չարաշահմամբ, որոնք կարող էին բացահայտել մարդկանց միջև կապերը, հարաբերությունները, նրանց սեփականությունը և հավելյալ այլ մասնավոր տեղեկություններ, և եթե արտահոսք լիներ, դրանք կարող էին դառնալ շանտաժի կամ խարդախության գործիք: Քաղաքական գործընթացներում անձնական տվյալների չարաշահումը եղել է Եվրոպայի խորհրդի փորձագետներին և քաղաքացիական հասարակությանը մտահոգող խնդիրներից մեկը: Անձնական տվյալների պաշտպանության ոլորտում տեխնոլոգիական սպառնալիքների վրա ավելի ու ավելի են սկսել կենտրոնանալ «Անձնական տվյալների պաշտպանության մասին կոնվենցիայի»՝ անդամ և անդամ չհանդիսացող պետությունների կողմից ստորագրումից ի վեր:

Եվրոպայի խորհրդի «Անձնական տվյալների պաշտպանության մասին կոնվենցիայի» արժեքավոր ներդրումներից մեկը առանցքային հասկացությունների և գաղափարների սահմանումն է, որոնք ավելի ուշ կիրառվել են տվյալների և անձնական կյանքի անձեռնմխելիության մասին գրեթե բոլոր քաղաքականություններում: Անձնական տվյալների հասկացությունը սահմանվել է որպես ցանկացած տեղեկություն, որը վերաբերում է նույնականացված կամ նույնականացվող անհատին: Հաջորդ սերնդի փաստաթղթերը, օրինակ՝ Եվրամիության 95/46/EC[4] դիրեկտիվը և ապա Ընդհանուր տվյալների պաշտպանության կանոնակարգը, գործածել են ավելի ընդարձակ սահմանում՝ տրամադրելով օրինակներ և ենթադրություններ: Այդուհանդերձ, տվյալ հասկացության էվոլյուցիան շատ կարևոր է, որովհետև այն արտացոլում է, թե ինչպես են տեխնոլոգիաներն ընդլայնում անձնական տվյալների շրջանակը:

Եվրոպայի խորհրդի կոնվենցիա	**Տվյալների պաշտպանության ԵՄ դիրեկտիվ**	**Ընդհանուր տվյալների պաշտպանության ԵՄ կանոնակարգ**
Ցանկացած տեղեկություն, որը վերաբերում է նույնականացված կամ նույնականացվող անհատին («տվյալների սուբյեկտ»):	Ցանկացած տեղեկություն, որը վերաբերում է նույնականացված կամ նույնականացվող ֆիզիկական անձին («տվյալների սուբյեկտ»), նույնականացվող անձը այն անհատն է, որը կարող է նույնականացվել՝ ուղղակիորեն կամ անուղղակիորեն, մասնավորապես՝ հղում անելով նույնականացման համարին կամ նրա ֆիզիկական, ֆիզիոլոգիական, մտավոր, տնտեսական, մշակութային կամ սոցիալական ինքնությունը հատկորոշող մեկ կամ մի քանի գործոններին:	Ցանկացած տեղեկություն, որը վերաբերում է նույնականացված կամ նույնականացվող ֆիզիկական անձին («տվյալների սուբյեկտ»), նույնականացվող ֆիզիկական անձն այն անհատն է, որը կարող է նույնականացվել՝ ուղղակիորեն կամ անուղղակիորեն, մասնավորապես՝ հղում անելով նույնականացնող այնպիսի տեղեկության, ինչպիսին են՝ անունը, նույնականացման համարը, գտնվելու մասին տվյալները, առցանց նույնացուցիչը կամ ֆիզիկական, ֆիզիոլոգիական, գենետիկ, մտավոր, տնտեսական, մշակութային կամ սոցիալական ինքնությունը հատկորոշող մեկ կամ մի քանի գործոնները:

Անձնական տվյալների պաշտպանության սահմանման էվոլյուցիան

[4] Եվրոպական խորհրդարանի և Խորհրդի 1995թ. հոկտեմբերի 24-ի՝ անձնական տվյալների մշակման դեպքում անհատների պաշտպանության և այդպիսի տվյալների ազատ տեղաշարժի մասին 95/46/EC դիրեկտիվը: Փոխարինվել է անձնական տվյալների մշակման դեպքում ֆիզիկական անձանց պաշտպանության և այդպիսի տվյալների ազատ տեղաշարժի մասին և 95/46/EC դիրեկտիվը չեղարկող կանոնակարգով (Ընդհանուր տվյալների պաշտպանության կանոնակարգ), որն ընդունվել է 2016թ. մայիսին և ուժի մեջ է մտել 2018թ. մայիսին:

Ինչպես տեսնում ենք այս աղյուսակում, անձնական տվյալներն ի սկզբանե սահմանվել են որպես տվյալների սուբյեկտին վերաբերող տեղեկատվություն: Տվյալների պաշտպանության մասին ԵՄ դիրեկտիվի սահմանումը նման է իր էությամբ, սակայն ներառում է մի շարք կոնկրետ տվյալներ, օրինակ՝ մտավոր, սոցիալական կամ մշակութային ինքնությունը, ինչպես նաև բազմագործոն նույնականացումը, որը մենք հիմա անվանում ենք պրոֆայլինգ (բնութագրի որոշարկում): Սահմանումը ներառում է նաև ֆիզիկական ինքնությունը, որն այլ կերպ կոչվում է կենսաչափական տվյալ:

Թեև կենսաչափական տվյալները 90-ականներին լայնորեն չէին օգտագործվում մարդկանց նույնականացնելու համար, դրանք հիշատակվում են որպես տեղեկատվություն, որը կարող է օգտագործվել մարդկանց նույնականացման համար: Սա անհատների անձնական կյանքի գաղտնիությանը սպառնացող հավանական վտանգի կանխատեսման փայլուն օրինակ է: Քսան տարի անց կենսաչափական տվյալները դարձան մարդկանց նույնականացնելու տարածված մեթոդ, և արդեն կային համապատասխան շտկող մոտեցումներ և մեխանիզմներ՝ այս մարտահրավերներին դիմակայելու համար: Մյուս տեխնոլոգիաները քաղաքականություն մշակողների և անձնական կյանքի գաղտնիության հարցերով զբաղվող փորձագետների ուշադրությանն են ներկայացնում ավելի մեծ թվով անհատների նույնականացման խնդիրը և արտացոլված են Ընդհանուր տվյալների պաշտպանության կանոնակարգում:

Արժե հիշատակել, որ համացանցում անձնական կյանքի անձեռնմխելիության վերաբերյալ Եվրոպայի խորհրդի առաջին փաստաթղթերից մեկը Համացանցում անձնական կյանքի պաշտպանության մասին Նախարարների կոմիտեի No R(99)5 հանձնարարականն էր: Այնուամենայնիվ, Հանձնարարականը սահմանափակվում է օգտատերերի և Համացանցային ծառայություններ մատուցողների համար ուղեցույցներով, որոնք վերաբերում են պատշաճ աշխատակարգերին, հավանական սպառնալիքներին և մասնավոր ու պետական հատվածների դերակատարների միջև համագործակցությանը:

Կարգավորումների նոր սերունդը (առաջին հերթին՝ Ընդհանուր տվյալների պաշտպանության կանոնակարգը) ներառում է ինքնությունը նույնականացնող տեղեկությունները, որոնք կապված են անհատների՝ համացանցում և ընդհանրապես հաղորդակցությունների տեխնոլոգիաներում վարքի հետ: Ավանդաբար մարդկանց նույնականացման համար օգտագործվող անձնական տեղեկություններին, օրինակ՝ կենսաչափական տվյալներին և պրոֆայլինգին, հավելվել է նույնականացման մեթոդների մի նոր դաս, որում ներառվում են տեղորոշման տվյալները և առցանց նույնացուցիչները: Անձնական տվյալների այս երկու կատեգորիաները վճռորոշ են դարձել համացանցային ծառայությունների և համացանցի օգտատերերի՝ տեղադրության վրա հիմնված պրոֆայլինգի ավելի ու ավելի մեծացող դերի շնորհիվ:

Անհատների վարքին հետևելու և նրանց պրոֆայլինգի՝ տեխնոլոգիաներով պայմանավորված հավանական սպառնալիքների մասին խոսելիս մենք պետք է հիշատակենք Թվային վարքի հետագծելիությունից և հսկողության այլ տեխնոլոգիաներից բխող հիմնարար իրավունքներին սպառնացող ռիսկերի մասին Նախարարների կոմիտեի ևս մի հռչակագիր (Թվային հետագծելիության ռիսկերի հռչակագիրը, որն ընդունվել է 2013թ. հունիսի 11-ին՝ փոխնախարարների 1173-րդ հանդիպմանը): Հռչակագիրը սկսվում է հետևյալ նախադասությամբ. «Անձնական կյանքի անձեռնմխելիության իրավունքին միջամտելու հակվածությունն էականորեն մեծացել է արագընթաց տեխնոլոգիական զարգացումների և իրավական շրջանակների՝ դրանց դանդաղ հարմարվելու արդյունքում»:

Նախարարների կոմիտեի հռչակագրերն իրավական պարտադիր ուժ ունեցող փաստաթղթեր չեն: Դրանց սովորաբար ներկայացրած սկզբունքները համաձայնեցված քաղաքականության ուղեցույցներ են, ոչ թե ստորագրյալ յուրաքանչյուր անդամ-պետության պարտավորություն: Այնուամենայնիվ, նույնիսկ այս տիպի փաստաթղթերը կարող են համարվել իրավունքի աղբյուր, հատկապես եթե կոնկրետ հայց է ներկայացվում Մարդու իրավունքների եվրոպական դատարան: Թվային հետագծելիության ռիսկերի մասին հայտարարությունը վերաբերում է մասնավոր և ընտանեկան կյանքի անձեռնմխելիության իրավունքներին (Մարդու իրավունքների եվրոպական կոնվենցիայի 8-րդ հոդված) և Մարդու իրավունքների եվրոպական դատարանի համապատասխան նախադեպային իրավունքին:

Թվային հետագծելիության ռիսկերի մասին հռչակագիրը շեշտում է, որ Մարդու իրավունքների եվրոպական կոնվենցիայի 8-րդ հոդվածի և ՄԻԵԴ նախադեպային իրավունքի համաձայն, պետություններն ունեն բացասական պարտավորություններ, այն է՝ զերծ մնալ հիմնարար իրավունքներին միջամտելուց, և դրական պարտավորություններ, այն է՝ ակտիվորեն պաշտպանել այդ իրավունքները: Այլ կերպ ասած՝ պետություններն ունեն բացասական պարտավորություններ՝ սահմանափակվել անհատների անձնական կյանքին օրենքով սահմանված և ժողովրդավարական հասարակությունում հանրային շահի պաշտպանության համար անհրաժեշտ միջամտության դեպքերով: Ինչպես և հանուն հանրային շահի պաշտպանության պետության միջամտության ցանկացած դեպքում, միջոցառումները պետք է լինեն համարժեք և ոչ անհարկի խիստ: Պետությունները նաև դրական պարտավորություններ ունեն՝ պաշտպանել անհատների մասնավոր կյանքը այլոց անօրինական միջամտությունից, ներառելով, սակայն չսահմանափակվելով մասնավոր ընկերություններով և այլ հանրային դերակատարներով:

Կարևոր է նկատի ունենալ այն, որ Թվային հետագծելիության ռիսկերի մասին հռչակագիրը կոչ չի անում ամբողջովին արգելել հետևող տեխնոլոգիաները: Անկասկած, հետագծող սարքերը, հավելվածները և դրանց առանձնահատկությունները կարող են ծառայել օրինական նպատակների և օգուտ բերել հանրությանը: Տեղորոշմամբ հետագծելիության տեխնիկական հնարավորությունները և օգտատերերի պրոֆիլները օգնում են ընկերություններին բարելավել ծառայությունների որակը և այդ ծառայություններն ավելի անվտանգ դարձնել: Պետական մարմինները կարող են օգտագործել թվային հետագծումը՝ տրամադրելու ավելի լավ ծառայություններ, փրկելու մարդկանց կամ կանխելու և պայքարելու հանցավորության դեմ:

Մյուս կողմից, շարժական սարքերում և դրանց հավելվածներում ներկառուցված թվային հետագծելիության տեխնիկական հնարավորությունները կարող են օգտագործվել նաև անօրինական նպատակներով: Այսպիսի տեխնիկական հնարավորությունների չարաշահումը կարող է հանգեցնել անօրինական հասանելիության, տվյալների գաղտնալսման և միջամտության, համակարգի հսկողության և սարքերի չարաշահման, կամ հակաօրինական գործողությունների այլ տեսակների ու ձևերի: Օրինակ՝ տեղորոշման հետագծելիությունը կարող է օգտագործվել անձի տիպիկ վարքը որոշարկելու և նրան հարձակումների դիմաց ավելի խոցելի դարձնելու համար: Պրոֆայլինգը կարող է կիրառվել սոցիալական ցանցերի օգտատերերի միկրոթիրախավորման և սպամ-ուղերձներ հղելու համար:

Հետևյալ 6 պարբերությունը Թվային հետագծելիության ռիսկերի մասին հռչակագրի տեքստի վերջին մասն է.

- Անդամ պետություններին զգուշացնում է մարդու իրավունքների, ժողովրդավարության և օրենքի գերակայության համար թվային հետագծելիության ու հսկողության այլ տեխնոլոգիաների ռիսկերի մասին և հիշեցնում է դրանց օրինական օգտագործումն ապահովելու անհրաժեշտությունը, ի նպաստ անհատների, տնտեսության, հասարակության և իրավապահ մարմինների կարիքների:

- Քաջալերում է անդամ պետություններին՝ հաշվի առնել այդ ռիսկերը երրորդ երկրների հետ երկկողմ քննարկումներում և, անհրաժեշտության դեպքում, դիտարկել արտահանման համար պատշաճ հսկողության ներդրումը՝ այդ չափորոշիչները խաթարելու նպատակով տեխնոլոգիայի անօրինական օգտագործումը կանխելու համար:

- Ողջունում է որոշ անդամ-պետությունների տվյալների պաշտպանության մարմինների՝ No 108 կոնվենցիայի դրույթներին և դրանց ազգային օրենսդրությանը համապատասխանությունը ապահովելու համար հետևող և վերահսկող տեխնոլոգիաների հետևանքների մասին իրազեկությունը բարձրացնելուն և այդ գործելակերպը ուսումնասիրելուն ուղղված քայլերը:

- Ուշադրություն է հրավիրում կիբերտարածքում անօրինական վերահսկողության և հետևելու՝ քրեական օրենսդրությամբ սահմանվող հետևանքներին և կիբերհանցագործությունների դեմ պայքարում Բուդապեշտի կոնվենցիայի կարևորությանը:

- Ողջունում է ինչպես պետական, այնպես էլ ոչ պետական դերակատարների կողմից ձեռնարկատերերի և, առավել ևս, մասնավոր հատվածում ու տեխնոլոգիա մշակողների շրջանում իրազեկությունը բարձրացնելու ուղղությամբ ձեռնարկված միջոցառումները՝ մարդու իրավունքների վրա այդպիսի տեխնոլոգիաների օգտագործման հնարավոր ազդեցության, ինչպես նաև հնարավոր այն քայլերի վերաբերյալ, որոնք կարելի է ձեռնարկել նախագծման փուլում՝ այդ իրավունքներին և ազատություններին միջամտելու ռիսկերը նվազագույնի հասցնելու համար (օրինակ՝ «գաղտնիության ապահովում ըստ նախագծման» և «գաղտնիության ապահովում նախակարգավորմամբ»):

- Հիշեցնում է Եվրոպայի խորհրդի՝ Համացանցի կառավարման 2012-2015 թվականների ռազմավարությունը, որը ներառում է սույն Հռչակագրում նշված մարտահրավերներին առնչվող գործողությունների մի շարք ուղղություններ, և ակնկալում է Եվրոպայի խորհրդի իրավասու մարմինների աշխատանքի կոնկրետ արդյունքներ:

Ի տարբերություն Նախարարների կոմիտեի՝ Համացանցում հաղորդակցության ազատության մասին հռչակագրի, այս հռչակագիրը չի սահմանում ներպետական օրենսդրությունն ընդունելիս կամ վերանայելիս անդամ-պետությունների համար որևէ հատուկ և պարտադիր սկզբունք: Օգտակարության տեսանկյունից այն շատ ավելի թույլ է, քան Նախարարների կոմիտեի՝ համացանցի ազատության, կառավարման կամ համացանցին առնչվող որևէ այլ կոնկրետ թեմայի առնչվող մյուս հռչակագրերը: Այնուամենայնիվ, այստեղ նույնպես հնարավոր է գտնել մի շարք օգտակար արդյունքներ:

Գաղտնիության ապահովում նախագծման շնորհիվ

Հիմնական դրական արդյունքը «գաղտնիության ապահովում ըստ նախագծման» և «գաղտնիության ապահովում նախակարգավորմամբ» սկզբունքի ընդունումն է որպես չափորոշիչ, որին պետք է հետևի տվյալ ոլորտը, իսկ պետությունները պետք է առնվազն քաջալերեն ոլորտին՝ ենթարկվելու այդ չափորոշիչներին: Այս սկզբունքները Նախարարների կոմիտեի կողմից նոր հորինված կամ ձևակերպված բաներ չեն: Արդեն մի քանի տարի է, ինչ «գաղտնիության ապահովում ըստ նախագծման» և «գաղտնիության ապահովում նախակարգավորմամբ» սկզբունքները հայտնի են SS ոլորտում:

«Գաղտնիության ապահովում ըստ նախագծման» սկզբունքը ձևակերպել է *Անն Չավուքյանը,* կանադացի իրավաբան և Օնտարիոյի՝ Տվյալների գաղտնիության նախկին հանձնակատարը: Այս սկզբունքը դարձել է չափորոշիչ և ներդրվել է տվյալների գաղտնիության բազմաթիվ փաստաթղթերում, այդ թվում՝ Եվրամիության Ընդհանուր տվյալների պաշտպանության կանոնադրությունում: Այս սկզբունքը շատ կարևոր է և հարկ է այն մանրակրկիտ բացատրել: «Գաղտնիության ապահովում ըստ նախագծման» սկզբունքը ներառում է 7 հիմնական կանոն.

- Պրոակտիվ, ոչ թե ռեակտիվ. կանխարգելիչ, ոչ թե վերականգնող,

- Գաղտնիությունը՝ որպես լռելյայն կարգավորում,

- Ներկառուցված գաղտնիություն,

- Լիարժեք ֆունկցիոնալություն՝ ոչ թե զրոյական, այլ դրական ելք,

- Սկզբից մինչև վերջ (end-to-end) անվտանգություն. պաշտպանություն ամբողջ կենսափուլի ընթացքում,

- Տեսանելիություն և թափանցիկություն. ապահովվում է բաց լինելը,

- Օգտատերերի անձնական կյանքի անձեռնմխելիությունը. ապահովվում է օգտատերերին միտված և նրանց վրա կենտրոնացված լինելու հանգամանքը:

Առաջին կանոնը նշանակում է, որ անհրաժեշտ է անձնական կյանքի անձեռնմխելիության պաշտպանության միջոցներ ձեռնարկել նախքան օգտատերերի անձնական կյանքի գաղտնիության վտանգումը: Հարկ է նկատի ունենալ, որ այս կանոնը վերաբերում է ոչ միայն սարքի կառուցվածքին կամ ծրագրին, այլ նաև գաղտնիությունն ապահովող ընթացակարգերին և քաղաքականություններին: Որպես առհասարակ գաղտնիությանը վերաբերող կանոն՝ այն նաև պետք է կիրառվի բիզնես գործընթացների նախագծման համար:

Գաղտնիությունը լռելյայն կանոնը նաև համընդհանուր չափորոշիչ է և պետք է կիրառելի լինի թե՛ գործընթացների, թե՛ պրոդուկտների նկատմամբ: Այս կանոնի հիմքում ընկած գաղափարն այն է, որ ցանկացած գործընթաց կամ պրոդուկտ պետք է նախագծվի և իրականացվի՝ ապահովելով գաղտնիության առավելագույն պաշտպանությունը առավելագույն կարգավորումներով: Դրանք կարելի է հարմարեցնել նվազ պաշտպանվածների նկատմամբ՝ ըստ օգտատերերի ցանկության: Անձնական կյանքի անձեռնմխելիության պաշտպանությունը չպետք է բեռ լինի համակարգից կամ սարքից օգտվողի համար:

Ներկառուցված գաղտնիությունը մեկ այլ կարևոր կանոն է, ըստ որի՝ գաղտնիության ապահովումը պետք է լինի պրոդուկտի մշակման նպատակներից մեկը: Այն պետք է պլանավորվի և ստուգվի նախագծի մշակման և փորձարկման յուրաքանչյուր փուլում: Գաղտնիության ապահովման գործիքները չպետք է ավելացվեն այն ժամանակ, երբ համակարգի նախագիծն արդեն ավարտված է:

Լիարժեք ֆունկցիոնալություն կամ ոչ թե զրոյական, այլ դրական ելքի կանոնը նշանակում է, որ գաղտնիության առավելագույն աստիճանը չի ապահովվի այլ ֆունկցիոնալությունները, օրինակ՝ պրոդուկտի օգտագործելիությունը կամ հուսալիությունը թուլացնելու շնորհիվ: Հատկապես անընդունելի է համակարգի անվտանգության հաշվին գաղտնիության պատշաճ մակարդակի ապահովումը: Թեև որոշ դեպքերում դա կարող է բարդ լինել, համակարգը նախագծողները պետք է աշխատեն բոլորի համար դրական արդյունք ապահովել:

Սկզբից մինչև վերջ անվտանգություն. պաշտպանություն ամբողջ կենսափուլի ընթացքում. սա հայտնի կանոն է, որը լայնորեն կիրառվում է համակարգի անվտանգության մոդելում: Դա կարող է համարվել «գաղտնիության ապահովում ըստ նախագծման» կանոնի այնպիսի տրամաբանական շարունակությունը, որն ընդգրկում է պրոդուկտի կամ համակարգի ամբողջական կենսափուլը: Սա նշանակում է, որ գաղտնիության պաշտպանությունը պետք է ապահովվի պրոդուկտի կամ համակարգի ամբողջ կենսափուլի ընթացքում, այդ թվում:

Տեսանելիություն և թափանցիկություն. ապահովվում է բաց լինելը: Այս կանոնի ներքո ենթադրվում է գաղտնիության ապահովման մոդելի կիրառում՝ հիմնվելով բաց աղբյուրից օգտվելու փիլիսոփայության վրա: Համակարգը բաց պահելու նպատակը ոչ միայն վստահության նպատակ է հետապնդում, թեև համակարգին վստահելու տարրը նույնպես կարևոր է: Ի տարբերություն փակ կամ սեփականություն հանդիսացող (proprietary) մոդելների՝ բաց մոդելն օգնում է նախագծողներին և ճարտարապետներին հետադարձ կապ ստանալ մասնագիտական համայնքից և իրազեկ լինել անվտանգությունը և օգտատերերի կյանքի գաղտնիությունը հավանաբար վտանգող թերությունների և սխալների մասին:

Եվ վերջին, սակայն ոչ պակաս կարևոր կանոնը **Օգտատերերի անձնական կյանքի անձեռնմխելիության և օգտատերերի վրա կենտրոնացած լինելու** կանոնն է: Օգտատերերի վրա կենտրոնացող մոտեցումը կարևոր է ցանկացած պրոդուկտ և ծառայություն նախագծելու համար: Սովորաբար սա նշանակում է, որ պրոդուկտը պետք է ձևավորվի օգտատերերի կարիքներին ավելի արդյունավետ կերպով արձագանքելու և դրանք բավարարելու համար: Այստեղ կարող են ներառվել գաղտնիության կարգավորումների հեշտ կառավարումը, գաղտնիության մակարդակի բնազդային ընկալումը և գաղտնիության հնարավոր ռիսկերի մասին իրազեկությունը. այս թվարկումը, սակայն, սպառիչ չէ: Օրինակ՝ օգտատերը կարող է ցանկանալ ակտիվացնել տեղորոշման ծառայությունը: Համակարգը նրան պետք է իրազեկի գաղտնիության հավանական ռիսկերի մասին և հնարավորություն տա միացնել և անջատել ծառայությունն ինտուիտիվ, հեշտ կարգավորվող գործիքներով:

Իհարկե, վերը նկարագրված սկզբունքները և կանոնները Եվրոպայի խորհրդի անդամ-պետությունների համար սահմանված պարտավորություններ չեն: Իդեալական դեպքում պետական իշխանությունները պետք է նկատի առնեն «գաղտնիություն ըստ կառուցվածքի» սկզբունքը՝ էլեկտրոնային կառավարման և էլեկտրոնային փաստաթղթավորման համակարգի մշակման համար: Պետական իշխանությունները կարող են նաև աշխատել մասնավոր ընկերությունների և մասնագիտական ասոցիացիաների հետ՝ այս սկզբունքներն ամրապնդելու և տարածելու նպատակով: Այնուամենայնիվ, դժվար է պատկերացնել, որ «գաղտնիությունը լռելյայն» սկզբունքը կընդունվի որպես իրավական պարտադիր ուժ ունեցող պարտավորություն կամ որպես հասարակական կազմակերպությունների և անհատների համար չափորոշիչ:

Թվային հետագծելիության ռիսկերի մասին Նախարարների կոմիտեի հռչակագրի այլ արժանահիշատակ արդյունքները քաջալերում են անդամ-պետություններին՝ բանակցել այլ երկրների (ոչ անդամ պետությունների) հետ երկկողմ պայմանագրերի շրջանակում՝ ներմուծելու փորձագիտական հսկողության այնպիսի ձևեր, որոնք կարող են օգնել կանխելու Եվրոպայի խորհրդի՝ գաղտնիության մասին չափորոշիչի ապօրինի կիրառման կամ խաթարման ներուժ ունեցող տեխնոլոգիաների առևտուրը:

Թվային հետագծելիության ռիսկերի մասին Նախարարների կոմիտեի հռչակագրի ոչ պակաս կարևոր արդյունքներից է այն հանգամանքը, որ անդամ-պետություններին կոչ է արվում ուշադրության առնել հավանական վտանգների թվային հետագծելիության հնարավորությունները՝ հատկապես հանցագործությունների հետաքննության նպատակով: Նախարարների կոմիտեն հղում է անում Եվրոպայի խորհրդի Կիբերհանցագործությունների մասին կոնվենցիային՝ որպես օգտատերերի անձնական կյանքի անձեռնմխելիության չափորոշչի: Հանցագործությունների հետաքննության ոլորտում գաղտնիության խնդիրը, որը կիբերիրավագիտության ոլորտի ամենախնդրահարույց կետերից մեկն է, նորից կքննարկվի այս փաստաթղթում և տարբեր համատեքստերում:

Եվրոպայի խորհուրդը վստահաբար խթանող դեր է խաղացել նոր սերնդի մարդու իրավունքների, այսպես կոչված՝ «թվային իրավունքների» համար հիմքերի ստեղծման գործում: Տվյալների պաշտպանության կոնվենցիայից, Համացանցում հաղորդակցության ազատության հռչակագրից և Թվային հետագծելիության ռիսկերի մասին հռչակագրից բացի, Եվրոպայի խորհուրդն ընդունել է համացանցի կառավարմանը, դոմենային անվանման կառավարմանը վերաբերող և այլ փաստաթղթեր, որոնք այստեղ չեն քննարկվում, քանի որ ուղղակիորեն կապված չեն հիմնական թեմայի՝ թվային իրավունքների հետ:

Ինքնապաշտպանությունը թույլատրվո՞ւմ է

Թվային գաղտնիության հասկացությունը կարելի է սահմանել վերը նշված վերլուծության հիման վրա: Այն անպայմանորեն հիմնված է Մարդու իրավունքների եվրոպական կոնվենցիայի 8-րդ հոդվածով և Եվրոպայի խորհրդի մի շարք այլ փաստաթղթերով պաշտպանվող անձնական կյանքի անձեռնմխելիության հասկացության վրա: Թվային գաղտնիությունը կարող է դիտարկվել որպես թվային միջավայրում մասնավոր և ընտանեկան կյանքի վրա ազդեցություն ունեցող հանգամանք: Ինչպես արդեն հիշատակվել է, պետական իշխանությունները բացասական պարտավորություն ունեն՝ ձեռնպահ մնալ համացանցի օգտատերերի անձնական կյանքին միջամտելուց, և դրական պարտավորություններ ունեն՝ պաշտպանել նրանց անցանկալի միջամտությունից և երրորդ անձանց կողմից անհատների անձնական տվյալների չարաշահումներից: Միևնույն ժամանակ, արժանահիշատակ է նաև մեր օրերում ակտիվ բանավեճերի թեմա դարձած՝ օգտատերերի ինքնապաշտպանության իրավաչափությունը:

Իր կառուցվածքով և տրամաբանությամբ՝ համացանցը բաց հաղորդակցության մոդել է, որը հնարավորություն է տալիս վերջնական օգտատերերին, կորպորատիվ և հանրային դերակատարներին՝ գործածել ինքնության, անանունության, գաղտնիության պաշտպանության և հաղորդակցության գաղտնիության տարբեր գործիքները: Մի կողմից, սա օգնում է համացանցի օգտատերերին պաշտպանել իրենց անձնական կյանքը և անանունությունը՝ անկախ ծառայություն մատուցողների կողմից առաջարկվող ծառայության տեսակից: Մյուս կողմից,

համացանցի բաց մոդելը նրանց խոցելի է դարձնում անանուն հակառակորդների համար: Այս համատեքստում, պետական իշխանությունները նաև բացասական պարտավորություն ունեն՝ չսահմանափակել անհատների ինքնապաշտպանության իրավունքները, և ունեն դրական պարտավորություն՝ պաշտպանել օգտատերերին հակառակորդներից, մանիպուլյատորներից և խարդախներից:

Պետական իշխանությունների բացասական պարտավորությունների համատեքստում հարկ է հիշատակել անհատների թվային իրավունքների պաշտպանության հետ կապված մի կարևոր մոտեցում: Ինչպես ավանդական ընկալմամբ անձնական կյանքի անձեռնմխելիության պաշտպանության դեպքում, այստեղ նույնպես անհատները պետք է ունենան թվային մասնավոր կյանքը ինքնուրույնաբար պաշտպանելու իրավունք: Առավել լայն կիրառություն ունեցող թվային գաղտնիության պաշտպանության գործիքներից մեկը վիրտուալ մասնավոր ցանցն (VPN) է՝ իր տարատեսակներով: Այս համատեքստում, պետությունների բացասական պարտավորությունը պետք է լինի VPN-ների և գաղտնիությունը պաշտպանող այլ գործիքների կիրառության սահմանափակումներից զերծ մնալը:

VPN-ը գաղտնիությունը պաշտպանող մեխանիզմ է, որը որոշ չափով պաշտպանում է համացանցի օգտատերերին միջանկյալ հարձակումներից և ցանցային որոնումների ժամանակ հարցումների՝ տեղական մակարդակում, այսինքն՝ ծառայությունը մատուցողների կողմից, գաղտնալսումից: Անձնական կյանքի ավելի ուժեղ պաշտպանություն և հաղորդակցական ծառայությունների գաղտնիություն կարելի է ձեռք բերել գաղտնագրման՝ կրիպտոգրաֆիայի միջոցով: Կրիպտոգրաֆիան թաքցնում է հաղորդակցության բովանդակությունը, այսինքն՝ ապահովում է ուղերձների գաղտնիությունը, սակայն ամբողջովին չի թաքցնում օգտատերերի ինքնությունը: Ի վերջո, VPN-ի ու կրիպտոգրաֆիայի համադրությունը և վերադիր ցանցի ճարտարապետությունը (overlay network architecture) ապահովում են գաղտնիության և անանունության էական մակարդակ:

Բոլոր տեխնոլոգիաները կարող են կիրառվել օգտատերերի կողմից գրեթե ցանկացած եվրոպական երկրում, Հյուսիսային և Հարավային Ամերիկաներում և Ասիայի երկրների մեծ մասում՝ որոշ բացառություններով, ինչպես, օրինակ՝ Չինաստանը, Սիրիան, Իրանը, Պակիստանը, և մասամբ՝ Ռուսաստանում ու Թուրքիայում: Հարկ է նկատել, որ Ռուսաստանը և Թուրքիան անդամակցում են Եվրոպայի խորհրդին, որը հատուկ անդրադառնում է գաղտնիության պաշտպանության համար VPN օգտագործելու իրավունքին Որոնողական համակարգերի կիրառման ժամանակ մարդու իրավունքների պաշտպանության մասին Նախարարների կոմիտեի Rec(2012)3 հանձնարարականում: Սա թվային գաղտնիության պաշտպանության ոլորտում պետությունների թե՛ դրական, թե՛ բացասական պարտավորությունների վերաբերյալ ևս մեկ կարևոր փաստաթուղթ է:

Գաղտնիությունը թափանցիկ աշխարհում

Rec(2012)3 հանձնարարականը փորձ է՝ արձագանքել որոնողական համակարգերի հետ կապված մտահոգություններին: Մասնավորապես, այն վերաբերում է այնպիսի հավանական սպառնալիքներին, ինչպիսին են որոնման արդյունքների ընտրողական ոչ թափանցիկ ցուցակները, մի կողմից՝ լռելյայն բացահայտ և հակասական բովանդակության ցուցակման, մյուս կողմից՝ ոչ թափանցիկ զտման ռիսկերով: Գաղտնիության իրավունքների ապահովումը Որոնողական համակարգերի մասին հանձնարարականի առանցքային կետերից է. այս փաստաթուղթն անդամ պետություններին տալիս է իրավիճակի բարելավման ցուցումներ:

Ավելի կոնկրետ՝ Որոնողական համակարգերի մասին հանձնարարականը անդամ-պետություններին կոչ է անում ապահովել համապատասխանությունը տվյալների պաշտպանության սկզբունքներին և ձեռնարկել հետևյալ գործողությունները.

- Համոզվել, որ որոնողական համակարգերի օպերատորների կողմից անձնական տվյալների հավաքումը նվազագույնի է հասցված: Ոչ մի օգտատիրոջ IP հասցե չպետք է պահպանվի, եթե դա անհրաժեշտ չէ օրինական նպատակի հետապնդման համատեքստում և եթե այդ

նույն արդյունքներին կարելի է հասնել ընտրանքի մոդելավորման, սոցիոլոգիական հարցման կամ անձնական տվյալների անվանազերծման միջոցով: Հարկ է քաջալերել անանուն որոնումները խթանող նորարարական մոտեցումները:

- Համոզվել, որ չեն գերազանցվում տվյալների օրինական մշակման և կոնկրետ նպատակներով պահպանման խիստ անհրաժեշտ ժամկետները: Որոնողական համակարգերի օպերատորները պետք է կարողանան բացահայտ և հստակ պատճառաբանություններով արդարացնել անձնական տվյալների հավաքումն ու պահպանումը: Այսպիսի հիմնավորումները պետք է հասարակության համար մատչելի և հեշտ հասանելի լինեն:

- Համոզվել, որ որոնողական համակարգերի օպերատորները կիրառում են անվտանգության ապահովման առավել համապատասխան միջոցներ՝ անձնական տվյալները երրորդ անձանց անօրինական մուտքից պաշտպանելու նպատակով, ինչպես նաև ապահովել տվյալների հետ կապված խախտումների մասին համապատասխան ծանուցման սխեմաների առկայությունը: Միջոցառումների շարքում կարելի է ներառել օգտատիրոջ և որոնողական համակարգերի օպերատորների միջև հաղորդակցության «սկզբից մինչև վերջ» (end-to-end) գաղտնագրումը:

- Ապահովել անհատների իրազեկվածությունը իրենց անձնական տվյալների մշակման և իրենց իրավունքների իրացման հնարավորությունների մասին նրանց համար հասկանալի ձևով՝ օգտագործելով պարզ և հստակ լեզու՝ տվյալների սուբյեկտի լեզվական կարիքներին ու կրթական մակարդակին համապատասխան: Որոնողական համակարգերի օպերատորները պետք է ի սկզբանե հստակ իրազեկեն օգտատերերին նրանց տվյալների օգտագործման բոլոր նախատեսված ձևերի մասին (շեշտելով, որ այսպիսի մշակման սկզբնական նպատակն է ավելի լավ արձագանքել նրանց որոնումներին) և հարգեն օգտատերերի՝ անձնական տվյալների հետ կապված իրավունքները: Նրանք պետք է անհատներին տեղեկացնեն նրանց անձնական տվյալների նկատմամբ ոտնձգությունների դեպքերի մասին:

- Ապահովել որոնողական համակարգերի օպերատորներին պատկանող տարբեր ծառայություններից/հարթակներից ստացվող տվյալների խաչաձև կորելյացիաները բացառապես այն դեպքերում, երբ կոնկրետ ծառայության համար օգտատերը տվել է իր միանշանակ համաձայնությունը: Նույնը վերաբերելի է օգտատիրոջ պրոֆիլի լրամշակման դեպքերին, ինչպես նշվում է նաև անհատների պաշտպանության մասին CM(2010)13 հանձնարարականում՝ պրոֆայլինգի համատեքստում անձնական տվյալների ավտոմատացված մշակմանն անդրադառնալիս:

Հավանաբար տարօրինակ է տեսնել, որ Նախարարների կոմիտեն բոլոր այս միջոցառումները խորհուրդ է տալիս ընդունել այն պետություններին, որոնք գուցե չունեն համապատասխան իրավական գործիք՝ դրանք որոնողական համակարգերի օպերատորների նկատմամբ կիրառելու համար: Այնուամենայնիվ, շատ դեպքերում, ավելի խոշոր պետությունների կողմից այսպիսի միջոցառումների ձեռնարկումը նպաստավոր է ավելի փոքր պետությունների համար, իսկ միասնական մոտեցումը կարևոր է այս սկզբունքի կիրարկման օրինականության համար:

Չնայած Rec(2010)3 հանձնարարականներն ընդունվել են որոնողական համակարգերի վերաբերմամբ, շատ սկզբունքներ կարող են համընդհանուր լինել և վերաբերելի են համակարգչային հավելվածներին ու համակարգերին: Այստեղ կրկին բախվում ենք հարցին, թե համատեղ կարգավորումը որտեղ կարող է կարևոր դեր խաղալ: Շատ դեպքերում, խիստ կարգավորումները կարող են վնասել տեխնոլոգիաներին և ծրագրային ապահովմանը վերաբերող կարգավորումների, այդ թվում՝(համատեղ կարգավորումների մշակումը, իսկ ոլորտի ինքնակարգավորումը կարող էր շատ ավելի արդյունավետ լինել: Այնուամենայնիվ, կառավարությունները կարող են բարձր չափորոշիչն առաջ մղողների դեր խաղալ՝ սեփական պրոդուկտները և ծառայությունները մշակելիս, տեղեկատվական տեխնոլոգիական պրոդուկտներն արտապատվիրելիս կամ ձեռք բերելիս:

Ավելի խիստ կանոններ են ուրվագծվում Եվրոպայի խորհրդի մեկ այլ փաստաթղթում՝ Նախարարների կոմիտեի՝ Սոցիալական ցանցային ծառայությունների պարագայում Մարդու իրավունքների պաշտպանության մասին անդամ-պետություններին ուղղված CM/Rec(2012)4 հանձնարարականում (Սոցիալական ցանցերի ծառայություններում մարդու իրավունքների մասին հանձնարարական).

- Տրամադրել սոցիալական ցանցերի օգտատերերի համար այնպիսի միջավայր, որը թույլ է տալիս նրանց շարունակել իրենց իրավունքների և ազատությունների իրացումը:

- Հստակ և հասկանալի լեզվով բարձրացնել օգտատերերի իրազեկությունը մարդու իրավունքներին հնարավոր մարտահրավերների և այն եղանակների մասին, որոնցով այս ծառայություններից օգտվելիս հնարավոր է խուսափել այլոց իրավունքների վրա բացասական ազդեցությունից:

- Պաշտպանել օգտատերերին՝ առանց նրանց արտահայտվելու ազատությունը և տեղեկատվության հասանելիությունը սահմանափակելու:

- Խթանել տեղեկատվության մշակման մասին թափանցիկությունը և զերծ մնալ անձնական տվյալների անօրինական մշակումից:

- Կազմել ինքնակարգավորման և համատեղ կարգավորման մեխանիզմներ ըստ անհրաժեշտության՝ նպաստելու այս հանձնարարականի Հավելվածում ուրվագծված նպատակներին:

- Ապահովել հաշմանդամություն ունեցող անձանց համար ծառայությունների հասանելիությունը՝ այդկերպ խթանելով հասարակությանը նրանց ինտեգրումը և լիարժեք մասնակցությունը:

Ինչպես կարող ենք տեսնել Սոցիալական ցանցերի ծառայություններում մարդու իրավունքների մասին հանձնարարականում, գաղտնիությունը հավանական ռիսկերից մեկն է, որոնց կարող են բախվել օգտատերերը սոցիալական ցանցերի օգտագործման ընթացքում:

Թե՛ որոնման համակարգերը, թե՛ սոցիալական ցանցային հարթակները քաջալերում են հավաքել անձնական տվյալների նվազագույն ծավալը, և նույնիսկ երբ օգտատերերը համօգտագործում են այսպիսի տվյալները կամավոր կերպով, ծառայություն մատուցողը/սեփականատերը պետք է կիրառի համապատասխան միջոցառումներ անձնական տվյալների պաշտպանության համար: Մեկ այլ պահանջ է թափանցիկ կերպով անձնական տվյալների մշակումը: Ընդհանուր առմամբ, բիզնես գործընթացների և ալգորիթմների թափանցիկությունը դարձել է տվյալների պաշտպանության համապատասխանության հիմնական ցուցիչներից մեկը:

Սոցիալական ցանցերի ծառայություններում մարդու իրավունքների մասին հանձնարարականում թվարկված չափորոշիչները կարող են ուղղակիորեն կիրառվել անձնական տվյալները մշակող համակարգչային հավելվածների բոլոր տեսակների նկատմամբ: Այստեղ մենք ավելի ուշ ցույց ենք տալու՝ ինչպես են թափանցիկ կանոնները կիրառվում մեկ այլ զարգացում ապրող SS հատվածում՝ արհեստական բանականության ոլորտում: Թե՛ սոցիալական ցանցը, թե՛ արհեստական բանականությունը SS այնպիսի ոլորտներ են, որտեղ անձնական տվյալներ են մշակվում միկրոթիրախավորման մարքեթինգային գործունեության, ուստի և՝ օգտատիրոջ պրոֆայլինգի համար:

Պրոֆայլինգը ինքնության նոր տեսակ է

Պրոֆայլինգի մասին խոսելիս հարկ է հիշատակել Եվրոպայի խորհրդի Նախարարների կոմիտեի մեկ այլ՝ Պրոֆայլինգի համատեքստում անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին CM/Rec(2010)13 հանձնարարականը (Անհատների պրոֆայլինգի մասին հանձնարարականը): Փաստորեն, Տվյալների պաշտպանության

մասին կոնվենցիայի կիրառման վերաբերյալ բացատրական փաստաթուղթ լինելով՝ CM/Rec(2010)13 հանձնարարականը սահմանում է պրոֆայլինգի գործընթացների վերաբերյալ անդամ-պետությունների ու մշակողների համար պարտադիր կոնկրետ կանոններ:

Չկա Անհատների պրոֆայլինգի մասին հանձնարարականն այստեղ ներկայացնելու անհրաժեշտություն, քանի որ այս հատուկ համատեքստում այդ փաստաթուղթը Տվյալների պաշտպանության կոնվենցիայի մեկնաբանություն է: Այդուհանդերձ, արժե ուրվագծել օրինական մշակման հիմնական սահմանումները և սկզբունքները: Պրոֆայլինգի սահմանումը կարևոր է, քանի որ այն հաճախ օգտագործվող սկզբունք է: CM/Rec(2010)13 հանձնարարականը սահմանում է այն որպես «տվյալների ավտոմատացված մշակման մեթոդ, որը բաղկացած է անհատի «պրոֆիլի» կիրառումից, մասնավորապես՝ նրան վերաբերող որոշումների կայացման կամ նրա անձնական նախընտրությունները, վարքը և վերաբերմունքը կանխատեսելու համար»:

Ինչո՞ւ են Նախարարների կոմիտեն և Եվրոպայի խորհրդի փորձագետներն արձագանքում պրոֆայլինգի ռիսկերին և ինչո՞ւ են այս հարցի վերաբերյալ մշակել կոնկրետ հանձնարարականներ: Բացատրությունը պարզ է և բարդ միևնույն ժամանակ: Պրոֆայլինգը որպես նոր կոնկրետ կատեգորիա և գաղտնիության ռիսկ է դիտարկվում հիմնականում նոր անձնական տվյալների (պրոֆիլի) ստեղծման պատճառով, որը, կախված պրոֆայլինգի նպատակից, կարող է ավելի լավ թիրախավորել անհատին կոնկրետ միջավայրում:

Երբ անձնական տվյալները մշակվում են առանց պրոֆայլինգի, տվյալները ճշգրիտ են և վերաբերում են նույնականացված կամ նույնականացվող անհատներին: Տվյալների սուբյեկտներն ընդհանուր առմամբ իրազեկ են կամ կարող են կռահել, թե իրենց մասին ինչ բնույթի տեղեկատվություն է տնօրինում տվյալները վերահսկողը: Քանի որ պրոֆայլինգը գոյացնում է անհատի համար նոր տվյալներ՝ այլ անձանց վերաբերող տվյալների հիման վրա, տվյալների սուբյեկտը ապրիորի չի կարող կասկածել կորելյացիայի գործընթացների գոյությունը, որոնք կարող են հանգեցնել հավանականության հաշվարկների հիման վրա այլ անհատներին բնորոշ հատկանիշները նրան վերագրելուն:

Իր բնույթով պրոֆայլինգը շատ հստակ գործընթաց է, որը գուցե կհամապատասխանի կամ չի համապատասխանի անձնական տվյալների հավաքման սկզբնական նպատակին: «Մեծ տվյալների» մասին գիտության կիրառմամբ պրոֆայլինգը շատ ավելի ռիսկային է դառնում անձնական տվյալների մշակման սովորական ընթացքի համեմատ: Ալգորիթմները կարող են կորելյացիաներ գտնել տարբեր տվյալների միջև և հանգեցնել ոչ միայն նույնականացման նոր օրինաչափության, այլև սեգմենտավորման և նույնիսկ ավելի վատ խտրական խմբավորման: Ավտոմատացված պրոֆայլինգի հետ կապված աճող ռիսկերը համապատասխան շտկման գործողությունների են արժանացել Ընդհանուր տվյալների պաշտպանության կանոնակարգի ներքո:

Ընդհանուր տվյալների պաշտպանության կանոնակարգը (22-րդ հոդված) սահմանափակումներ է նախատեսում՝ կապված պրոֆայլինգի համար անձնական տվյալների օգտագործման հետ: Դրանք ձևակերպված են հետևյալ կերպ. «Տվյալների սուբյեկտն իրավունք ունի չենթարկվել բացառապես ավտոմատացված մշակման, այդ թվում՝ պրոֆայլինգի վրա հիմնված որոշման, որը հանգեցնում է նրան վերաբերող իրավական հետևանքների կամ գրեթե նույնչափ լրջությամբ ազդում է նրա վրա»: 22-րդ հոդվածը սահմանում է բացառություններ պայմանագրի, տվյալների սուբյեկտի համաձայնության հիման վրա մշակվող դեպքերի կամ այն դեպքերի համար, որոնք նպատակ ունեն երաշխավորել տվյալների սուբյեկտի իրավունքները, ազատությունները և օրինական շահերը: Այլ դեպքերում տվյալները վերահսկողը պետք է իրականացնի տվյալների սուբյեկտի իրավունքների պաշտպանության միջոցառումներ, այդ թվում՝ որոշումների կայացման ժամանակ մարդկային միջամտության տեսքով: Կարևոր փաստ է այն, որ պրոֆայլինգը տեխնոլոգիական և բիզնես իրողություն է, և հարկ է դրան պատշաճ կերպով արձագանքել:

Ավտոմատացված որոշումների կայացում. հա՞րկ է մարդկանց պաշտպանել արհեստական բանականությունից

Մարդկային հասարակության վրա մեծամասշտաբ ազդեցություն ունեցող շատ տեխնոլոգիաների նման արհեստական բանականությունը (որը նաև հաճախ կոչում են «ավտոմատացված որոշումների կայացում» կամ «ալգորիթմային որոշումների կայացում») բնականորեն մի շարք ռիսկեր է պարունակում անհատների քաղաքացիական իրավունքների և ազատությունների համար: Տեխնոլոգիաները, որպես այդպիսին, չեն կարող ռիսկային կամ վտանգավոր լինել. մարդիկ են, որ դրանք վտանգավոր են դարձնում իրենց իսկ համար:

Չնայած հանրային կառավարման և բիզնեսի ոլորտներում արհեստական բանականության (ԱԲ) գործածման հսկայական օգուտներին, այն նաև զգալի ռիսկեր է պարունակում մարդու իրավունքների տեսանկյունից՝ վտանգելով անհատների անձնական կյանքի անձեռնմխելիության իրավունքը և կիրառելով ոչ բացահայտ խտրական աշխատակարգեր: ԱԲ-ի օգտագործման ընթացքում, թե՛ պետական իշխանությունները, թե՛ մասնավոր հատվածի ղեկավար կազմը պետք է ծայրաստիճան զգույշ լինեն և նկատի ունենան մարդու իրավունքների խախտումների հետ կապված ռիսկերը: ԱԲ-ի կիրառման ընթացքում անհատների քաղաքացիական իրավունքների և ազատությունների երաշխավորման սկզբունքները շատ նման անձնական տվյալների մշակման դեպքում կիրառվող սկզբունքներին:

Արհեստական բանականության կիրառման դեպքում մարդու իրավունքներին և ազատություններին սպառնացող գործոնները մեղմացնող միջոցները նույնպես հնարավոր է գտնել Եվրոպայի խորհրդի փաստաթղթերում: ԱԲ-ի հետ կապված ռիսկերի մեղմացմանն ուղղված ամբողջական մոտեցում առաջարկող այդպիսի փաստաթղթերից մեկը Նախարարների կոմիտեի CM/Rec(2020)1 հանձնարարականն է անդամ-պետություններին ալգորիթմային համակարգերի (ԱՀ)՝ մարդու իրավունքների վրա ունեցած ազդեցության վերաբերյալ: CM/Rec(2020)1 հանձնարարականը համապարփակ փաստաթուղթ է, որը վերաբերում է ալգորիթմային համակարգերի մշակման և գործարկման տարբեր կողմերին:

Հանձնարարականը բաղկացած է երկու հիմնական մասից՝ նախաբան և ուղեցույցներ: Նախաբանը նկարագրում է, թե մարդու իրավունքների նկատմամբ ինչպիսի սպառնալիքներ կարող է պարունակել արհեստական բանականությունը, որոնք կլինեն անձնական տվյալների մշակման համար ալգորիթմային համակարգերի անպատասխանատու օգտագործման և այդպիսի տվյալների մշակման վրա հիմնված ավտոմատացված որոշումների կայացման հետևանքները: Այդ փաստաթղթի նախաբանը անդամ-պետություններին կոչ է անում ձեռնարկել առաջարկված միջոցները՝ բացառելու մարդու իրավունքների և հիմնարար ազատությունների համար ԱԲ-ի հավանական սպառնալիքները:

CM/Re(2020)1 հանձնարարականի երկրորդ մասը՝ Հավելվածը, տրամադրում է մարդու իրավունքների վրա ալգորիթմային համակարգի ազդեցությունների թիրախավորման մանրամասն ուղեցույց: Ուղեցույցների մեծ ծավալի պատճառով այստեղ քննարկվում կամ համառոտ ներկայացվում են միայն ամենաէական հատվածները: Առաջինը և ամենակարևորը օրենսդրության ընդունումն է, որը կկառավարի ալգորիթմային համակարգերի մշակումն ու կիրառումը: Ալգորիթմային համակարգերի՝ մարդու իրավունքների վրա ազդեցությունների վերաբերյալ հանձնարարականը քաջալերում է անդամ-պետություններին՝ վերանայել գոյություն ունեցող օրենսդրությունը և նկատի առնել նոր իրավական ակտերի ընդունումը, որով անդրադարձ կարվի ալգորիթմային համակարգերի հետ համատեքստում մարդու իրավունքների հարցերին:

Ալգորիթմային համակարգերի՝ մարդու իրավունքների վրա ազդեցությունների մասին հանձնարարականները խորհուրդ են տալիս կառուցել ինստիտուցիոնալ շրջանակ, որը կկարողանա իրականացնել համապատասխան պրոդուկտների փորձագիտական վերլուծություն և տալ անաչառ, մասնագիտական կարծիք: Այն նաև մեծապես քաջալերում է մասնավոր հատվածի, քաղաքացիական հասարակության, գիտնականների և պետական իշխանությունների

միջև համագործակցությունը՝ մարդու իրավունքների վրա ԱԲ-ի ազդեցության ուսումնասիրության ժամանակ: Մի առանձին հատված վերաբերում է մասնավոր հատվածին և նրան, թե ինչպես պետք է ինքնակարգավորումն անդրադառնա մարդու իրավունքների խախտումների հավանական ռիսկերին՝ ինքնավար ալգորիթմային համակարգեր կիրառելիս:

Թե՛ պետական, թե՛ մասնավոր հատվածին վերաբերելի հիմնական սկզբունքներից մեկը մարդու իրավունքների վրա ԱԲ/ԱՀ-ի ազդեցության պարտադիր վերլուծությունն է: Ռիսկերի վերլուծությունը հարկ է կատարել հնարավորինս թափանցիկ կերպով, իսկ արդյունքները պետք է բաց լինեն հանրության համար: Պետական կառավարման ոլորտում ալգորիթմային համակարգերի օգտագործումը պետք է մեծապես արդարացված լինի:

Մեկ այլ կարևոր սկզբունք է այն, որ միայն անվանազերծված անձնական տվյալները կարող են օգտագործվել ալգորիթմային համակարգերի կողմից մշակման համար: Երբ պլանավորվում են տվյալների մշակման կամ ավտոմատացված որոշումների կայացման արդյունքները, անհատները (տվյալների սուբյեկտը կամ օգտատերը) պետք է իրազեկված լինեն դրա մասին և ունենան այդ գործընթացից դուրս գալու հնարավորություն մշակման ցանկացած փուլում: Չմասնակցելու կամ դադարեցնելու խնդրանքը պետք է լինի պարզ, հասկանալի և արագ:

ԱԲ/ԱՀ-ի մշակման և գործառնման սկզբունքները և կանոնները արագընթաց մշակման փուլում են: Ակնկալվում է, որ առաջիկա մի քանի տարիներին շատ միջազգային հաստատություններ կանդրադառնան այս նոր մարտահրավերին: Տվյալ պահին CM/Rec(2020)1 հանձնարարականն ամենաօգտակար փաստաթուղթն է, որ կառավարությունները և քաղաքացիական հասարակությունը կարող են օգտագործել ռիսկերի մեղմացման համար:

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅՈՒՆ

Ինչպես պարզեցինք Եվրոպայի խորհրդի փաստաթղթերի վերլուծությունից, կա առնվազն չորս թվային իրավունք, որոնք մենք կարող ենք անվանել Մարդու իրավունքների եվրոպական կոնվենցիայի, ՄԱԿ-ի Մարդու իրավունքների հռչակագրի ու Քաղաքացիական և քաղաքական իրավունքների մասին միջազգային դաշնագրի ներքո ավանդական մարդու իրավունքների կա՛մ փոխակերպում, կա՛մ հետագա ընդլայնում: Այդ իրավունքները շարադրված են ստորև.

- Համացանցի միջոցով տեղեկությունների որոնումների, ստացման և տարածման համար համացանցի հասանելիության և օգտագործման իրավունք՝ առանց բովանդակության նախնական հսկողության և մեդիայով պայմանավորված սահմանափակման,

- Համացանցով ծառայությունների տրամադրման իրավունք՝ առանց սուբյեկտով պայմանավորված թույլտվության, միմիայն հաղորդելու հիմքի վրա, և առանց ծառայություն մատուցողներին պարտավորեցնելու մշտադիտարկել իրենց ծառայություններից օգտվելու շրջանակներում հաղորդվող բովանդակությունը,

- Համացանցի անանուն օգտագործման, այդ թվում՝ տեղեկությունների անանուն որոնման, ստացման և առանց նախնական պարտադիր թույլտվության, ինքնության նույնականացման հաղորդակցման իրավունք,

- Թվային գաղտնիության իրավունք՝ ներառյալ անձնական կյանքի և անձնական տվյալների պաշտպանությունը իշխանությունների անօրինական միջամտությունից, երրորդ անձանց կողմից անօրինական օգտագործումից, ինչպես նաև անձնական կյանքի ինքնապաշտպանության գործիքների օգտագործման իրավունքը, սակայն չսահմանափակվելով դրանցով:

Պրոֆայլինգը և արհեստական բանականությանը (ալգորիթմային համակարգերին) վերաբերող ռիսկերը չեն նշվում որպես մարդու իրավունքների առանձին կատեգորիա, քանի որ դրանք ընդգրկում է թվային գաղտնիության իրավունքների ավելի լայն հասկացությունը: Դասակարգումը ֆորմալ չէ և ոչ էլ խիստ իրավական: Վերը նշված թվային իրավունքներից յուրաքանչյուրը կարելի է ընդլայնել կամ նեղացնել՝ կախված համատեքստից:

Այժմ, երբ իրավունքների շրջանակը սահմանված է, արժե ներկայացնել, թե ինչպես են այս իրավունքները ներմուծվում և իրականացվում:

Համընդհանուր ծառայությունը որպես համացանցի հասանելիության իրավունք

Մարդու իրավունքների եվրոպական կոնվենցիայի 10-րդ հոդվածով սահմանված մարդու իրավունքների հիման վրա պետությունն ունի բացասական պարտավորություն՝ վերացնել վարչական այնպիսի խոչընդոտները, ինչպիսին են համացանց մուտք գործելու համար նախաթույլտվությունը և նախանույնականացումը: Կառավարությունների՝ համացանցի հասանելիության ազատության հետ կապված բացասական պարտավորությունները ենթադրում են նաև հատուկ կանոններ համացանցում հրապարակված բովանդակության վերաբերյալ: Չի թույլատրվում զտել կամ արգելափակել բովանդակությունը՝ բացառությամբ այն դեպքերի, երբ այդպիսի գործողությունը պայմանավորված է անհատի որոշմամբ կամ օրենքով սահմանված կարգով հարկադիր կատարման ենթակա միջոց է՝ հանցագործություն կանխելու նպատակով:

Բացասական պարտավորությունները սովորաբար կատարման տեսանկյունից պարզ են: Պետական մարմինները պարզապես պետք է հետևեն անդամ-պետությունների ներկայացուցիչների կողմից գործադրված և ընդունված սկզբունքներին և ուղեցույցներին:

Այնուամենայնիվ, կառավարությունը հաճախ փորձում է սահմանափակել անհատների ազատությունները՝ այդպիսի սահմանափակումներն արդարացնելով հանրային շահով: Այդ սահմանափակումների իրական պատճառը, սակայն, ավելի բարդ համապատասխանության մոդել գտնելու շահագրգռություն չունենալն է: Դրական պարտավորությունների իրականացումը շատ ավելի դժվար է՝ համապատասխան մոտեցում ընտրելու, ֆինանսավորման և կիրարկման տեսանկյունից, և այստեղ մենք կարող ենք տեսնել մոտեցումների և մոդելների տարբերություններ:

Նման մեխանիզմներից մեկը համընդհանուր ծառայությունների հասկացությունն է, որը մշակվել է 1990-ականներին: Հասկացությունը ձևավորել են երկու միջազգային հաստատություններ՝ Համաշխարհային բանկը և Եվրոպական միությունը: Այն լայնորեն ներդրվել է շատ զարգացած և հատկապես զարգացող երկրներում: Համընդհանուր ծառայության գաղափարը հիմնված է սահմանված գնով, երկրի ողջ տարածքում հասանելի ծառայությունների նվազագույն շրջանակի ապահովման վրա:

Ի սկզբանե, համընդհանուր ծառայությունների շրջանակը ներառում էր միայն ձայնային հեռախոսի և հանրային հեռախոսի ծառայությունը և դրանից օգտվողներին: Այնուամենայնիվ, 2000-ականների կեսերին երկրների մեծ մասում, որտեղ համընդհանուր ծառայության մոդելը ենթադրում էր համացանցային հասանելիություն, համացանցային ծառայությունները նույնպես ներառվել են համընդհանուր ծառայությունների փաթեթում: Մի շարք երկրներ, օրինակ՝ ԵՄ անդամ-պետությունները, ավելի առաջ գնացին և լայնաշերտ համացանցային ծառայությունները դարձրին համընդհանուր ծառայություններ փաթեթի մի մաս: Պակաս բարեկեցիկ երկրներում, որտեղ համընդհանուր ծառայությունների սուբսիդավորումն իրագործելի չէ, համընդհանուր հասանելիությունն ապահովվեց համայնքային հասանելիության ծառայությունների միջոցով:

Ինչպես նշվել է, համընդհանուր ծառայությունների մոդելը հիմնված է տեղերում (սովորաբար գյուղական համայնքներում) ծառայությունների հասանելիության սուբսիդավորման սկզբունքի վրա, որտեղ առևտրային ծառայությունները տնտեսապես շահութաբեր չեն: Համընդհանուր ծառայությունների համար սուբսիդիաների երեք հիմնական մոդելներ կան: Մեկը կոչվում է «համընդհանուր պարտավորություն», երկրորդը՝ «համընդհանուր ֆոնդ», իսկ երրորդ մոդելը՝ «պետական ուղիղ սուբսիդիաներ»: Պետական ուղիղ սուբսիդիաները ուղիղ և պարզ մոտեցում են, որի շրջանակում կառավարությունը ներդրում է անում ցանցում, գործարկում է այն կամ արտապատվիրում է գործառնությունը կարգավորված գներով:

Համընդհանուր ծառայության պարտավորությունը, որը հաճախ անվանում են նաև «խաչաձև սուբսիդավորման» մոդել, ծառայություններ մատուցողների և ցանցային օպերատորների լիցենզավորման նախապայմանն է. նրանք պետք է տրամադրեն համընդհանուր ծառայություններ երկրի ամբողջ տարածքում՝ կարգավորված գնով: Ծառայության ծախսերը սովորաբար ծախսածածկվում են ծառայությունների շահութաբեր հատվածի շնորհիվ: Իսկ վերջին մոդելը համընդհանուր ծառայությունների հիմնադրամն է, երբ առևտրային ծառայություն մատուցողները պարտավոր են վճարել համընդհանուր ծառայության վճար (սովորաբար եկամտի որոշ տոկոսի չափով), որը կառավարությունը կամ անկախ կարգավորողն օգտագործում է՝ ուղղակիորեն սուբսիդավորելու համընդհանուր ծառայություն մատուցողներին: Մոդելների՝ պետական և համայնքային ֆինանսավորման, համաֆինանսավորման և պետական-մասնավոր հատվածների գործընկերության համադրությունը կիրառվում է՝ կոնկրետ շուկայում առավել արդյունավետ մոդելի կառուցման համար:

Ցանցի չեզոքությունը

Եվրոպական երկրների գերակշիռ մեծամասնությունը տարիներ առաջ լուծել է ավանդական ԶԼՄ-ներում բովանդակության սահմանափակումներին առնչվող հարցը: Իհարկե, արագընթաց զարգացող թվային մեդիան մշտապես նոր մարտահրավերներ է բերում ներպետական դատական համակարգերի դատարանների դահլիճներ և ներկայացնում դրանք Մարդու իրավունքների եվրոպական դատարանի վճռին: Այնուամենայնիվ, հիմնական սկզբունքները՝ նախնական

հսկողության բացակայությունը և առանձին մեդիայով պայմանավորված սահմանափակումների անընդունելիությունը, իրականացվում են գրեթե բոլոր անդամ-պետություններում:

Մի շարք երկրներում, սակայն, հատկապես՝ Արևելյան Եվրոպայի (թեև ոչ միայն այնտեղ), թվային գրաքննությունը վերածվել է բովանդակության գոյացման հարթակների, այդ թվում՝ սոցիալական ցանցերի դեմ պայքարի: Մենք արդեն քննարկել ենք Ռուսաստանում և Ղազախստանում կոնկրետ համացանցային արձանագրությունների սահմանափակման փորձերը: Կոնկրետ տեխնոլոգիաների, օրինակ՝ հաղորդակցության արձանագրությունների, ցանցի ճարտարապետության և երթուղավորման սխեմաների սահմանափակումներն այսօր իրական սպառնալիք են համացանցի ազատության համար:

Կարևոր իրողություն է այն, որ բովանդակությանն առնչվող այդ սահմանափակումները միշտ չէ, որ ձեռնարկվում են պետական իշխանությունների կողմից: Համացանցի թրաֆիքի գերակայությունների տնտեսական խտրականության վերացման ուղղությամբ լրջագույն պայքար է ընթանում ամբողջ աշխարհում, քանի որ հեռահաղորդակցությունների օպերատորները գիտակցում են, որ ավանդական բիզնես մոդելները չունեն նախկին շահութաբերությունը: Եվրոպայի խորհուրդն արձագանքեց թրաֆիքի խտրականության խնդրին 2010թ. սեպտեմբերի 29-ին Եվրախորհրդի Նախարարների կոմիտեի ընդունած ցանցային չեզոքության մասին հռչակագրում:

Հռչակագիրը փաստում է, որ համացանցային բովանդակության հասանելիությունը կարող է համարվել ազատ միայն այն ժամանակ, երբ հավելվածները և ծառայությունները խտրականության չեն ենթարկվում դրանց բնույթից՝ առևտրային կամ ոչ առևտրային հանգամանքից ելնելով: Ցանցի չեզոքության սկզբունքը հայտարարվել է համընդհանուր կանոն, որը պետք է կիրառվի՝ անկախ համացանցային միակցվածության համար օգտագործվող ենթակառուցվածքից կամ ցանցից:

Համացանցում ծառայություններ մատուցելու իրավունքը

Որպես հաղորդակցության էական միջոց ստեղծված համացանցը շատ շուտով վերածվեց բիզնեսի հարթակի: Փոքր և խոշոր բիզնեսները, տեղական և համաշխարհային մակարդակի վաճառողներն իրենց ուշադրությունը կենտրոնացրին թվային առևտրային հարթակների վրա: Պետական իշխանությունները գիտակցում են, որ, մի կողմից, համացանցային առևտուրը հսկայական ներուժ ունի տնտեսական աճի համար, իսկ մյուս կողմից՝ պարունակում է մի շարք ռիսկեր թե՛ բիզնեսների, թե՛ նրանց հաճախորդների համար: Նախարարների կոմիտեի՝ Համացանցում հաղորդակցության ազատության մասին հռչակագիրը հայտարարում էր համացանցում բիզնեսի ազատության ընդհանուր սկզբունքները, այդ թվում՝ ծառայություն մատուցողների սահմանափակ պատասխանատվության և բիզնես մեթոդներին (համացանցային) վերաբերող կոնկրետ կարգավորումների բացակայությունը:

Ամենաարժեքավոր իրավական փաստաթուղթը, որն էական դեր է խաղացել ամբողջ աշխարհում համացանցում իրականացվող բիզնեսի և էլեկտրոնային առևտրի զարգացման համար, Եվրոպական խորհրդարանի և Խորհրդի 2000թ. հունիսի 8-ի 2000/31/EC դիրեկտիվն է տեղեկատվական հասարակության ծառայությունների, մասնավորապես՝ Ներքին շուկայում էլեկտրոնային առևտրի մի շարք իրավական հարցերի վերաբերյալ: Փաստաթուղթը հայտնի է նաև որպես Էլեկտրոնային առևտրի մասին ԵՄ դիրեկտիվ: Էլեկտրոնային առևտրի դիրեկտիվը սահմանում է հիմնարար կանոնները, որոնք նախասահմանված էին տասնամյակներ շարունակ էլեկտրոնային առևտրի համար ոչ միայն ԵՄ-ում, այլ նաև շատ այլ երկրներում, այդ թվում՝ Արևելյան Եվրոպայի պետություններում:

Էլեկտրոնային առևտրի դիրեկտիվը սահմանում է՝ անդամ-պետությունները պետք է երաշխավորեն, որ տեղեկատվական հասարակությանը ծառայություն մատուցողի գործունեությունը չենթարկվի նախնական թույլտվության կամ համարժեք ազդեցություն ունեցող որևէ այլ պահանջի: Այնուհանդերձ, ընդհանուր թույլտվության սկզբունքից բացի, Էլեկտրոնային առևտրի դիրեկտիվը երկրներին վերապահում է գործողությունների որոշ տեսակների համար,

օրինակ՝ նոտարների, փաստաբանների կողմից վստահորդին դատարաններում և բժշկական հաստատություններում ներկայացնելու դեպքերում, նախնական թույլտվություն կիրառելու իրավունք: Դիրեկտիվը նախատեսում է վերապահումներ նաև առցանց խաղատների և վիճակախաղերի համար:

Էլեկտրոնային առևտրի դիրեկտիվի մեկ այլ անհրաժեշտ դրույթ սահմանում է, որ ԵՄ անդամ-պետությունները պետք է ապահովեն ծառայություն մատուցողի՝ հաղորդված տեղեկատվության համար պատասխանատվություն չկրելը, պայմանով, որ այդպիսի ծառայություն մատուցողը՝

- չէ տեղեկության հաղորդման նախաձեռնողը,
- չի ընտրել հաղորդման ստացողին, և
- չի ընտրում կամ փոփոխում հաղորդման մեջ պարունակվող տեղեկությունը:

Էլեկտրոնային առևտրի մասին դիրեկտիվի համապատասխան դրույթով նաև պահանջվում է, որ անդամ-պետությունները ծառայություն մատուցողների համար չսահմանեն նրանց փոխանցած կամ կուտակած տեղեկությունների մշտադիտարկման ընդհանուր պարտավորություն, ինչպես նաև չնախատեսեն անօրինական գործունեության մասին վկայող փաստերի կամ հանգամանքների ակտիվ որոնման ընդհանուր պարտավորություն:

Դիրեկտիվը պարունակում է պետությունների համար մի շարք այլ, դրական պարտավորություններ, որոնք կարևոր են թվային շուկաներում ընկերությունների նորմալ գործառնությունների համար: Մասնավորապես, այն նաև վերաբերում է այնպիսի հարցերի, ինչպիսին են չմիջնորդավորված էլեկտրոնային առևտրային հաղորդակցությունները, դատական վեճերի լուծումը, առցանց պայմանագրերի վավերականությունը և էլեկտրոնային առևտրին ու էլեկտրոնային բիզնեսներին վերաբերող մի շարք այլ կարևոր հարցեր: Կարգավորման այդ չափորոշիչները, սակայն, լիարժեքորեն վերաբերելի չեն այս ուսումնասիրության թեմային, որն առաջնայնորեն կենտրոնանում է թվային իրավունքների, ոչ թե թվային տնտեսության լայն, տնտեսական բնույթի հարցերի վրա:

Անանուն հասանելիության իրավունք և թվային գաղտնիության իրավունք

Անանուն հասանելիության իրավունքը հստակորեն սահմանված է Եվրոպայի խորհրդի մի շարք փաստաթղթերով, այդ թվում՝ Համացանցում հաղորդակցության համար ազատության մասին Նախարարների կոմիտեի հռչակագրով: Թվում է՝ շատ հեշտ է իրականացնել պետության բացասական պարտավորությունը, բայց այն բախվում է խոշոր հարձակումների իրավապահ մարմինների կողմից ոչ միայն նոր ժողովրդավարություններում, այլ նաև մի շարք ավանդաբար լիբերալ ժողովրդավարություններում: Դեպքերի գերակշիռ մասում անանունությունը և թվային գաղտնիությունը միասին են վիճարկվում, և փաստացի այս երկու իրավունքները սերտորեն փոխկապակցված են:

Անանունությունն օգնում է գաղտնիության պահպանմանը, իսկ պահպանված գաղտնիությունն, ըստ սահմանման, օգնում է թաքցնել անհատների ինքնությունը: Մեծ տվյալների դարաշրջանում նույնիսկ անվանազերծված անձնական տվյալները կարող են օգտագործվել անհատներին հետևելու և անուղղակիորեն նրանց ինքնությունը պարզելու նպատակով: Սա է այս երկու իրավունքները միասին դիտարկելու պատճառներից մեկը: Անանունության և գաղտնիության միաժամանակյա գնահատման համար մեկ այլ պատճառ է այս երկու փոխկապակցված թվային իրավունքները կարգավորող օրենսդրության կրկնականությունը:

Եվրոպական միությունը թվային իրավունքների ճանաչման և պաշտպանության գործում առաջատար հաստատություններից մեկն է: ԵՄ Տվյալների պաշտպանության 95/46/EC դիրեկտիվը այն չափորոշիչներից մեկն էր, որին շատ երկրներ հետևեցին տասնամյակներ

շարունակ: ԵՄ Ընդհանուր տվյալների պաշտպանության կանոնակարգը, որը փոխարինեց Տվյալների պաշտպանության դիրեկտիվը 2018-ին, Է՛լ ավելի բարձր մակարդակի է հասցնում անձնական տվյալների պաշտպանությունը: Շուկայի այս խոշոր ծավալների և գնողունակության շնորհիվ, ԵՄ չափորոշիչներն ընդունվել են Եվրոպա ապրանքներ մատակարարել և ծառայություններ մատուցել ձգտող շատ այլ երկրներում:

Չնայած անձնական տվյալների պաշտպանության բարձր մակարդակի չափորոշիչներին, 2006թ. մարտի 15-ին Եվրոպական խորհրդարանը և Խորհուրդն ընդունեցին Տվյալների պահպանման դիրեկտիվը[5]: Տվյալների պահպանման դիրեկտիվը հանրայնորեն մատչելի էլեկտրոնային հաղորդակցության ծառայություններ մատուցողներից կամ հանրային հաղորդակցությունների ցանցերից պահանջում էր պահպանել անհատների կամ իրավաբանական անձանց թրաֆիքը և տեղորոշման տվյալները: Այս տվյալների կազմում էին ներառվում մուտքային զանգի հեռախոսահամարը, բաժանորդի կամ գրանցված օգտատիրոջ անունն ու հասցեն, օգտատիրոջ նույնականացման տվյալները (եզակի նույնացուցիչը, որը տրվում է էլեկտրոնային հաղորդակցությունների ծառայության հետ պայմանագիր կնքած յուրաքանչյուր անձի), համացանցային արձանագրության հասցեները, հավաքված համարները, զանգի վերահասցեավորման կամ զանգի փոխանցման գրանցումները:

Այսպիսի տեղեկությունների պահպանման ժամկետն առնվազն վեց ամսից մինչև երկու տարի էր, իսկ այդ տվյալների մշակման և կուտակման միակ նպատակը լուրջ հանցագործությունների, օրինակ՝ կազմակերպված հանցավորության և ահաբեկչության կանխարգելումը, հետաքննությունը, բացահայտումը և դատական կարգով հետապնդումն էր: Անհատների հաղորդակցության բովանդակությունը չէր պահպանվում: Տվյալների պահպանման դիրեկտիվի վերը նշված դրույթի հիման վրա ԵՄ անդամ բազմաթիվ պետություններ ընդունել են ներպետական օրենսդրություն, որը համացանցային ծառայություններ մատուցողներից պահանջում է պահպանել օգտատերերի անձնական տվյալները՝ առանց տվյալների սուբյեկտների համաձայնության:

Իռլանդիայում և Ավստրիայում մի խումբ իրավաբաններ վիճարկել են ազգային պետությունների կողմից ընդունված օրենսդրությունը: Իռլանդական փաստաբանական ֆիրման՝ «Դիջիթըլ Ռայթս Այըրլանդ»-ը վիճարկել է ներպետական օրենսդրությունը այն հիմնավորմամբ, որ Դիրեկտիվները սահմանում են անհամաչափ միջոցներ՝ առանց անհատների տվյալների համար համարժեք երաշխիքների տրամադրման: Ըստ եվրոպական դատահիրավական շրջանակի, ներպետական դատարանները գործերով որոշումներ կայացնելիս իրավունք ունեն իրավական հարցումներ հղել Արդարադատության եվրոպական դատարանին եվրոպական իրավական շրջանակի ներքո ներպետական օրենսդրության վավերականության վերաբերյալ:

Արդարադատության եվրոպական դատարանը գտել է, որ ազգային իրավասու մարմիններին հասանելիություն տրամադրելու համար տվյալների պահպանումը ենթադրում է տվյալների մշակում և հետևաբար ազդում է հիմնարար իրավունքների խարտիայի երկու հիմնական իրավունքների՝ 7-րդ հոդվածով երաշխավորված անձնական կյանքի անձեռնմխելիության իրավունքի և 8-րդ հոդվածով երաշխավորված անձնական տվյալների պաշտպանության իրավունքի վրա: Արդարադատության եվրոպական դատարանը նաև գտել է, որ Տվյալների պահպանման դիրեկտիվի համապատասխան դրույթը խախտում է համաչափության սկզբունքը: Տվյալների պահպանման դիրեկտիվն ուժը կորցրած է ճանաչվում 2006թ. ուժի մեջ մտնելու պահից ի վեր: ԵՄ անդամ-պետությունները, որոնք փոխադրել են այս Դիրեկտիվն իրենց ներպետական իրավական համակարգեր, պետք է քայլեր ձեռնարկեն՝ ապահովելու համապատասխանությունը այս վճռին:

Տվյալների պահպանման դիրեկտիվի մասին Արդարադատության եվրոպական դատարանի վճիռը փայլուն օրինակ է, թե ինչպես են հիմնարար իրավունքները, այդ թվում՝ անհատների թվային

[5] Եվրոպական խորհրդարանի և Խորհրդի 2006թ. մարտի 15-ի 2006/24/EC դիրեկտիվ՝ հանրությանը էլեկտրոնային հաղորդակցական ծառայությունների կամ հանրային հաղորդակցությունների ցանցերի տրամադրման կապակցությամբ գոյացված կամ մշակված տվյալների պահպանման և 2002/58/EC դիրեկտիվում փոփոխություններ անելու մասին

իրավունքների վրա հիմնված, գերակշռում եվրոպական օրենսդրության նկատմամբ, որը ներմուծում է ոչ համաչափ անվտանգության միջոցներ: Այնուամենայնիվ, դատական կարգով վերանայումը և կիրարկումը գաղտնիության և անանունության պաշտպանության սովորական գործիքներ չեն: Հիմնական գործիքները շարունակում են մնալ տվյալների պաշտպանության, անձնական կյանքի անձեռնմխելիության օրենսդրության խախտումների համար տույժերն ու տուգանքները, իսկ անձնական տվյալների կանխամտածված և դիտավորյալ չարաշումների համար՝ քրեական պատասխանատվությունը: Ընդհանուր տվյալների պաշտպանության կանոնակարգի ներքո սահմանված տույժերն ու տուգանքները տատանվում են 10-20 միլիոն եվրոյի կամ խախտումներ թույլ տված ընկերությունների տարեկան համաշխարհային շրջանառության 2%-4%-ի միջակայքում:

ԹՎԱՅԻՆ ԻՐԱՎՈՒՆՔՆԵՐԸ ՀԱՅԱՍՏԱՆՈՒՄ

Հայաստանը Եվրոպայի խորհրդի անդամ է և Անձնական տվյալների ավտոմատացված մշակման դեպքում անհատների պաշտպանության մասին Եվրոպայի խորհրդի կոնվենցիայի ստորագրյալ անդամ: Հայաստանը նաև ստորագրել է Կիբերհանցագործությունների մասին Բուդապեշտի կոնվենցիան՝ այն նույնպես կարևոր իրավական գործիք է, որը սահմանում է հայաստանյան իշխանությունների դրական և բացասական պարտավորությունները կիբերհանցագործությունների հետաքննության պատշաճ իրականացման աշխատակարգերի և այլ չափորոշիչների առնչությամբ: Հայաստանն ունի հարաբերականորեն բարձր համացանցի ազատության վարկանիշ (75 ըստ «Ֆրիդոմ Հաուս»-ի Համացանցի ազատության հետազոտության[6]) և զբաղեցնում է Արգենտինայի և Ճապոնիայի միջև միջանկյալ դիրք՝ մեկ միավորով զիջելով Ֆրանսիային և ԱՄՆ-ին:

Համացանցի հասանելիության իրավունքը (Հայաստան)

Չնայած իր տարածքի փոքրությանը՝ Հայաստանը դեռևս սահմանափակ հնարավորություններ ունի երկրի ամբողջ տարածքում համընդհանուր հասանելիության տրամադրման համար: Հայաստանյան իշխանություններն ի սկզբանե[7] ընդունել էին համընդհանուր ծառայության ֆոնդի մոդելը, որն այդպես էլ չի ստեղծվել՝ հիմնական քաղաքականության և շուկայում խաղացողների միջև իրավական մանրակրկիտ շրջանակի, համընդհանուր ծառայությունների դիմաց վարձավճարների և սուբսիդավորման մեխանիզմի շուրջ անհամաձայնության պատճառով: Միևնույն ժամանակ, շարժական համացանցի ծածկույթը բավականին լավն է Հայաստանում, և ընդհանրապես, ծառայությունները հասանելի են ամենուր՝ հարաբերականորեն մատչելի գներով:

Ցանցի չեզոքություն (Հայաստան)

Ցանցի չեզոքությունը չի ներմուծվել Հայաստան: Հայաստանի ազգային կարգավորող մարմինը մի քանի հայտարարություններով է հանդես եկել՝ տեխնոլոգիաների չեզոքությունը համարելով կարգավորման և քաղաքականությունների իրականացման կարևոր սկզբունք: Չնայած այս փաստին, ցանցի չեզոքության սկզբունքն այդպես էլ չի ընդունվել որպես իրավական պարտադիր ուժ ունեցող կարգավորում: Քաղաքացիական հասարակության փորձը՝ ջատագովել ցանցի չեզոքության չափորոշիչների ընդունումը Էլեկտրոնային հաղորդակցության մասին օրենքի ներքո, բախվեց ցանցերի օպերատորների ուժեղ դիմադրությանը: Օրենքում փոփոխությունների և լրացումների շուրջ բանավեճը դեռևս ընթացքի մեջ է և կախված կլինի կառավարության ու իշխող խորհրդարանական խմբակցության անդամների դիրքորոշումից:

Համացանցային բիզնեսների կարգավորումը (Հայաստան)

Անցած երկու տասնամյակների ընթացքում եվրոպական ինտեգրման ուղղությամբ իրականացված մի շարք նախաձեռնությունների շնորհիվ, էլեկտրոնային առևտրի մասին հայաստանյան օրենսդրությունն արտացոլում է համացանցային բիզնես գործունեության համար համապատասխան իրավունքների սկզբունքները: Այնուամենայնիվ, էլեկտրոնային առևտրի մասին հայաստանյան օրենսդրությունն ամբողջովին չի համապատասխանում ԵՄ էլեկտրոնային առևտրի դիրեկտիվին: Մասնավորապես, Հայաստանը չունի չմիջնորդավորված էլեկտրոնային առևտրային հաղորդակցությունների (էլեկտրոնային սպամի) վերաբերյալ լավ սահմանված

[6] Համացանցի ազատության գնահատում, «Ֆրիդոմ Հաուս», 2019թ., «Համացանցի ազատությունը 2019 թվականին» https://freedomhouse.org/country/armenia/freedom-net/2020

[7] Էլեկտրոնային հաղորդակցության մասին ՀՀ օրենքը, 2005թ., 40-րդ հոդված

կանոններ և չունի առցանց արբիտրաժի պահանջ: Այնուամենայնիվ, Էլեկտրոնային առևտրի դիրեկտիվի մի մասը, որը վերաբերում է ծառայություն մատուցողների սահմանափակ պատասխանատվությանը, լիարժեք կերպով ներառված է Քաղաքացիական օրենսգրքի փոփոխված 416.1 և 416.2 հոդվածներում:

Էլեկտրոնային առևտուրը, այնուհանդերձ, համացանցային բիզնեսի միակ տեսակը չէ, և համացանցով բիզնես անելու իրավունքը չի սահմանափակվում էլեկտրոնային առևտրով կամ էլեկտրոնային վաճառքով: Բոլոր թվային բիզնեսների համար հիմնական տարր է հեռահաղորդակցության ծառայությունների առկայությունը: Հեռահաղորդակցությունների կարգավորման շրջանակը շատ ավելի բարդ է և ներառում է բազմաթիվ դիրեկտիվներ ու կանոնակարգեր: Չկա հեռահաղորդակցության բիզնեսների կարգավորման բոլոր սկզբունքները քննարկելու անհրաժեշտություն, սակայն կարելի է դիտարկել միայն նրանք, որոնք շատ կարևոր են համացանցային բիզնեսի ազատության և համացանցում հաղորդակցության ազատության համատեքստում:

ԵՄ-ում նախաձեռնել են հեռահաղորդակցությունների նշիչների ազատականացումը՝ որպես այս ոլորտի զարգացման հիմք: Եվրոպացի քաղաքականություն մշակողները կարծում էին, որ ոլորտը կարող էր աճ գրանցել միայն ազատական կարգավորման միջավայրի պայմաններում: Քաղաքականության այսպիսի մոտեցումն արտացոլվել է Եվրամիության Հասանելիության դիրեկտիվում (որին շուտով փոխարինելու կգա Եվրոպական էլեկտրոնային հաղորդակցության օրենսգիրքը), որը փաստում է, որ էլեկտրոնային հաղորդակցությունների բիզնեսը պետք է ենթարկվի ոչ թե լիցենզավորման, այլ ընդհանուր թույլտվության, եթե դրա համար չեն պահանջվում հատկացումներ սուղ ռեսուրսներից կամ պետական բյուջեից: Հեռահաղորդակցությունների ոլորտի մասին Հայաստանի Հանրապետության օրենսդրությունը, որը մեծապես հիմնված է եվրոպական կարգավորման սկզբունքների վրա, դեռևս պահանջում է ցանցային օպերատորներից՝ ձեռք բերել լիցենզիա գնահատման ընթացակարգի միջոցով:

Անանունության և թվային գաղտնիության իրավունքը

Հայաստանում անանունության և թվային գաղտնիության իրավունքի իրացումը նախնական փուլում է: Հայաստանը ստորագրել և վավերացրել է Եվրոպայի խորհրդի անձնական տվյալների պաշտպանության մասին դիրեկտիվը, այնուամենայնիվ, Հայաստանի Հանրապետությունն իր օրենսդրությունը եվրոպական սկզբունքներին մեծամասամբ համապատասխանեցրեց միայն 2015 թվականին: Համացանցային հասանելիության անանունության սկզբունքը պահպանվում է, բայց պարբերաբար վիճարկվում է՝ բջջային նույնականացման մոդելի կիրառմամբ, ինչպես հետխորհրդային շատ երկրներում: Այսպիսի յուրաքանչյուր փորձ բախվում է համացանցային հանրության դիմադրությանը, բայց որոշ ժամանակ անց վերադառնում է նորից ու նորից:

Համեմատաբար վերջերս քաղաքացիական հասարակությունը փորձ ձեռնարկեց՝ առաջարկել մի կարգավորում, ըստ որի կարգելվեր անձնական տվյալների զանգվածային կուտակումը: Սակայն այն ձախողվեց իրավապահ մարմինների և Բարձր տեխնոլոգիաների արդյունաբերության նախարարության դիմադրության պատճառով: Այնուամենայնիվ, քաղաքացիական հասարակության ակտիվ ներկայացուցիչները շարունակում են ջատագովել փոփոխություններ՝ առաջ մղելով ցանցի չեզոքության կարգավորումը: Անձնական տվյալների պաշտպանության օրենքի խախտումների համար նախատեսված տուգանքների չափերն աննշան են և այդ իսկ պատճառով չեն կարող երաշխավորել տվյալների պաշտպանության պատշաճ մակարդակ:

ԹՎԱՅԻՆ ԻՐԱՎՈՒՆՔՆԵՐԻ ՀԵՏ ԿԱՊՎԱԾ ՄԱՐՏԱՀՐԱՎԵՐՆԵՐԸ ՀԱՅԱՍՏԱՆՈՒՄ

Սամվել Մարտիրոսյան

ԻՆՏԵՐՆԵՏԻ ԱԶԱՏՈՒԹՅԱՆ ՀԻՄՆԱԿԱՆ ԽՆԴԻՐՆԵՐԸ ՀԱՅԱՍՏԱՆՈՒՄ

Մինչ բազմաթիվ ազատություններին վերաբերող միջազգային զեկույցներում և վարկանիշային ցուցակներում Հայաստանը հայտնվում է միջանկյալ դիրքերում և չի կարող փայլել կայուն, ինստիտուցիոնալ ժողովրդավարական առաջընթացի մասին խոսող ցուցանիշներով, ինտերնետի ազատությունները տարիներ շարունակ եղել են շատ ավելի բարվոք վիճակում:

Freedom House կազմակերպության ամենամյա Freedom on the Net ռեյթինգում Հայաստանը, բացառությամբ 2017-ի, ընդգրկվել է ազատ երկրների ցանկում, և միայն 2016-ին ՀՀ ոստիկանության պարեկապահակետային ծառայության (ՊՊԾ) գնդի գրավումից հետո մոտ մեկ ժամով Ֆեյսբուք սոցիալական ցանցի արգելափակումը հանգեցրեց Հայաստանի վարկանիշի նվազեցմանը և երկիրը մեկ տարով հայտնվեց կիսաազատ երկրների ցանկում, բայց արդեն հաջորդ տարի նորից վերականգնեց իր դիրքերը:

Ինտերնետի ազատությունների տեսանկյունից Հայաստանում ծայրահեղ ծանր է եղել երկու ժամանակաշրջան:

Առաջինը 2008-ի մարտին նախագահական ընտրություններին հաջորդած արտակարգ դրության ժամանակաշրջան էր, որի ընթացքում արգելափակումներ մտցվեցին ինտերնետային տիրույթում:

Երկրորդ ժամանակատվածը մեկնարկեց 2020-ի մարտին, երբ COVID-19-ի համավարակով պայմանավորված Հայաստանում հայտարարվեց արտակարգ դրություն, որն իր հետ բերեց պաշտոնապես հայտարարված գրաքննություն:

Սրան զուգահեռ գործարկվեց համակարգ, որը բջջային հեռախոսների միջոցով և բջջային օպերատորների կողմից տրամադրվող տվյալների հիման վրա թույլ էր տալիս վերահսկել Հայաստանի ամբողջ բնակչության շարժը և սոցիալական կապերը: Դրան գումարվեցին Արցախյան պատերազմի բերած գրաքննությունն ու արգելափակումները, որոնք ուղեկցվում էին Ադրբեջանից և Թուրքիայից իրականացվող զանգվածային հաքերային հարձակումներով:

Այս բոլոր դեպքերը բացահայտում են այն հիմնական խնդիրները, որոնք գոյություն ունեն Հայաստանի համացանցում:

Մարտի մեկի հետ կապված դեպքերը

2008-ի մարտի 1-ի իրադարձություններից հետո հայտարարվեց արտակարգ դրություն:

Արդեն մարտի 2-ին, ժամը 23-00-ի սահմաններում ինտերնետային ծառայություն մատուցող ընկերությունները (ըստ մեր ունեցած տվյալների՝ ԱԱԾ-ի ցուցումով) սկսեցին արգելափակել Հայաստանի այցելուների մուտքը մի շարք հայկական ՁԼՄ-ների և ընդդիմադիր կազմակերպությունների կայքեր:

Առաջին օրերի ընթացքում, չճշտված պատճառներով, ցանցից անհետացան նաև panorama.am և regnum.ru կայքերը, սակայն հետագայում դրանք գործեցին անխափան (հարկ է նշել, որ մի շարք բլոգներում և ֆորումներում հնչում էին կարծիքներ, թե այս երկու կայքերը նույնպես ենթարկվել էին արգելափակման):

Առաջին երկու օրվա ընթացքում ֆիլտրումը կատարվում էր քաոսային կերպով՝ տարբեր պրովայդերներ տարբեր ցուցակներով էին փակում կայքերը:

Մարտի 3-ին Հայաստանի ինտերնետային միությունը (ՀԻՄ) սկսեց արդեն դոմեյնների արգելափակումը, ինչի հետևանքով .am տիրույթում գտնվող արգելափակված կայքերը դարձան անհասանելի թե՛ Հայաստանում, թե՛ երկրի սահմաններից դուրս: Այդ կայքերն ընթերցելու միակ հնարավորությունը դրանց իրական IP հասցեով այցելելն էր, օրինակ՝ a1plus.am կայքը հասանելի էր հետևյալ IP հասցեով՝ 75.125.179.218:

Քանի որ արտակարգ դրության ժամանակ այդ կայքերն իրենց խմբագիրների կամքով չէին թարմացվում, ապա ամենայն հավանականությամբ ԱԱԾ–ն դիմել էր այս քայլերին, որպեսզի արտաքին աշխարհի այցելուների համար ինտերնետից հեռացվեին նույնիսկ արխիվային նյութերը:

Հայաստանի ինտերնետային միության խորհրդի նախկին անդամ Դավիդ Սանդուխչյանը մեզ հայտնեց, որ առաջին շրջանում այս գործողությունների մասին տեղյակ չեն պահել ՀԻՄ–ի խորհրդի անդամներին:

Մարտի 5-ին արգելափակվեց youtube.com կայքը, քանի որ այնտեղ ընդդիմությունը սկսել էր տեղադրել մարտի 1-ի դեպքերի վերաբերյալ տեսանյութեր:

Քանի որ այս անգամ իշխանությունները սկսեցին ֆիլտրել ոչ հայկական կայքը, նրանց քայլը արձագանք ստացավ միջազգային լրատվամիջոցներում: Բլոգներում և ֆորումներում տարածվեց տեղեկություն, որ Միջազգային ինտերնետային միությունը (ISOC) դիմել է ՀԻՄ-ին, հայտնելով, որ այն խախտում է իր պարտավորությունները և կարող է զրկվել միջազգային անդամակցությունից:

Որպես հետևանք՝ հայկական կազմակերպությունը կզրկվեր .am տիրույթում դոմեյնների գրանցման իրավունքից:

Նույն օրը քաղաքացիները սկսեցին ձեռնարկել գործնական միջոցներ՝ ինտերնետային շրջապատումից ելքեր գտնելու համար: Բացվեց azathayastan.googlepages.com բլոգը, որտեղ տեղադրվում էին նյութեր արգելափակված Armenia Today և «Ազատություն» ռադիոկայանի կայքերից:

«Ազատություն»-ը տեղադրում էր իր նյութերը նոր հասցեով azatutyun.eu:

Մի քանի պրովայդերներ որոշ ժամանակով փակեցին ռուսական Regnum.ru գործակալության կայքը (ստուգվել են web.am, netsys):

Այս ընթացքում ինտերնետից օգտվողների շրջանում սկսեցին տարածվել տարբեր տեխնիկական միջոցներ, որոնք թույլ էին տալիս այցելել փակված կայքերը (անոնիմայզերներ, արտաքին պրոքսիներ):

Մարտի 8-ին ՀԻՄ-ն, ի վերջո պաշտոնապես հայտարարեց, որ մի շարք կայքերի զրկել է իրենց դոմեյնային անուններից (հայտարարությունը տեղադրվեց կազմակերպության կայքում):

Մարտի 19-ին մասնակիորեն արգելափակվեց xosqi-azatutyun.livejournal.com բլոգը, որտեղ հայերը արտասահմանից տեղադրում էին նյութեր Հայաստանում չբացվող կայքերից: Բլոգերների հետաքննությունը հայտնաբերեց, որ արգելափակումը կատարվում է միայն XTER.net պրովայդերի կողմից:

Մարտի 21-ին արգելափակումները վերացան: Օրվա առաջին կեսին «Հայկական Ժամանակ» կայքի հասցեում դեռևս տեղադրված էր թերթի հոսթինգը տրամադրող Web.am պրովայդերի կայքէջը:

Այս ամենը երկարաժամկետ հետևանքներ թողեց Հայաստանի վրա:

Տարիներ շարունակ այս դեպքերից հետո իշխանությունները խուսափում էին ինտերնետային արգելափակումներից, քանի որ վերջնական փորձը ցույց տվեց, որ հանրությունը շատ օպերատիվ կերպով գտավ շրջանցումների հնարավորություններ, իսկ այն տեղեկատվությունը, որը պետք է քողարկվեր, հակառակը՝ ավելի լայն տարածում ստացավ:

Փաստացի, հաջորդ ինտերնետային արգելափակումը եղավ 2016-ի հուլիսին. ՊՊԾ գրավման առավոտը Ֆեյսբուքը արգելափակվեց մոտ մեկ ժամով: Ընդ որում՝ արգելափակումը ազդել էր ոչ բոլոր օգտատերերի վրա: Արգելափակումների անարդյունավետությունը հանգեցրեց այն բանի, որ նույնիսկ 2018-ի հեղափոխության օրերին փորձ չարվեց սահմանափակել համացանցը:

COVID-19-ի ազդեցությունները

2020-ի գարնանից մինչև աշուն գործող արտակարգ դրությունը և կարանտինը յուրահատուկ ազդեցություն ունեցան ինտերնետի վրա:

Արտակարգ դրության առաջին օրերից հայտարարվեց գրաքննություն, որը վերաբերում էր կորոնավիրուսի մասին տեղեկատվությանը. այն չպետք է հակասեր պաշտոնականին:

Ընդ որում՝ գրաքննության կանոնները վերաբերում էին ոչ միայն լրատվամիջոցներին, այլ նաև սոցցանցային օգտատերերին: Ոստիկանությունը գործում էր ուժային և հաճախ անտրամաբանական մեթոդներով: Օրինակ, Տիգրան Խզմալյանի տուն այցելել էին գիշերը, որպեսզի պահանջեն հեռացնել մի ֆեյսբուքյան գրառում, որն իրականում չէր հակասում ցենզուրայի պահանջներին:

Գրաքննությանը գումարվեցին մարդկանց տեղաշարժը վերահսկելու փորձերը՝ կոնտակտավորներին բացահայտելու համար: Առաջին փուլում հանրությանը առաջարկվեց ներբեռնել դրա համար ստեղծված հատուկ հավելված: Այդ հավելվածի առաջին տարբերակը պարունակում էր վնասակար ծրագիր, ինչը կարելի է ստուգել նաև այսօր: Հետագայում այդ հավելվածը փոխարինվեց անվտանգով:

Ավելի ուշ գործարկվեց կենտրոնացված համակարգ, որը մեկ տեղում էր հավաքագրում բոլոր երեք բջջային օպերատորներից ստացված տվյալները բաժանորդների մասին: Հավաքագրվում էին օնլայն ռեժիմով հեռախոսազանգերի և կարճ հաղորդագրությունների մետատվյալները: Բացի դրանից՝ ստացվում էին մարդկանց տեղաշարժի տվյալները՝ հիմնված բջջային հեռախոսների և կայանների կապի վրա: Համակարգը գործեց մինչև սեպտեմբերի կեսը: Այն վերահսկում էր ԱԱԾ-ն, իսկ ստեղծողը անհայտ մասնավոր ընկերություն էր:

Հանրության մի շարք հարցեր այդպես էլ պատասխաններ չստացան.

ա. Չտրվեց երաշխիք, որ համակարգը չի օգտագործվել այլ նպատակներով, օրինակ, կոնկրետ մարդկանց և նրանց կապերը բացահայտելու:

բ. Այդպես էլ հստակ չասվեց, թե ով է ստեղծել համակարգը:

գ. Ըստ օրենքի՝ արտակարգ դրության ավարտին համակարգով հավաքագրված տվյալները պետք է ոչնչացվեին: Քանի որ ոչ մի անկախ վերահսկողություն համակարգի հանդեպ չի եղել, չկա ոչ մի երաշխիք, որ տվյալները ոչնչացվել են, ավելին՝ որ համակարգն այլևս չի գործում:

COVID-19-ի ազդեցությունները Արցախյան պատերազմը և ռազմական դրությունը

Հայաստանում ռազմական դրությունը, որը հայտարարվեց Արցախյան պատերազմի սկսվելու պահից լրջագույն ազդեցություն թողեց նաև համացանցի վրա:

Անմիջապես հայտարարվեց գրաքննության ռեժիմ, որը գործում էր թե՛ լրատվամիջոցների, թե՛ սոցցանցերի օգտատերերի հանդեպ: Գործում էր շատ կոշտ տուգանքների ռեժիմ: Այսպես, օրինակ, Ոստիկանությունը հայտնել էր միջանկյալ արդյունքների մասին. հոկտեմբերի 19-ի ժամը 16.00-ի դրությամբ հայտնաբերել է արգելված հրապարակումների 108 դեպք, որոնցից 26-ը՝ լրատվական գործունեություն իրականացնողների, 82-ը՝ լրատվական գործունեություն չիրականացնող անձանց կողմից:

Ներդրված կանոնները բավականին խիստ էին:

«Հայաստանի Հանրապետությունում ռազմական դրություն հայտարարելու մասին» կառավարության որոշմամբ սահմանվել էին հրապարակումների և հաղորդումների իրականացման մի շարք արգելքներ: Մասնավորապես, ՀՀ և ԱՀ ընթացող մարտական գործողություններով պայմանավորված քաղաքացիական անձանց (խմբերի) շարժի, մարտական գործողությունների հետևանքով պատճառված կորուստների և վնասների վերաբերյալ հաղորդումների՝ հրապարակումների, տեղեկատվական նյութերի, հարցազրույցների և դրանց հետ անմիջականորեն առնչվող այլ տեղեկությունների հրապարակային տարածումը, փոխանցումը, ներառյալ՝ ինտերնետային կայքերում և սոցիալական ցանցերում, այսուհետ կատարվելու է բացառապես պետական մարմինների կողմից տրամադրված պաշտոնական

տեղեկատվության հղումով՝ ամբողջությամբ արտացոլելով պաշտոնական տեղեկատվությունը (առանց խմբագրման):

Արգելվում էր պետական և տեղական ինքնակառավարման մարմինների ու պաշտոնատար անձանց՝ ռազմական դրության իրավական ռեժիմի և պետական անվտանգության ապահովմանը առնչվող գործողությունները (այդ թվում՝ ելույթները, հրապարակումները) քննադատող, հերքող, դրանց արդյունավետությունը կասկածի տակ դնող կամ որևէ այլ կերպ արժեզրկող հաղորդումների հրապարակումը:

Արգելվում էր ՀՀ և ԱՀ պաշտպանունակության ու անվտանգության դեմ ուղղված քարոզչությունը, այդ թվում՝ ՀՀ և ԱՀ պաշտպանունակությունը կասկածի տակ դնող հաղորդումների հրապարակումը: Այդ կանոնների խախտման դեպքում լրատվական գործունեություն իրականացնողները տուգանվում էին՝ 700 հազարից 1 միլիոն դրամի չափով:

Վարչական տույժի նշանակումից հետո հրապարակումն անհապաղ չվերացնելու դեպքում տուգանքը 1 միլիոնից 1 միլիոն 500 հազար դրամ էր: Վարչական տույժ նշանակելու օրվանից հետո կրկին կատարելու դեպքում լրատվական գործունեություն իրականացնողը տուգանվում էր նախկինում նշանակված տուգանքի կրկնապատիկի չափով: Այդ կանոնների խախտումը լրատվական գործունեություն չիրականացնողների կողմից առաջացնում է տուգանքի նշանակում 300 հազարից 700 հազար դրամի չափով:
Հրապարակումն անհապաղ չվերացնելու դեպքում լրատվական գործունեություն չիրականացնող անձը կտուգանվի 700 հազարից 1 միլիոն դրամի չափով: Վարչական տույժ նշանակելու օրվանից հետո կրկին կատարելու դեպքում լրատվական գործունեություն չիրականացնող անձը կտուգանվի նախկինում նշանակված տուգանքի կրկնապատիկի չափով:

Գործի դրվեցին նաև ինտերնետի հասանելության արգելափակումներ: Առաջինը՝ հոկտեմբերի 1-ի դրությամբ, արգելափակվեց TikTok սոցցանցը: Արգելափակումը մասնակի էր. մի շարք օգտատերերի մոտ այն բացվում էր, չնայած դժվարությամբ: Պաշտոնապես այդպես էլ չընդունվեց արգելափակման փաստը: Քանի որ արգելափակումը լիարժեք չէր, ապա բարդ է նաև ֆիքսել, թե երբ այն դադարեց ամբողջությամբ գործել: Ամենայն հավանականությամբ, արդեն հոկտեմբերի ավարտին սոցցանցը լիարժեք գործում էր ՀՀ տարածքում:

Հոկտեմբերի երկրորդ հատվածում ներդվեցին ավելի խիստ արգելափակումներ: Հայաստանի տարածքում անհասանելի դարձան բոլոր .az և .tr դոմենային տիրույթի կայքերը: Ո՞րն էր իմաստը արգելանքի տակ դնելու ողջ ադրբեջանական և թուրքական համացանցային տիրույթը հայտնի չէ. այս դեպքում նույնպես պաշտոնապես ոչ մի հայտարարություն չի արվել: Պատերազմի ավարտից հետո արգելափակումները վերացվեցին:

Փաստացի, 2020-ը ամենաբարդ տարին է եղել Հայաստանի ինտերնետի պատմության մեջ: Սահմանափակումների և արգելափակումների մի մասը օբյեկտիվ պայմաններից են բխել: Սակայն պետությունը հաճախ չի ստեղծել հանրային վերահսկողության գործիքներ, իսկ որոշ դեպքերում պարզապես չի էլ իրազեկել հանրությանը սահմանափակումների մասին:

Եվ այս պահին դեռ հարց է՝ կհաջողվի՞ քաղաքացիական հասարակությանը և իշխանություններին վերադարձնել Հայաստանը ազատ ինտերնետով երկրների շարք 2021-ին, թե՞ այս հարցը կհետաձգվի մինչ այն ժամանակը, երբ կստեղծվեն ավելի բարենպաստ քաղաքական և հասարակական պայմաններ:

ԼՐԱՏՎԱՄԻՋՈՑՆԵՐԸ ԵՎ ԹՎԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ. ՀԱՅԱՍՏԱՆԻ ՓՈՐՁԸ

Հայաստանում լրատվամիջոցները տարիներ շարունակ եղել են կիբեր հարձակումների թիրախ: Դեռ 2000-ականների սկզբից լրատվականները հաքերային հարձակումների էին ենթարկվում ադրբեջանական խմբավորումների կողմից:

Մինչև տասականները ակտիվ հարձակումներ էին իրականացնում նաև թուրքական հաքերային խմբերը՝ հիմնականում պայմանավորելով դրանք Ցեղասպանության հետ կապված թեմաներով. ամեն ապրիլի 24-ին կամ որևէ երկրում Եղեռնի ճանաչման թեմայի բարձրացմանը զուգընթաց:

Արդեն տասականներին իրավիճակը շատ ավելի լրջացավ, քանի որ Ադրբեջանում ձևավորվեցին հաքերային թիմեր, որոնք աշխատում էին հիմնականում հայաստանյան ուղղությամբ:

Այդ թիմերը ունեին երկու թիրախային խմբեր՝ պետական կայքերն ու լրատվամիջոցները:

2012-ին Ռամիլ Սաֆարովին Հունգարիայից արտահանձնմանը հետևած Երևանի և Բաքվի միջև դիվանագիտական և քարոզչական հակամարտությանը հաջորդեց լայնամասշտաբ հաքերային գրոհ Հայաստանի դեմ: Գրոհի ընթացքում ոչ միայն իրականացվեցին ավանդական հարձակումներ կայքերի վրա, այլ կիրառվեցին DDoS տիպի լայնածավալ հարձակումներ:

Այդ, ինչպես նաև դրան հաջորդած մի շարք DDoS հարձակումների քանակական ուժգնությունը թույլ է տալիս ենթադրել, որ հարձակումները կատարվում էին պետական հովանավորությամբ: Այս անգամ առաջնային թիրախը հենց լրատվամիջոցներն էին, ինչին հաջորդեցին նաև հարձակումներ պետական կայքերի վրա:

Նույն 2012-ի ընտրություններից առաջ դրվեց նոր վատ ավանդույթների սկիզբ. կիրառվեցին առաջին ներքաղաքական հաքերային հարձակումները: Դրանից հետո պարբերաբար լրատվականները հանդիսանում էին DDoS հարձակումների թիրախ: Սակայն ներքաղաքական հարձակումներն ունեն յուրահատկություններ, որոնք հարձակումները դարձնում են դժվար ուսումնասիրելի:

Նման հարձակումների մի մասը պարզապես չի բարձրաձայնվում՝ զանազան ներքաղաքական և տնտեսական նկատառումներից ելնելով:

Մյուս հատվածը, ենթադրաբար, իրականությանը չի համապատասխանում և օգտագործվում է խմբագրությունների կողմից քաղաքական շահարկումների կամ հանրային փիառի համար: Բազմաթիվ բարձրաձայնած հարձակումների դեպքեր չեն քննվել, անկախ փորձագետների կողմից չեն հաստատվել:

Իսկ եղած դեպքերը չեն հանգեցրել բացահայտումների, որոնք թույլ կտան որևէ եզրահանգումներ անել:

Վերլուծությունը հիմնականում արվում է ենթադրությունների մակարդակով, որպես սկզբունք վերցվում է հին և պարզ cui prodest: Ավելին, գոյություն ունի հնարավորություն, որ ներքաղաքական հարձակումները կարող են քողարկվել ադրբեջանական հաքերային թիմերի կողմից հարձակումների տակ, քանի որ դրանք հիմնական և ամենահաճախ հանդիպող տարբերակն են:

Ամենալուրջ հարձակումներին Հայաստանը, ինչպես նաև հայաստանյան մամուլը ենթարկվեց 2020-ին: Հուլիսի Տավուշյան դեպքերի և Արցախյան պատերազմի ժամանակ մամուլը հանդիսանում էր հիմնական թիրախներից:

Սովորաբար ռազմական գործողությունները սկսելու պահից լրատվական կայքերը հայտնվում են DDoS հարձակումների տակ: Սա արդեն կանոն է, որը սկսել է ձևավորվել վերոնշված 2012-ի դեպքերից հետո: Եվ հենց 2012-ի և դրան հաջորդած դեպքերի հետևանք է, որ հայաստանյան լրատվամիջոցների մեծ մասն արդեն օգտագործում է պաշտպանողական համակարգեր, հիմնականում Cloudflare:

Ամեն դեպքում, միայն պաշտպանական համակարգի միացումը չի լուծում խնդիրը. հարձակվողները տարբեր հնարքներ են կիրառում և անհրաժեշտ է լինում մասնագիտական միջամտություն:

Արցախյան պատերազմի դեպքում DDoS հարձակումները ադրբեջանական կողմից իրականացվում էին անընդհատ ռեժիմով: Հարձակման տակ են եղել գրեթե բոլոր հայաստանյան լրատվականները: Ընդ որում՝ հարձակումներն իրականացվել են անընդհատ ուղղությունների փոփոխություններով, ինչը պահանջում էր պաշտպանության տեսանկյունից նույնպես անընդհատ ուշադրություն և միջամտություն:

Օրինակ, Ադրբեջանի գիտությունների ակադեմիայից աշխատում էին հայկական կայքերի դեմ (Նկարը Պապյան Արթուրի Թվիթերից).

	Date	Action taken	ASN	IP address
>	21 Oct, 2020 18:40:04	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:03	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:03	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:03	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:03	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:02	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:02	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:02	Block	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:02	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:02	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:02	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:01	Challenge	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:01	Block	AS202993 -IIT	185.147.24.81
>	21 Oct, 2020 18:40:01	Challenge	AS202993 -IIT	185.147.24.81

Մուրադյան Ռուբենը հայտնում էր, որ լրատվամիջոցներին կառավարությունից հորդորում էին պարզապես արգելափակել Ադրբեջանից և Թուրքիայից մուտքը:

Սակայն, ադրբեջանական և թուրքական IP հասցեներն ամբողջական արգելափակելը ճիշտ լուծում չէ, քանի որ նման պահերին դիտվում է իրական օգտատերերի կտրուկ աճ՝ դեպի հայկական լրատվականներ: Բացի դրանից, հաքերներն ակտիվ օգտվում են VPN, TOR թրաֆիկից՝ քողարկելով Ադրբեջանի հատվածից եկող հարձակումները:

Նաև բազմաթիվ են հարձակումներ, որոնց իմաստն է կայքի վրա տեղադրել կա՛մ կեղծ տեղեկատվություն, կա՛մ քարոզչական նյութ:

Այսպես, հենց Cloudflare հաշիվների վրա հարձակումը պատերազմի ժամանակ հանգեցրեց այն բանի, որ մի շարք հայտնի լրատվամիջոցների այցելուները վերահասցեավորվեցին այլ տեղ: Եվ իրար հետևից տասնյակ կայքեր միաժամանակ կոտրվեցին. մի մասը պարզապես անմիջական հարձակման հետևանքով:

Փաստացի, սեպտեմբերի 27-ին հայաստանյան մամուլի հիմնական հատվածը կարճ ժամանակով, բայց հանվեց շարքից: Ցանկում էին, օրինակ, հետևյալ կայքերը.

http://1in.am

http://a1plus.am

http://armenpress.am

http://armtimes.com

http://blognews.am

http://hetq.am

http://mamul.am

http://mediamax.am

http://news.am

http://zhamanak.com

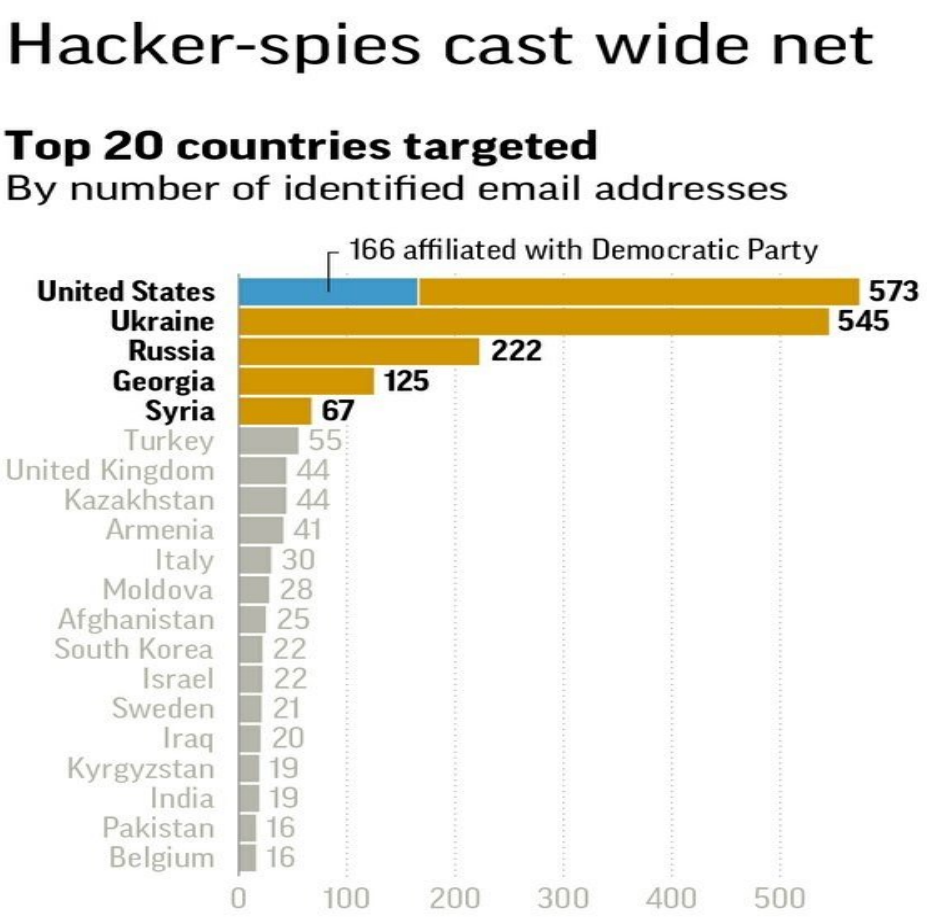
Ընդհանրապես վերջին տասը տարիների ընթացքում կոտրվել են տասնյակ հայաստանյան լրատվական կայքեր: Դրանց մեծ մասը հանդիսացել են ադրբեջանական և թուրքական հաքերային խմբերի թիրախ:

Թիրախ հանդիսանում են նաև լրագրողները: Կրկին, հիմնական արձանագրվող դեպքերը կապ ունեն ադրբեջանական հաքերների հետ: Չնայած՝ դեպքերի մեծ մասը խոսում է այն մասին, որ լրագրողները չեն հանդիսանում առանձնացված թիրախ: Հաքերները իրականացնում են զանգվածային ֆիշինգային հարձակումներ, որոնց զոհ հանդիսանում են նաև լրագրողները:

Սակայն, հայտնի են նաև թիրախային հարձակումների դեպքեր: Դրանց մեծ մասը չի հանրայնացվում, ինչի պատճառով հնարավոր չէ ունենալ հստակ վիճակագրություն:

Այսպես, 2020-ի վերջին հայտնվեց «Russia hackers pursued Putin foes, not just US Democrats» զեկույցը, այս անգամ այն հրապարակեց Associated Press-ը: Եվ կրկին մենք տեսնում ենք արդեն հարազատ դարձած Fancy Bear խումբը: Եվ կրկին պարզ է դառնում, որ լայնածավալ կիբերհարձակումների ցանկում, որը կատարվել է միանգամից մեծ քանակի պետությունների տարածքում, կան նաև հայաստանցիներ:

Ըստ ներկայացված քանակական ցանկի, Հայաստանից եղել է 41 թիրախ:



«Russia hackers pursued Putin foes, not just US Democrats» զեկույց

Հարձակումների հայաստանյան զոհերի ցանկը չի հրապարակվել, հայտնի է միայն, որ 2015-ին, Էլեկտրիկ Երևանի բողոքի ակցիաների ընթացքում հարձակման է ենթարկվել EVN Report-ի խմբագիր Մարիա Թիթիզյանը:

Մեր ունեցած տվյալների համաձայն՝ այդ 41 հոգու մեջ կան ինչպես լրագրողներ, այնպես էլ քաղաքագետներ և վերլուծաբաններ, որոնց բոլորին կարելի է նկարագրել որպես ավելի արևմտամետ:

Ներքին տվյալները, որոնք հայտնի են CyberHUB-AM կազմակերպությանը, թույլ են տալիս ասել, որ թիրախավորված հարձակումները հայաստանյան լրագրողների և լրատվամիջոցների դեմ, իհարկե, զանգվածային չեն, սակայն շատ ավելի մեծ ծավալ ունեն, քան դա հանրայնացվում է:

Եվ գնալով շատանում են դեպքերը, երբ կարելի է կասկածել պետական հաքերային խմբերին (state sponsored):

Նաև ակնհայտ է ներքաղաքական բնույթ կրող հարձակումների ակտիվության աճը:

ՀԱՅԱՍՏԱՆԸ
ՊԵՏԱԿԱՆ ՄԱԿԱՐԴԱԿՈՎ ԱՆՑԿԱՑՎՈՂ
ՀԱՔԵՐԱՅԻՆ ՀԱՐՁԱԿՈՒՄՆԵՐԻ ԹԻՐԱԽՈՒՄ

Եթե հետևում եք հայաստանյան մամուլին, ապա կիբեր հարձակումների հարցում կարող է ձևավորվել հստակ պատկերացում, թե հիմնական գործողությունները Հայաստանի բնակիչների, կազմակերպությունների դեմ իրականացնում են ադրբեջանական և թուրքական հաքերները:

Քանակական տեսանկյունից դա, կարծես թե, այդպես է: Եթե դիտարկենք վերջին տաս-տասնհինգ տարիները, ապա հարձակումների գերակշռող մասը իսկապես իրականացվել է ադրբեջանական և թուրքական հաքերային խմբերի կողմից: Միայն վերջին տարվա ընթացքում Ադրբեջանի և Թուրքիայի հաքերները կարողացան կոտրել մի քանի հազար հայկական հաշիվներ Ֆեյսբուքում և Ինստագրամում:

Մինչև 2009 թվականի հոկտեմբեր ամիսը, երբ ԱԱԾ-ն սկսեց վերահսկել Հայաստանի կիբերտիրույթի պետական հատվածը, ադրբեջանական հաքերային խմբավորումները տարին մի քանի անգամ զանգվածային հարձակումներ էին իրականացնում Հայաստանի Հանրապետության և Արցախի պետական կայքերի վրա: Երբ սկսվեց վերահսկողությունը, հաջողված հարձակումների թիվը կտրուկ նվազեց:

Սակայն, եթե խոսենք ոչ միայն զանգվածային հարձակումների, այլ թիրախավորված, կետային կիբեր գործողությունների մասին ընդդեմ պետական և ոչ պետական կարևոր կառույցների, ինչպես նաև անհատների, ապա կարելի է գտնել մի շարք հայտնի դեպքեր: Եվ այդ դեպքերի հետևում նշմարվում են պետության կողմից հովանավորվող (state sponsored) հաքերային խմբեր կամ հենց պետական համակարգեր:

Հայաստանի համար հիմնական սպառնալիք են հանդիսանում Ադրբեջանի հաքերային թիմերը: 2020 թվականի ամառվանից, դեռ մինչև Տավուշի մարտերը, սկսվեց կտրուկ ակտիվացում: Հունիսի և հուլիսի ընթացքում տեղի ունեցան տասնյակ հազարավոր մարդկանց անձնական տվյալների արտահոսքեր՝ որպես ադրբեջանական հաքերային թիմերի կողմից թիրախավորված հարձակումների հետևանք:

Արդեն Արցախյան պատերազմի ընթացքում հաքերներին հաջողվեց կոտրել մի շարք պետական կայքեր, ինչպես նաև ներթափանցել պետական փաստաթղթերի շրջանառության համակարգ, տիրանալ մի շարք բարձրաստիճան պաշտոնյաների էլեկտրոնային փոստերին և այլն:

Բացի դրանից՝ կոտրվեցին մի շարք լրատվամիջոցներ, իսկ գրեթե ողջ լրատվական և պետական հատվածը գտնվում էր անընդհատ և ուժգին DDoS հարձակումների տակ: Տվյալ գործողությունները դեռ պետք է վերլուծվեն ավելի մանրամասն: Իսկ եթե դիտարկենք հարձակումների պատմությունը, ապա այն ունի խորը արմատներ:
Ադրբեջանական հաքերային խմբերը Հայաստանի դեմ գործում են արդեն տասնամյակներ շարունակ:

Առաջին լուրջ գործողությունը հայկական կիբեր տարածքի դեմ իրականացվել է դեռ 2000 թվականի հունվարին: Այդ ժամանակ հայկական կայքերի վրա հարձակում իրականացրեցին երկու ադրբեջանական հաքերային թիմեր՝ Green Revenge и Hijack Team 187: Տվյալ թիմերի կապը պետական կառույցների հետ ապացուցված չէ: Սակայն այն, որ կիբեր ընդհարումների ժամանակ Ադրբեջանի անվտանգության կառույցները հաքերային խմբերի վրա կարողացան կիրառել լծակներ և դադարեցնել հարձակումները Հայաստանի վրա, խոսում է այն մասին, որ կապ գոյություն ուներ արդեն 2000 թվականին:

Տվյալ դեպքը վկայում է այն մասին, որ պետական մարմինները առնվազն տեղյակ էին հարձակում իրականացնող անձանց մասին կամ հնարավորություն են ունեցել անմիջական կապ հաստատել նրանց հետ:

Մինչև 2012 թվականը չկային բավարար հիմքեր կասկածելու, որ պետական մարմինների և բազմաթիվ հաքերային խմբերի միջև համագործակցություն է: Սակայն, 2011 թվականի նոյեմբերին ադրբեջանական հաքերային համայնքը համախմբվեց, գործող հիմնական խմբավորումներն ու անհատները միավորվեցին ասոցացված Anti-Armenia մեկ թիմում:

Արդեն 2012 թվականին, Ռամիլ Սաֆարովի Հունգարիայից արտահանձնմանն ու Երևանի և Բաքվի միջև դիվանագիտական և քարոզչական հակամարտությանը հետևեց լայնամասշտաբ հաքերային գրոհ Հայաստանի դեմ: Գրոհի ընթացքում ոչ միայն իրականացվեցին ավանդական հարձակումներ կայքերի վրա, այլ կիրառվեցին նաև DDoS տիպի հարձակումներ: Այդ գրոհի և դրան հաջորդած Հայաստանի վրա իրականացված մի շարք DDoS հարձակումների քանակական ուժգնությունը թույլ է տալիս ենթադրել, որ հարձակումները կատարվում էին պետական հովանավորությամբ, սակայն օգտագործվում էր կիբեր-վարձկանների հզորությունը:

Ադրբեջանն այդ պահին չուներ բավարար տեխնիկական հնարավորություններ նման հզորությամբ հարձակումներ իրականացնելու Հայաստանի կապի հանգույցների վրա: Ադրբեջանական հաքերային խմբավորումները նույնպես նման միջոցներ չունեին:

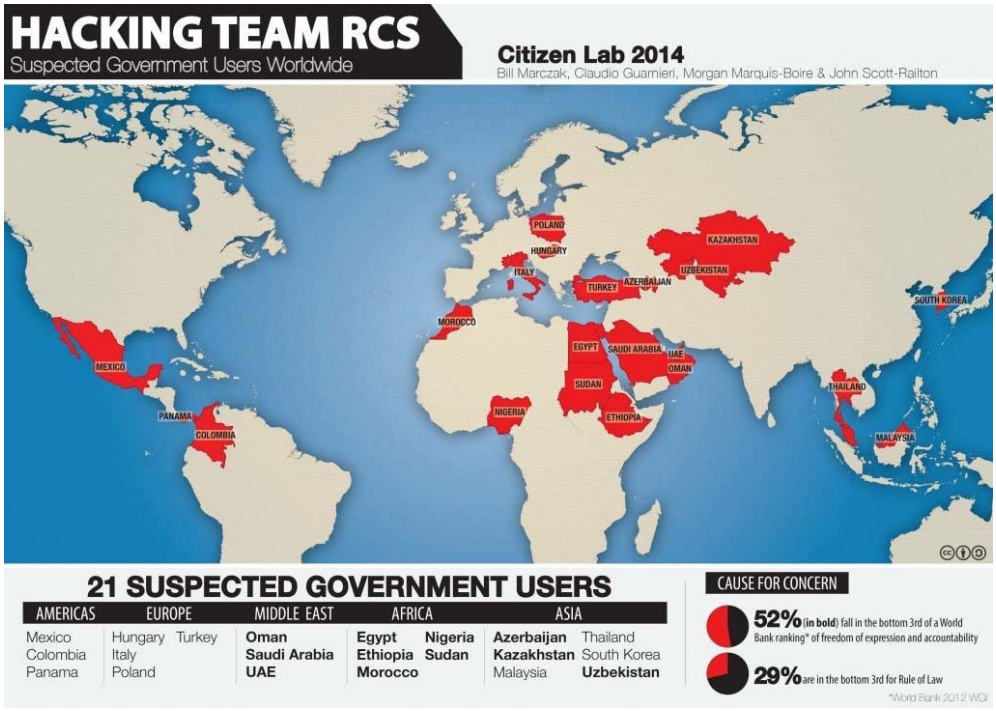
Նմանատիպ հզորությամբ հարձակումներ կիբեր-կրիմինալն իրականացնում է բավական մեծ գումարների դիմաց: Այսինքն, կարելի է ենթադրել, որ պետությունը հանդիսանում էր որպես պատվիրատու և հովանավոր, իսկ կատարողները՝ վարձկաններ էին:

Ենթադրաբար, հենց 2012 թվականի հայ-ադրբեջանական մեծ կիբեր ընդհարումից հետո Բաքվում սկսեցին մտածել սեփական, զուտ պետական մակարդակով գործող կիբեր միավորումներ ստեղծելու մասին:

2015 թվականի հուլիսին Wikileaks կազմակերպությունը հրապարակեց իտալական The Hacking Team հաքերային կազմակերպության ներքին նամակագրությունը, որը կորզվել էր այլ հաքերի կողմից: Այդ կազմակերպությունը ստեղծում և վաճառում է կիբեր լրտեսական ծրագրային ապահովում, որը թույլ է տալիս գաղտնալսել և վերահսկել համակարգիչներն ու հեռախոսները: Կազմակերպությունը վաճառում է իր արտադրանքը մի շարք երկրների իրավապահ մարմիններին: Որպես հետևանք, տվյալ ծրագրերն օգտագործվում են ոչ միայն հանցագործությունները բացահայտելու, այլև՝ ընդդիմադիրներին վերահսկելու նպատակով:

The Hacking Team-ի հիմնական լրտեսական ծրագրի՝ Remote Control System-ի կիրառումը Ադրբեջանի իշխանությունների կողմից արձանագրել է Citizen Lab կազմակերպությունը 2013 թվականի հուլիս-նոյեմբեր ամիսների ընթացքում: Հաշվի առնելով այն հանգամանքը, որ երկրում հոկտեմբերին կայացել են նախագահական ընտրություններ, կարելի է ենթադրել, որ համակարգի կիրառումը ունեցել է ներքաղաքական խնդիրներ լուծելու միտում:

Wikileaks-ի հրապարակած նամակագրությունը ցույց է տալիս, որ հետաքրքրությունը Ադրբեջանում առաջացել է 2011 թվականին, իսկ արդեն 2012 թվականին գործարքը կայացել է:



The Hacking Team-ի արտադրվող լրտեսական ծրագրի՝ Remote Control System-ի կիրառումը երկրների կառավարությունների կողմից: Ըստ Citizen Lab կազմակերպության

Հետագա բացահայտումները կապված են արդեն 2015 թվականի հետ: Amnesty International և մի շարք այլ կազմակերպությունների ուսումնասիրությունները թույլ են տվել գտնել ապացույցներ, որ 2015 թվականի նոյեմբերից ընդդիմադիր ադրբեջանցիների դեմ հատուկ ծառայությունները կիրառել են արդեն սեփական արտադրության վիրուսային ծրագրեր:

Ըստ մասնագետների, ընդդիմադիրներին ուղարկվող վիրուսային ծրագիրը թույլ է տալիս գողանալ գաղտնաբառերը, նկարել օգտվողի մոնիտորը, սակայն ծրագրային ապահովումը բավական պարզունակ է:

Կեղծ նամակ, որը ուղարկվել է մի շարք ադրբեջանցի ակտիվիստներին և որը պարունակում է վարակված ֆայլ: Ըստ Amnesty International-ի:

2017 թվականին արձանագրվել են DDoS հարձակումներ ընդդեմ ադրբեջանական ընդդիմադիր լրատվական կայքերի՝ Abzas.net, cumhuriyyet.net, azadliq.info : Այդ հարձակումների ժամանակ օգտագործվել են ադրբեջանական սերվերներ, որոնք կապակցված են կառավարության հետ, ինչը նշանակում է, որ Ադրբեջանի հատուկ ծառայությունները ձևավորում են սեփական համակարգ DDoS տիպի հարձակումներ իրականացնելու համար:

Իսկ այժմ դիտարկենք այլ երկրների հաքերային թիմերի կողմից հարձակումների մասին տեղեկատվությունը:

Եթե նայենք Էդվարդ Սնոուդենի բացահայտումներին, կտեսնենք, որ ԱՄՆ հատուկ ծառայությունների հետաքրքրությունը Հայաստանի հանդեպ միջինից բարձր է:

NSA բացահայտված համակարգերից մեկը, որը կոչվում է Boundless Informant, թույլ է տալիս քարտեզի վրա հետևել, թե որ երկրներից և ինչ ակտիվությամբ է ԱՄՆ այս հատուկ ծառայության կողմից կորզվում տեղեկատվությունը՝ բոլոր հնարավոր էլեկտրոնային շպիոնաժի միջոցներով:

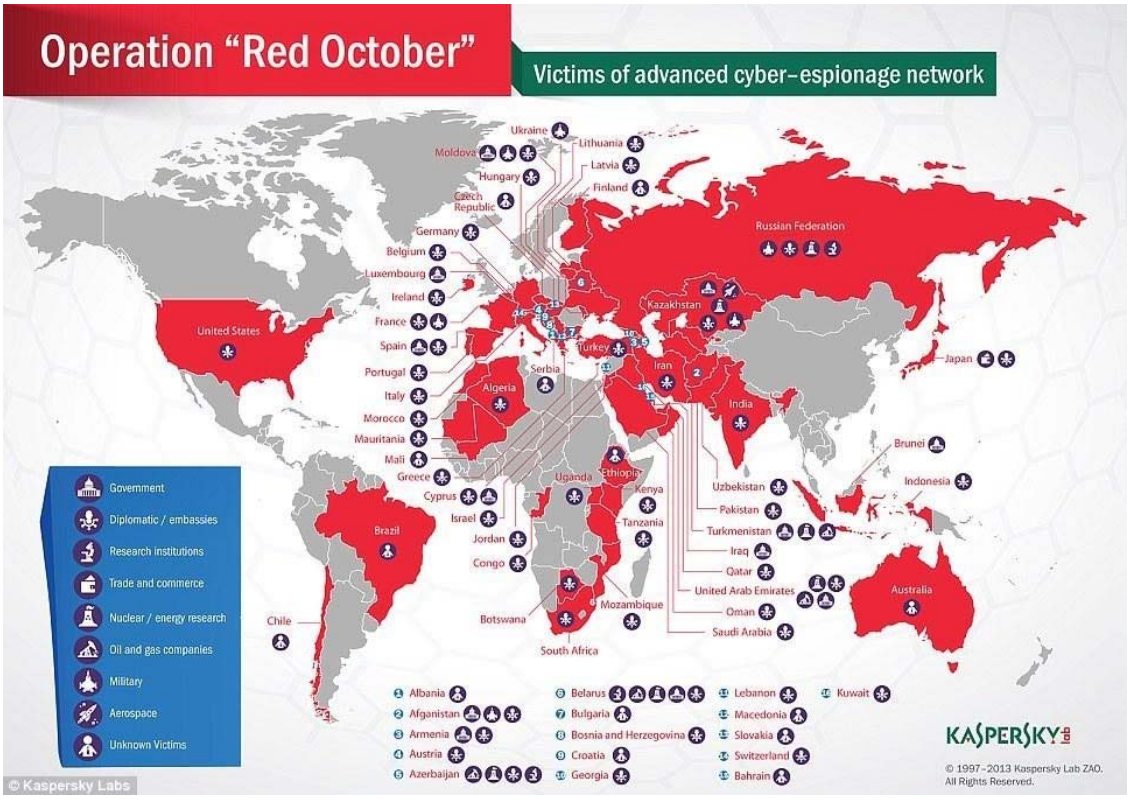
Սնոուդենի տրամադրած պատկերից երևում է, որ 2013 թվականի մարտ ամսվա ընթացքում միայն ԱՄՆ տարածքից ստացվել է մոտ 3 միլիարդ տարբեր տիպի տեղեկատվություն: Երկրները ներկայացված են ըստ այդ ամսվա ընթացքում դրանց հանդեպ NSA համակարգի ակտիվության, կանաչ գույնը վկայում է ցածր ակտիվության մասին, կարմիրը՝ հակառակը:

Այս պատկերի վրա Հայաստանը դեղին գույնի է՝ մոտավորապես Չինաստանի պես և Ռուսաստանից ավելի ակտիվ, ինչը խոսում է NSA-ի կողմից միջինից բարձր ակտիվության մասին:

2013 թվականին Կասպերսկի լաբորատորիայում հայտնաբերեցին սուպերլրտեսական վիրուս, որն անվանվեց Red October: Այն ներմուծվում էր պետական և ոչ պետական կարևոր ենթակառուցվածքներ և կատարում լայնածավալ կիբերլրտեսական գործողություններ՝ նույնիսկ վերականգնելով արդեն ջնջված ֆայլերը, որոնք կարող էին վիրուսի ստեղծողների համար լինել հետաքրքիր:

Պարզվեց, որ ծրագիրը գաղտնի գործել է հինգ տարի, և ոչ մի տեղ մինչ 2013 թվականը չէր հայտնաբերվել: Հայաստանը ամենավարակված երկրների տասնյակում էր, այստեղ Կասպերսկի լաբորատորիան հայտնաբերել էր տասը վարակման դեպք: Համեմատության համար՝ ամենավարակվածը Ռուսաստանն էր, և այստեղ արձանագրվել էր հարձակումների 37 դեպք:

Այդպես էլ պարզ չդարձավ, թե ով էր կանգնած Red October-ի հետևում: Անվտանգության մասնագետները ծրագրի մեջ առնվազն գտել էին ռուսերեն հետքեր, սակայն դրանք կարող էին միտումնավոր թողնված լինեին կոդի մեջ՝ ուշադրությունը շեղելու համար: Ավելին, Ռուսաստանը հիմնական թիրախն էր այս հարձակման: Ավելի հավանական է Չինաստանի հետքը: Օգտագործված տեխնոլոգիաներում կան հատվածներ, որոնք հղում են անում մի շարք ծրագրերի վրա, որոնք օգտագործվել են Թիբեթի ակտիվիստների դեմ և ենթադրաբար օգտագործվել են Չինաստանի հատուկ ծառայությունների կողմից:



FireEye կազմակերպությունը, որը զբաղվում է տեղեկատվական անվտանգությամբ, 2014 թվականի APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS? զեկույցում հայտնաբերել էր մի հաքերային խմբի լայնածավալ միջազգային ակտիվություն, որի թիրախներից մեկը նաև հայաստանյան զինվորականներն էին:

Խոսքը APT28 կամ Fancy Bear անվանումը կրող հաքերային խմբի մասին է, որը հիմա արդեն հայտնի է իր գործողություններով (հավանաբար, ազդեցություն է ունեցել ԱՄՆ ընտրությունների ժամանակ): Այս խումբը շատ մասնագետներ համարում են ռուսաստանյան պետական կիբեր խումբ, որը գործում է Կրեմլի շահերից ելնելով. «They compile malware samples with Russian language settings during working hours consistent with the time zone of Russia's major cities, including Moscow and St. Petersburg. They compile malware samples with Russian language settings during working hours consistent with the time zone of Russia's major cities, including Moscow and St. Petersburg»:

Ըստ FireEye-ի ուսումնասիրության, Fancy Bear-ի հաքերները ստեղծել էին կեղծ mail.rnil.am ֆիշինգային կայք, որը նմանակում էր Հայաստանի պաշտպանության նախարարության դոմեյնը՝ mil.am, և թույլ էր տալիս ֆիշինգային նամակների միջոցով թիրախավորել հայաստանյան զինվորականներին և իրենց դեմ իրականացնել կիբեր լրտեսական գործողություններ. «To target members of the Armenian military by hosting a fake login page»:

Թե ինչ վնաս են հասցրել հաքերները Հայաստանին, հայտնի չէ:

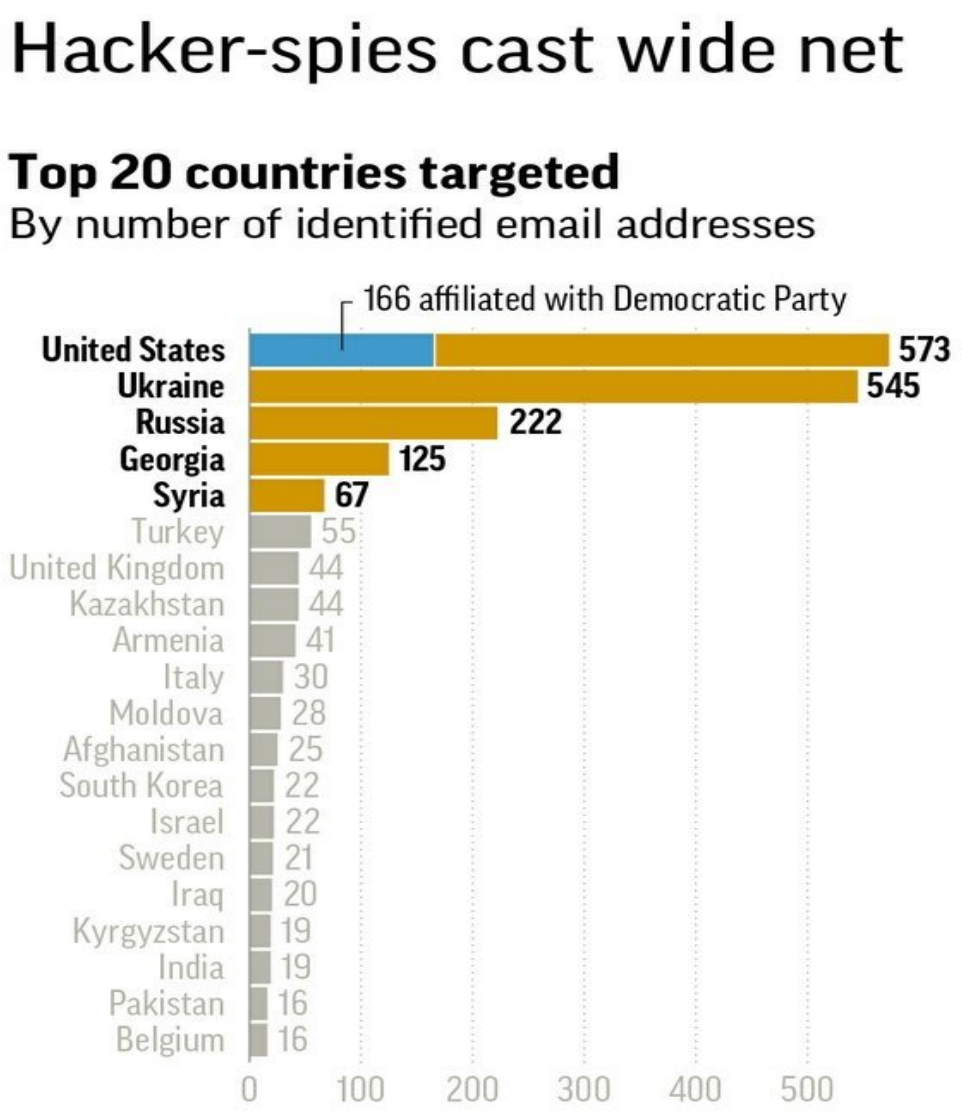
Rnil.am դոմեյնը պարբերաբար հայտնվել է տարբեր զեկույցներում, զանազան ֆիշինգային հարձակումներում, օրինակ, օգտագործվել է Bellingcat կազմակերպության դեմ, որն իրականացնում էր հետաքննություն MH17 խոցված ինքնաթիռի վերաբերյալ, ինչի հանդեպ մեծ հետաքրքրություն ունեին ռուսաստանյան իշխանությունները:

2017 թվականի մայիսին Citizen Lab կազմակերպությունը նոր բացահայտումներ արեց Fancy Bear հաքերային խմբի նոր գործողությունների մասին: Այս անգամ Հայաստանը նույնպես հայտնվեց զոհերի ցանկում: TAINTED LEAKS. Disinformation and Phishing With a Russian Nexus զեկույցից հայտնի է դառնում, որ այս անգամ թիրախ են դառել Հայաստանի կառավարության և բանակի ներկայացուցիչները: Ըստ կազմակերպության տվյալների,

Հայաստանը ֆիշինգային հարձակման հիմնական զոհ երկներից մեկն էր, ֆիշինգային հարձակումների մոտավորապես 3%-ը բաժին էր հասել հենց մեր հանրապետությանը:

Մեր ունեցած տվյալներով, հայաստանյան զոհերի ցանկում կան բարձրաստիճան զինվորականներ, ինչպես նաև դիվանագետներ:

Տարվերջին հայտնվեց «Russia hackers pursued Putin foes, not just US Democrats» զեկույցը, որն այս անգամ հրապարակեց Associated Press-ը: Կրկին տեսնում ենք արդեն հարազատ դարձած Fancy Bear խումբը: Եվ կրկին պարզ է դառնում, որ լայնածավալ կիբեր հարձակումների ցանկում, որը կազմվել է մեծ թվով պետությունների տարածքում, կան նաև հայաստանցիներ: Ըստ ներկայացված ցանկի, Հայաստանից եղել է 41 թիրախ:



Հարձակումների հայաստանյան զոհերի ցանկը չի հրապարակվել, հայտնի է միայն, որ 2015 թվականին էլեկտրիկ Երևանի բողոքի ակցիաների ընթացքում հարձակման է ենթարկվել EVN Report խմբագիր Մարիա Թիթիզյանը: Մեր ունեցած տվյալների համաձայն, այդ 41 հոգու մեջ կան ինչպես լրագրողներ, այնպես էլ քաղաքագետներ և վերլուծաբաններ, որոնց կարելի է բնութագրել որպես ավելի արևմտամետ:

Սա պետական կիբեր լրտեսության այն մի քանի դեպքերն են, որոնց մասին մենք տեղեկացված ենք: Հաշվի առնելով, թե վերջին տարիներին որքան արհեստավարժ է դարձել պետական հաքինգը, կարելի է եզրակացնել, որ Հայաստանի դեմ իրականացվող կիբեր գործողությունների մի մասը (միգուցե, զգալի մասը) դեռ բացահայտված չէ:

Նաև հասկանալի է, որ Հայաստանը հետաքրքրության թիրախ է գրեթե բոլոր խոշոր կիբեր հետախուզությունների համար:

ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆԸ ՀԱՅԱՍՏԱՆՈՒՄ... ԴԵՊԻ ՈՒ՞Ր ԵՆՔ ՄԵՆՔ ՇԱՐԺՎՈՒՄ

Տարիներ առաջ Հայաստանում անձնական տվյալների հարցը բացարձակ հետաքրքիր չէր ոչ հանրության լայն զանգվածներին, ոչ պետությանը: Ժամանակի ընթացքում իրավիճակը փոխվում է: Ցավոք, դրական փոփոխությունները դեպի ավելի լուրջ մտեցում այս հարցի հանդեպ ձևավորվում են բացասական փորձի հիման վրա: Արտահոսքերը միայն շատանում են ու մարդկանց համար սա վերջապես դառնում է մտահոգիչ:

Տեսնենք միայն հունիս-հուլիս 2020 ընթացքում եղած արտահոսքերի մի մասը:

Հունիսի 2. «Զնդան» ֆեյսբուքյան էջը հրապարակում է կորոնավիրուսից մահացածների ցուցակները:

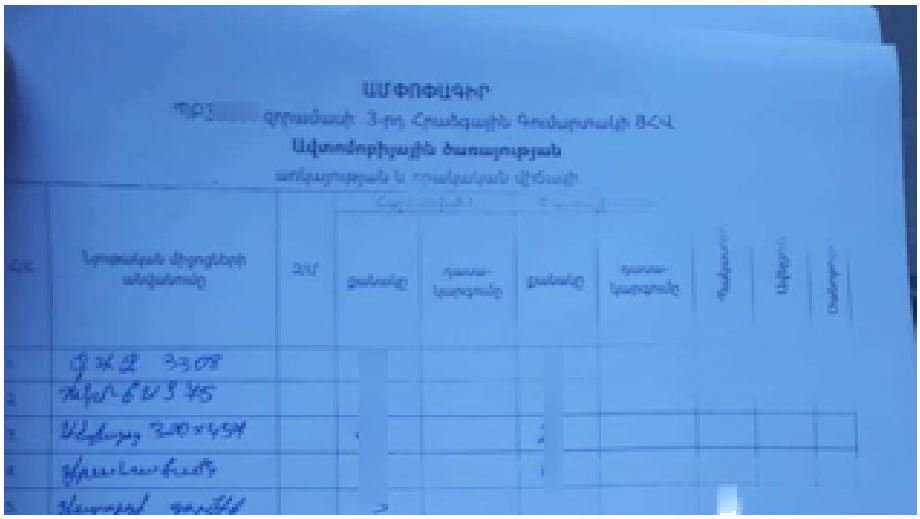
Հունիսի 11. Ադրբեջանական հաքերային խումբը, որն արդեն տարիներ շարունակ հարձակումներ է իրականացնում հայկական էլեկտրոնային փստերի և սոցցանցերի հաշիվների վրա, հրապարակում է 3000 ավելի տվյալ՝ կորոնավիրուսով վարակվածների և իրենց հետ կոնտակտ ունեցածների: Հրապարակվում են անուններ, ծննդյան թվեր, հասցեներ, հեռախոսահամարներ և անձնագրի սերիաներ:

Հունիսի 24-26. Նույն հաքերային խումբը հրապարակում է ևս մոտ 2000 հայաստանցու տվյալներ: Այս անգամ առանց անձնագրային տվյալների:

Հուլիսի 6. Ադրբեջանական հաքերային ֆորումում հրապարակվում են մի քանի հարյուր հայաստանցու անձնագրային տվյալներ: Ընդ որում դա անձնագրերի լուսանկարներ են, մի մասում մարդիկ նկարահանվել են անձնագրերի հետ: Նման նկարահանում պահանջում են, օրինակ, վարկային կամ նմանատիպ կազմկերպություններ, որոնց պետք է նույնականացնել մարդուն և համոզվել, որ նա չի օգտագործում մեկ այլ քաղաքացու անձնագիրը:

Սա արտահոսքի օրինակներից մեկն է: Անձնական տվյալների հատվածը ծածկված է

Հուլիսի 7. Ադրբեջանական հաքերները Ֆեյսբուքում հրապարակում են Արցախի Պաշտպանության բանակի զորամասի գույքագրմանը վերաբերող թերթիկներ, որոնք ներառում են նաև ավտոմոբիլային պարկի վերաբերյալ տեղեկություններ:



Սա արտահոսքի օրինակներից մեկն է: Տվյալների մի մասը տվյալ նկարում ջնջվել են:

Հուլիսի 30. Ցանցում տեղադրվում են 6000-ից ավելի հայաստանցու տվյալներ՝ էլեկտրոնային փոստ, հեռախոսահամար, հասցե, անձնագրի սերիաներ: Ամենայն հավանականությամբ, արտահոսքը եղել է բոնուսային քարտերից մեկի տվյալների շտեմարանից:

Վերահսկողություն և վիճակագրություն

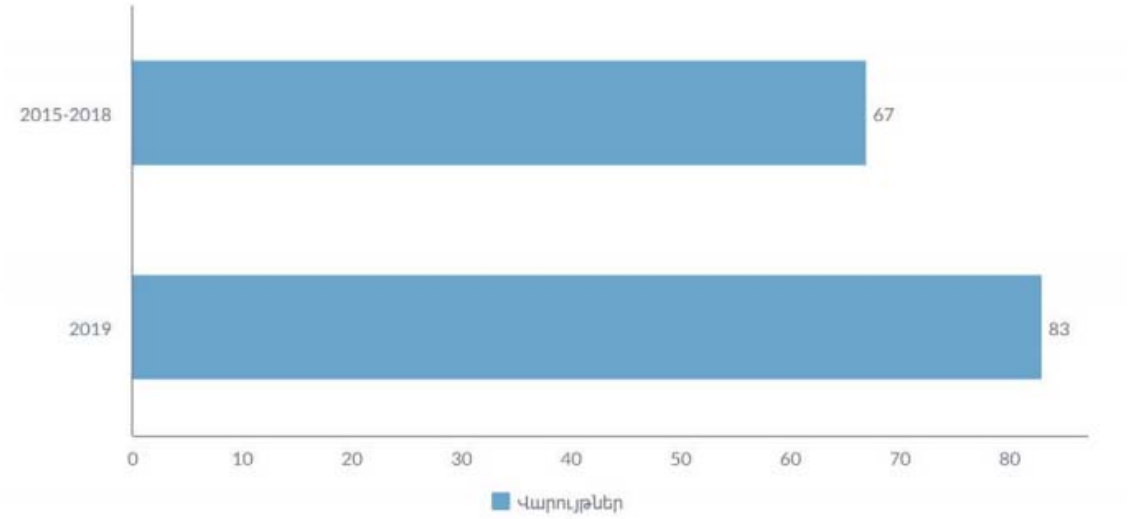
Անձնական տվյալների հարցում Հայաստանը անցել է հետաքրքիր ճանապարհ: 2002-ին ընդունվել, իսկ 2003-ին արդեն ուժի մեջ է մտել «Անհատական տվյալների մասին» օրենքը: Օրենքի ընդունումն ու հետագա կյանքը մնում են հեռու հասարակության գիտակցությունից, ինչպես նաև կառավարության գործառույթներից: Չստանալով միս ու արյուն, տվյալ օրենքը այդպես էլ մնում է թղթի վրա:

2015-ին ընդունվում ու ուժի մեջ է մտնում «Անձնական տվյալների պաշտպանության մասին» օրենքը: Սա արդեն պետության կողմից քիչ թե շատ գիտակցված քայլ էր: Ստեղծվում է Անձնական տվյալների պաշտպանության գործակալություն, որը գործում է Արդարադատության նախարարության համակարգում: Հետաքրքիր է պետականի և հասարակականի համագործակցության սկզբունքը, որը դրված է գործակալության հիմքում:

Ըստ օրենքի՝ «Անձնական տվյալների պաշտպանության լիազոր մարմնի ղեկավարը նշանակվում է հինգ տարի ժամկետով. . . իրավապաշտպան գործունեություն իրականացնող առնվազն հինգ հասարակական կազմակերպությունների համատեղ առաջարկությունների հիման վրա»:

Գործակալությունն ակտիվ գործունեություն է ծավալում, ներկայացված է սոցցանցերում, որտեղ նաև տրամադրում է խորհրդակցություն քաղաքացիներին:

Ըստ գործակալության հաշվետվության՝ 2019-ի ընթացքում Անձնական տվյալների պաշտպանության գործակալությունում քաղաքացիների դիմումների հիման վրա կամ գործակալության նախաձեռնությամբ հարուցվել է 83 վարչական վարույթ:



Համեմատության համար, գործակալության ստեղծումից ի վեր՝ 2015-2018-ի ընթացքում միասին հարուցվել է 67 վարույթ՝ 16-ով քիչ, քան միայն 2019-ին: 2015-ին հարուցվել է 2 վարույթ, 2016-ին՝ 11 վարույթ, 2017-ին՝ 21 վարույթ, 2018-ին՝ 33 վարույթ:

Ոճիր և պատիժ

Չնայած վարույթների թվերը աճում են, իրականությունը դրանից գրեթե չի փոխվում: Բերենք մի քանի հիմնական պատճառ.

ա. 200-500 հազար դրամ տուգանքները անձնական տվյալների խախտումների համար չափազանց մեղմ են: Օրինակ, անձնական տվյալներ մշակող կազմակերպության համար զուտ ֆինանսական տեսանկյունից, եթե մի կողմ թողնենք բիզնեսի պատասխանատվությունը, տեսականորեն ավելի շահավետ է մեկ անգամ վճարել տուգանք, քան վարձել մասնագետ և ամեն ամիս վճարել տուգանքին համարժեք գումար:

բ. Պետական կառույցներում տվյալների պաշտպանությունը պետք է դրվի ավելի ամուր հիմքերի վրա: Գործակալությունը ստեղծել է Պետական մարմինների կողմից անձնական տվյալների մշակման ուղեցույց, սակայն միայն մեկ ուղեցույցով հարցը չի լուծվում: Գործակալության գործառույթները չեն հերիքում ողջ պետական համակարգում ու դրան հարակից կառույցներում իրավիճակը շտկելու համար: Պետք է ունենալ ավելի ծավալուն հայեցակարգային մոտեցում, որը ենթադրում է կառավարության մակարդակով գործընթացների ներդրում, աշխատակազմի վերապատրաստում և վերահսկում:

գ. Հանրային կարծիքը անձնական տվյալների վերաբերյալ, չնայած փոխվում է, սակայն շատ դանդաղ: Հատկապես տվյալ ժամանակաշրջանում, երբ արտահոսքերի հավանականությունը միայն աճում է: Իսկ անչափահասների տվյալների վերաբերյալ տիրում է զանգվածային անգրագիտություն: Առանց հանրային իրազեկող արշավների հանրային կարծիքի բարելավումը հիմնականում հիմնվելու է միայն բացասական փորձի վրա:

դ. Հանրային իրազեկումը ենթադրում է նաև հստակ դեպքերի վերահսկում, դրանց հանրայնացում, հասկանալի վիճակագրության ներկայացում: Բացի դրանից, արդեն կատարված դեպքերը հետագայում չեն վերլուծվում հանրայնորեն, չի ներկայացվում համապատասխան մարմինների կողմից եզրակացություն, թե որն էր արտահոսքի պատճառը, ինչ է արվել դա բացառելու համար: Հանրությունը երբեք չի իմանում ոչ մեղավորների մասին, ոչ համապատասխան գործնական եզրակացությունների, ոչ շտկելուն ուղղված քայլերի (եթե, իհարկե, դրանք տեղի են ունենում):

ե. Ամենամեծ խնդիրներից մնում է պատահարների մասին հանրային իրազեկումը, ավելի շուտ դրանց բացակայությունը: Կան երկրներ, որտեղ արտահոսքի դեպքում կազմակերպությունը օրենքով է պարտավորված հանրայնացնել միջադեպը:
Տրամաբանությունը շատ պարզ է. մարդիկ պետք է տեղյակ լինեն, որ իրենց տվյալները բաց տեսքով հասանելի են բոլորին կամ հանցագործների ձեռքում են: Նման դեպքում մարդ ունենում է հնարավորություն միջոցներ ձեռնարկել:

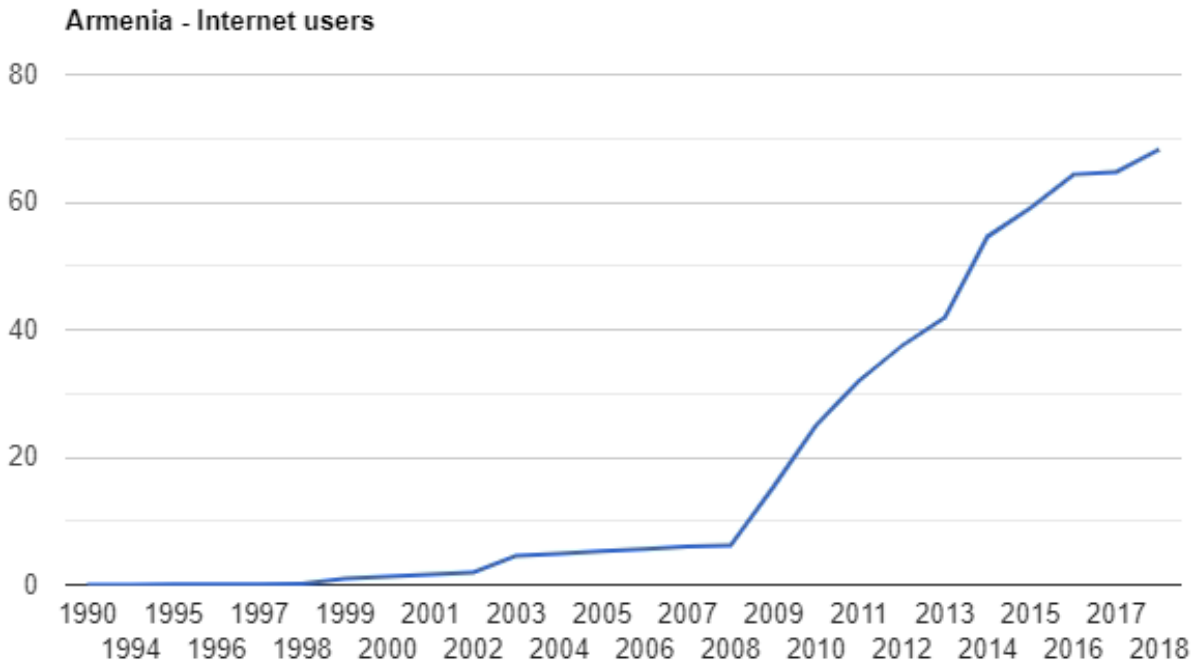
Այսպես, միայն ամառվա ընթացքում եղել է մոտ քսան հազար քաղաքացու անձնագրային տվյալների արտահոսք: Սակայն չկա մարդկանց դրա մասին տեղեկացնող մեխանիզմ: Այսինքն, մեծամասնությունը տեղյակ էլ չէ, որ իրենց տվյալներից կարող են օգտվել այլ անձիք: Երևի վերջին տարիների ընթացքում միայն մեկ դեպք է եղել, երբ մեծ արտահոսքից հետո կազմակերպությունն իր վրա պատասխանատվություն է վերցրել հանրայնորեն իրազեկել մամուլի միջոցով: Խոսքը ABCDomain հոսթինգի օգտատերերի գաղտնաբառերի արտահոսքն էր, ինչից հետո տեղի ունեցավ հայտարարություն կազմակերպության կողմից: Սա եզակի դրական օրինակն է:

Այս ամենի պարզ եզրակացությունը մեկն է. եթե չիրականացվեն լայնածավալ և բազմակողմանի գործողություններ, տվյալների արտահոսքերը միայն շարունակվելու են: Ավելի ճիշտ՝ աճելու են դրանց ծավալները:

ՍՈՑՑԱՆՑԵՐԸ ՀԱՅԱՍՏԱՆՈՒՄ.
ՀԻՄՆԱԿԱՆ ԽՆԴԻՐՆԵՐԸ ՕԳՏԱՏԵՐԵՐԻ ՀԱՄԱՐ

Սոցցանցերի պատմությունը Հայաստանում

Մինչև 2010 թվականը Հայաստանում ընդհանրապես դժվար էր խոսել ինտերնետից օգտվողների թվի մասին. դա բնակչության ընդամենը մի քանի տոկոսն էր: 2010 թվականի ավարտին Հայաստանում հայտնվեց քիչ թե շատ մատչելի և այն օրերի համար արագ ինտերնետ կապ և հենց այդ ժամանակվանից էլ սկսվեց սոցցանցերի ակտիվ օգտագործումը երկրում:



Եթե մինչ այդ առաջնային հարթակ էր հանդիսանում Livejournal բլոգային պլատֆորմը, որն ուներ սոցցանցային տարրեր, ապա տասականների սկզբից հենց սոցիալական ցանցերը եկան առաջին պլան:

Հատկապես արագ տարածվեց ռուսաստանյան Odnoklassniki (ok.ru) ցանցը, որը մինչև 2017 թվականի առաջին կեսը Հայաստանում ամենատարածված սոցցանցային հարթակն էր՝ 1,5 միլիոնանոց լսարանով:

1	youtube.com	Arts and Entertainment > TV and Video	+1
2	ok.ru	Internet and Telecom > Social Network	-1
3	facebook.com	Internet and Telecom > Social Network	=

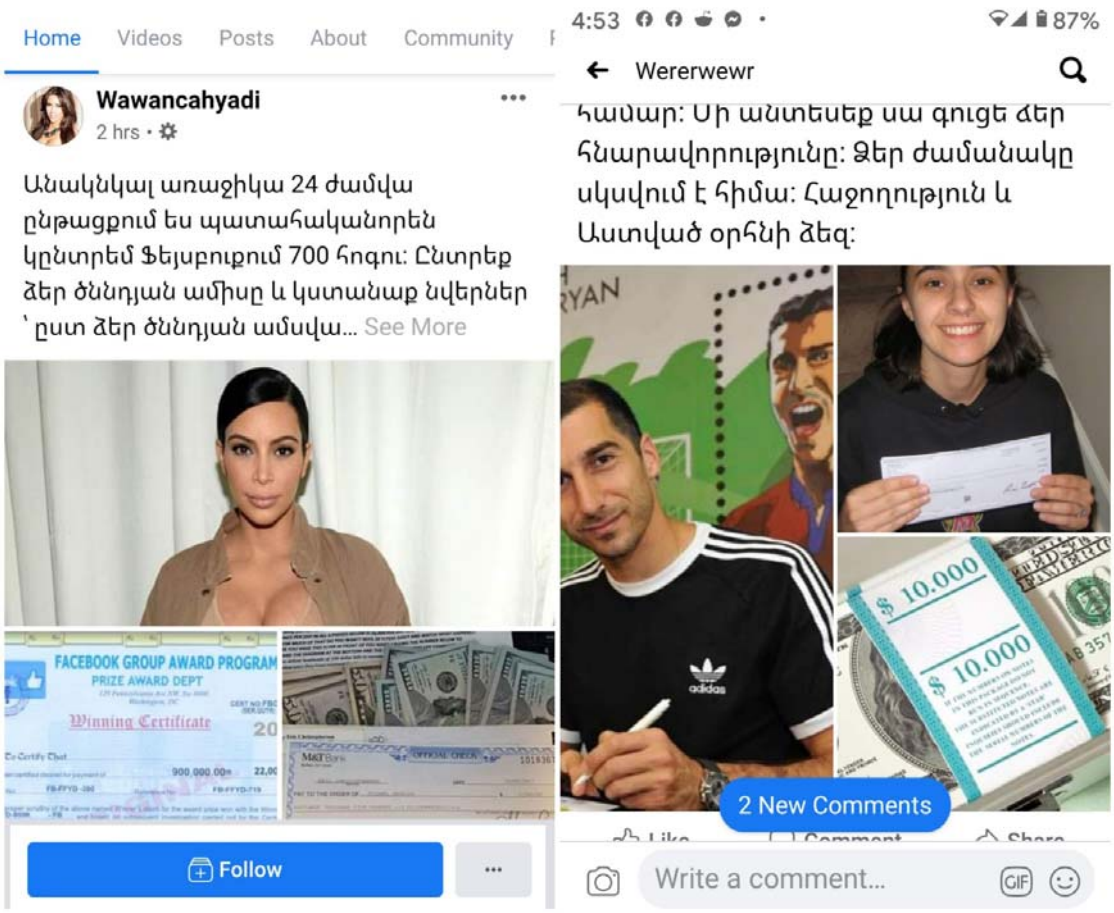
Similarweb պորտալի 2017 թվականի օգոստոսի տվյալները Հայաստանում ամենաայցելվող կայքերի վերաբերյալ ցույց են տալիս, թե ինչպես առաջին անգամ ok.ru-ն դիրքերը զիջում է YouTube-ին: Հետագայում արդեն առաջին պլան դուրս կգա Facebook-ը, իսկ 2018 թվականի հեղափոխությունը առիթ կդառնա քաղաքականացված լսարանի միգրացիայի՝ ok.ru-ից Facebook:

Կիբերհարձակումները

Հանրային և տնտեսական բազմաթիվ օգտակար հնարավորություններից բացի սոցիալական ցանցերը իրենց հետ բերում են նաև վտանգներ ինչպես անհատների, այնպես էլ ողջ հասարակության համար: Այդ վտանգներից են կիբեր-հարձակումները, որոնց հետևանքով մարդիկ կարող են կորցնել իրենց օգտահաշիվները սոցցանցերում, նրանց անձնական լուսանկարները կամ նամակագրությունը կարող են հանրայնացվել, նրանք կարող են ֆինանսական կորուստներ կրել:

Հարձակումներ իրականացնում են ինչպես միջազգային կիբեր-հանցագործ թիմերը, այնպես էլ անհատները:

Հայաստանում առավել հաճախ արձանագրվում են հարձակումներ, որոնք կապված են միջազգային զանգվածային կիբեր-խարդախությունների հետ, երբ թիրախավորվում են միլիոնավոր մարդիկ և հայաստանցիները այդ հարձակումների ընդամենը պատահական թիրախներից են:



Սակայն միջազգային կիբերկրիմինալը հաճախ իրականացնում է նաև տեղայնացված հարձակումներ: Այսպես՝ բանկային քարտի տվյալների հափշտակման շատ տարածված ձև գոյություն ունի, երբ հայտնիների անունից իբր գումար են առաջարկում բոլոր նրանց, ով մեկնաբանություն կգրի տվյալ գրառման տակ: Եվ այստեղ կարելի է տեսնել, թե ինչպես են շահարկվում հայտնի հայերի անունները, նրանց լուսանկարներով ու հայերեն տեքստով տարածվում են կեղծ գրառումներ: Ընդ որում նույնատիպ խաբեություն է իրականացվում նաև ուկրաինացիներին, վրացիներին թիրախավորելով:

Արձանագրվում են նաև դեպքեր, երբ խարդախությունը իրականացվում է հայաստանցիների կողմից: Տարօրինակ զուգադիպությամբ, նման խաբեությունների մեծ մասը իրականացվում է Odnoklassniki սոցցանցի միջոցով:

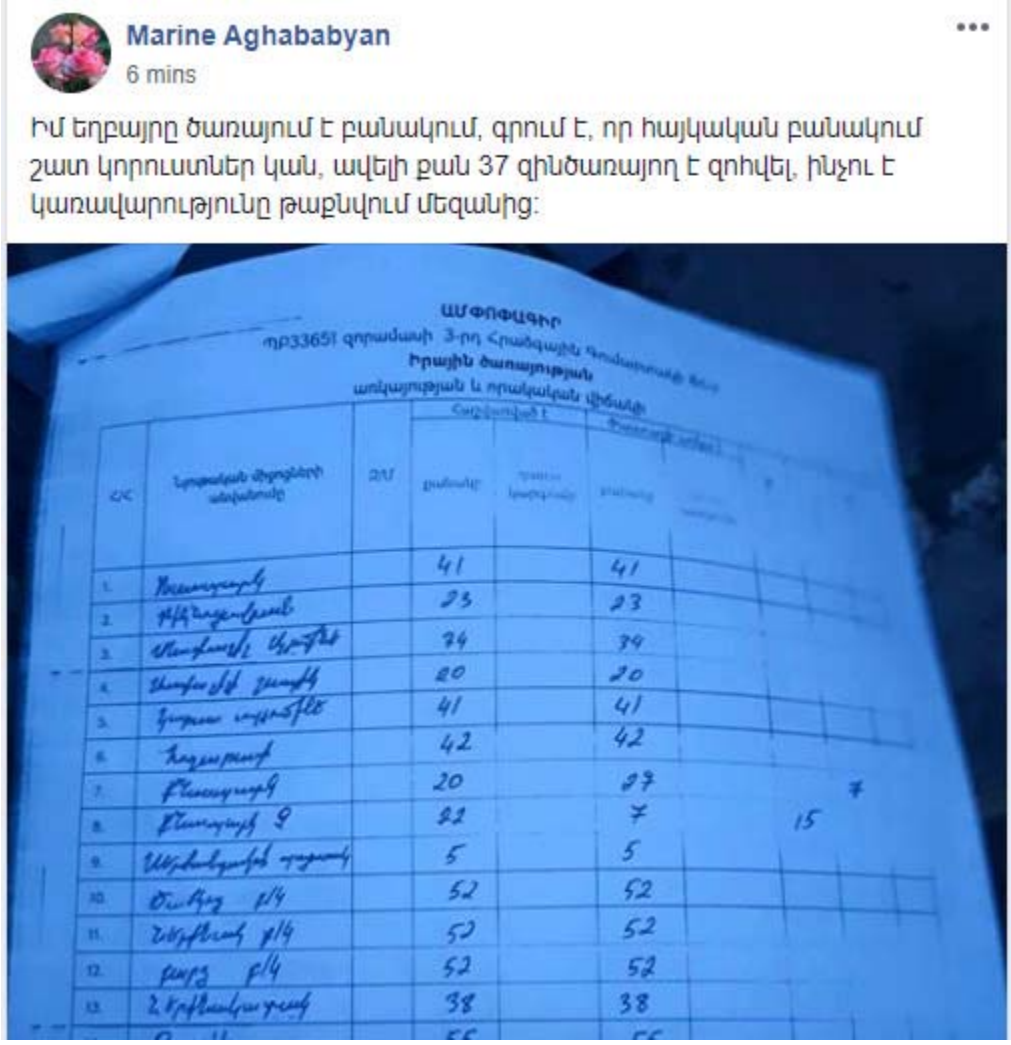
Առանձին տեղ են գտնում Ադրբեջանի հաքերային խմբերի կողմից զանգվածային հարձակումները հայաստանցիների և ընդհանրապես հայ օգտատերերի դեմ, երբ ֆիշինգային հարձակումների միջոցով փորձում են կորզել էլեկտրոնային փոստերի և սոցցանցերի հաշիվների գաղտնաբառերը: Տվյալ հարձակումները լինում են գրեթե միշտ և ուղղված են ռազմական գործողությունների ժամանակ տեղեկատվական պատերազմ վարելուն:

Պատերազմական վիճակի ազդեցությունը

Արդեն 2012, 2015 թվականների հայ-ադրբեջանական սրումները հանգեցրել էին լուրջ հակամարտություն սոցիալական ցանցերում, որը հիմնականում դրսևորվում էր ատելության խոսքի տարածմամբ: Սակայն Ապրիլյան պատերազմը և դրան հաջորդած սրացումները բերեցին լուրջ փոփոխությունների նաև այս ուղղությամբ: Ապրիլյանի ժամանակ Ադրբեջանի կողմից

առաջին անգամ զանգվածային կերպով կիրառվեցին կեղծ օգտահաշիվներ, որոնք ներկայանում էին որպես հայեր, սակայն կառավարվում էին ադրբեջանական կողմից և փորձում էին խուճապ առաջացնող տեղեկատվություն տարածել:

Հետագայում, արդեն 2017 թվականից, ադրբեջանական հատուկ ծառայությունների գործելաոճը փոխվեց. հաքերային խմբերը նախ կոտրում էին հայկական օգտատերերի հաշիվները, իսկ հետո արդեն այդ մարդկանց անունից տարածվում էր ապատեղեկատվությունը: Այս դեպքում կեղծիքը բացահայտելը դառնում է շատ ավելի բարդ, քանի որ ուսումնասիրողը տեսնում է, որ գործ ունի արդեն տարիներ գործող իրական հաշվի հետ, այլ ոչ թե վերջին օրերին բացված կեղծիքի:



Այստեղ մենք գործ ունենք հետաքրքիր դեպքի հետ: Մի կողմից հաքերները կոտրել են Հայաստանում բնակվողի հաշիվը: Բացի դրանից մեկ այլ անձի մոտից իր անձնական էլեկտրոնային փոստից կորզել են ռազմական բնույթի փաստաթուղթ: Եվ արդեն դա են տարածել կոտրած հաշվի միջոցով, ինչը շատ ավելի վստահելի է դարձնում տվյալ աղբյուրը:

Ադրբեջանական հաքերների թիրախային հարձակումները հայ օգտատերերի համար շատ վտանգավոր տիրույթ են դարձնում սոցցանցերը՝ համեմատելով միջին համաշխարհային վիճակագրության հետ:

Ատելության խոսք և զանգվածային արգելափակումներ

Ատելության խոսքը, անկասկած, այսօր խնդիր է բոլոր երկրների համար, քանի որ սոցցանցերը դարձել են հարթակ ամեն տեսակ ծայրահեղական խմբավորումների համար: Հայաստանում ատելության խոսքի տարածումը սոցցանցերում դարձել է մտահոգության առիթ թե՛ իշխանությունների, թե՛ ընդդիմադիրների, թե՛ լրագրողական կազմակերպությունների և լրատվամիջոցների համար: Ներքաղաքական դաշտում ատելության խոսքը արդեն տարիներ շարունակ դարձել է քաղաքական հակառակորդին ճնշելու միջոց:

Ատելության խոսքը միշտ էլ եղել է սոցցանցերի անբաժան մասը, սակայն հայաստանյան ինտերնետային հատվածում ատելության խոսքը հիմնականում դրսևորվել է երեք ուղղություններով.

ա. Ներքաղաքական լարվածություն՝ քաղաքական ուժերի և դրանց ներկայացուցիչների թիրախավորումից մինչև գաղափարախոսությունների դեմ հարձակումներ: Մասնավորապես՝ ծայրահեղ աջերի և լիբերալ հայացքների կրողների միջև հստակ առճակատումը, որը գնալով սաստկանում է ու հաճախ հենց շնորհիվ սոցցանցերի:

բ. Հայ-ադրբեջանական հակամարտության շարունակությունը սոցցանցերում: Սա ունի բազմաթիվ դրսևորումներ, իսկ Արցախյան երկրորդ պատերազմի ընթացքում սա ստացավ ծայրահեղ դրսևորումներ: Այսպես, Հայաստանի մարդու իրավունքների պաշտպանը պատերազմի ընթացքում մի քանի անգամ ելույթ ունեցավ՝ նշելով հայ օգտատերերի դեմ հարձակումների դեպքերը, որոնց մեջ նկատվում էր նաև Ադրբեջանի պետական քաղաքականություն: Մարդու իրավունքների պաշտպանը մի քանի առանձին ելույթներում նշել է ուղղորդված ատելության խոսքի տարածման մասին. ա, բ, գ: Անշուշտ, հայաստանյան օգտատերերը նույնպես տարածում են հակադարձ ատելության խոսք:

գ. Հայ-թուրքական հարաբերությունները նույնպես հանդիսանում են ատելության խոսքի տարածման պատճառ: Վերջին տարիներին հաճախ հայ-ադրբեջանական և հայ-թուրքական հակամարտությունները նույնացվում են օգտատերերի կողմից և բերում բազմակողմանի բախումների: